ID	Issue Status	Issue Type	Type
335	Remediated	ops-audit	OpsAudit Issue
379	Remediated	standalone	Standalone Issue
383	Remediated	control	Control Issue

394	Remediated	control	Control Issue
399	Remediated	control	Control Issue
400	Remediated	control	Control Issue
401	Remediated	control	Control Issue

402	Remediated	control	Control Issue
407	Remediated	ops-audit	OpsAudit Issue
412	Remediated	ops-audit	OpsAudit Issue

413	Remediated	ops-audit	OpsAudit Issue
414	Remediated	ops-audit	OpsAudit Issue
416	Remediated	ops-audit	OpsAudit Issue
420	Remediated	ops-audit	OpsAudit Issue

421	Remediated	ops-audit	OpsAudit Issue
424	Remediated	ops-audit	OpsAudit Issue
425	Remediated	ops-audit	OpsAudit Issue
431	Remediated	ops-audit	OpsAudit Issue
432	Remediated	ops-audit	OpsAudit Issue

433	Remediated	ops-audit	OpsAudit Issue
434	Remediated	ops-audit	OpsAudit Issue
436	Remediated	ops-audit	OpsAudit Issue

437	Remediated	ops-audit	OpsAudit Issue
438	Remediated	ops-audit	OpsAudit Issue
439	Remediated	ops-audit	OpsAudit Issue
440	Remediated	ops-audit	OpsAudit Issue

441	Remediated	ops-audit	OpsAudit Issue
442	Remediated	ops-audit	OpsAudit Issue
443	Remediated	ops-audit	OpsAudit Issue
444	Remediated	control	Control Issue

454	Remediated	standalone	Compliance Issue
455	Remediated	control	Control Issue
498	Remediated	control	Control Issue

499	Remediated	control	Control Issue
501	Remediated	control	Control Issue
502	Remediated	control	Control Issue

503	Remediated	control	Control Issue
506	Remediated	control	Control Issue
513	Remediated	ops-audit	OpsAudit Issue
525	Remediated	standalone	Standalone Issue
526	Remediated	control	Control Issue
529	Remediated	standalone	Standalone Issue

538	Remediated	control	Control Issue
544	Remediated	standalone	Standalone Issue
554	Remediated	control	Control Issue
562	Remediated	control	Control Issue

572	Remediated	control	Control Issue
579	Remediated	control	Control Issue

590	Remediated	control	Control Issue
595	Remediated	control	Control Issue

615	Remediated	control	Control Issue

616	Remediated	control	Control Issue
626	Remediated	control	Control Issue
627	Remediated	control	Control Issue
628	Remediated	control	Control Issue

654	Remediated	control	Control Issue
664	Remediated	control	Control Issue
665	Remediated	control	Control Issue
707	Remediated	ops-audit	OpsAudit Issue

312	Pending Remediation	ops-audit	OpsAudit Issue
313	Pending Remediation	ops-audit	OpsAudit Issue
339	Pending Remediation	ops-audit	OpsAudit Issue
348	Pending Remediation	ops-audit	OpsAudit Issue

354	Pending Remediation	ops-audit	OpsAudit Issue
376	Pending Remediation	standalone	Standalone Issue
378	Pending Remediation	standalone	Standalone Issue

411	Pending Remediation	ops-audit	OpsAudit Issue
415	Pending Remediation	ops-audit	OpsAudit Issue

417	Pending Remediation	ops-audit	OpsAudit Issue
419	Pending Remediation	ops-audit	OpsAudit Issue

423	Pending Remediation	ops-audit	OpsAudit Issue
427	Pending Remediation	ops-audit	OpsAudit Issue
428	Pending Remediation	ops-audit	OpsAudit Issue
429	Pending Remediation	ops-audit	OpsAudit Issue
430	Pending Remediation	ops-audit	OpsAudit Issue
435	Pending Remediation	ops-audit	OpsAudit Issue

459	Pending Remediation	ops-audit	OpsAudit Issue
460	Pending Remediation	ops-audit	OpsAudit Issue
461	Pending Remediation	ops-audit	OpsAudit Issue
462	Pending Remediation	ops-audit	OpsAudit Issue

505	Pending Remediation	control	Control Issue

509	Pending Remediation	control	Control Issue

524	Pending Remediation	standalone	Standalone Issue
528	Pending Remediation	standalone	Standalone Issue

531	Pending Remediation	ops-audit	OpsAudit Issue
535	Pending Remediation	control	Control Issue
537	Pending Remediation	control	Control Issue
556	Pending Remediation	ops-audit	OpsAudit Issue
563	Pending Remediation	control	Control Issue

570	Pending Remediation	control	Control Issue
571	Pending Remediation	control	Control Issue
574	Pending Remediation	control	Control Issue
576	Pending Remediation	control	Control Issue

580	Pending Remediation	control	Control Issue
581	Pending Remediation	control	Control Issue

586	Pending Remediation	control	Control Issue
589	Pending Remediation	control	Control Issue
591	Pending Remediation	control	Control Issue
593	Pending Remediation	control	Control Issue
596	Pending Remediation	control	Control Issue

597	Pending Remediation	control	Control Issue
598	Pending Remediation	ops-audit	OpsAudit Issue
608	Pending Remediation	control	Control Issue
610	Pending Remediation	standalone	Standalone Issue
613	Pending Remediation	control	Control Issue

621	Pending Remediation	ops-audit	OpsAudit Issue

625	Pending Remediation	control	Control Issue
633	Pending Remediation	control	Control Issue
652	Pending Remediation	control	Control Issue
653	Pending Remediation	control	Control Issue

656	Pending Remediation	standalone	Standalone Issue

658	Pending Remediation	control	Control Issue
659	Pending Remediation	control	Control Issue

666	Pending Remediation	standalone	Standalone Issue
669	Pending Remediation	ops-audit	OpsAudit Issue
671	Pending Remediation	standalone	EVP Reporting
672	Pending Remediation	standalone	EVP Reporting

673	Pending Remediation	standalone	EVP Reporting
674	Pending Remediation	standalone	EVP Reporting
675	Pending Remediation	standalone	EVP Reporting
676	Pending Remediation	standalone	EVP Reporting
677	Pending Remediation	standalone	EVP Reporting
683	Pending Remediation	standalone	Standalone Issue
685	Pending Remediation	control	Control Issue
688	Pending Remediation	standalone	EVP Reporting

689	Pending Remediation	standalone	EVP Reporting
693	Pending Remediation	standalone	EVP Reporting
706	Pending Remediation	ops-audit	OpsAudit Issue
708	Pending Remediation	ops-audit	OpsAudit Issue
710	Pending Remediation	ops-audit	OpsAudit Issue
712	Pending Remediation	standalone	Standalone Issue

713	Pending Remediation	control	Control Issue
47	Open	ops-audit	OpsAudit Issue
333	Open	ops-audit	OpsAudit Issue

355	Open	ops-audit	OpsAudit Issue
362	Open	ops-audit	OpsAudit Issue
364	Open	ops-audit	OpsAudit Issue

396	Open	ops-audit	OpsAudit Issue
405	Open	ops-audit	OpsAudit Issue
406	Open	ops-audit	OpsAudit Issue

409	Open	ops-audit	OpsAudit Issue
410	Open	ops-audit	OpsAudit Issue
418	Open	ops-audit	OpsAudit Issue
426	Open	ops-audit	OpsAudit Issue

648	Open	standalone	Standalone Issue
655	Open	ops-audit	OpsAudit Issue
662	Open	ops-audit	OpsAudit Issue
678	Open	control	Control Issue

682	Open	control	Control Issue

Issue
Backup monitoring and remediation policy does not exist for Data Access Layer There is currently not a process or documented policy to monitor and address backup failures as of the date of our review for DAL and associated Postgres DBs in the AWS platform.
MHK faxes going to error folder instead of inventory Based on an early review of all inbound faxes, it is believed that ~ 1-2% of total faxes received from 8/22/2022-2/17/2023 failed to enter the fax queue due to a code defect. Due to the delay in processing these faxes there is a potential of late authorization decisions. If the fax in the failed-fax folder is identified as a new request and the received date is prior to the received date for the case currently in the system, it could result in cases being decisioned past the due date.
Salesforce New Access - 1 PCMS user was provisioned without proper approval in Q1 2023. For one (1) Salesforce PCMS new user sampled for the period, access was provisioned without the appropriate approval.

Incident ticket not resolved within established service level timeframe in Q4 2022. One Q4 2022 problem/incident ticket tested was not resolved within established service level timelines.
Change tickets closed without verification Corp Change Management area closes tickets as successful without verification if the ticket has been open over a certain time limit
ADP user access review for Q1 2023 excluded 1 user For the Q1 2023 access review, one user was not included in the access review despite having access to ADP.
Salesforce transferred users not reviewed timely. Two Salesforce Provider Contracting (PCMS) transferred users in Q1 2023 were not reviewed within 30 days of transfer. Control exceptions were also noted in 2022.

User reviewed their own access to system backup schedules. User access to the Tivoli Workload Scheduler and Avamar is performed annually to ensure access is restricted to authorized individuals. As part of the Avamar annual recertification, a user reviewed and recertified their own access.
Risk Designations are not assigned for all positions and reviewed annually Policy/Procedure: The policy and procedure documents do not include any information on user roles and responsibilities and determine whether the organization assigns risk designations to all organizational positions as appropriate and review and revise designations every 365 days.
Enterprise Data Warehouse (EDW) Cloudpak applicances (CP4D) do not have antivirus, firewalls, or file integrity monitoring software installed, as they are appliances. Enterprise Data Warehouse (EDW) Cloudpak applicances (CP4D) do not have antivirus, firewalls, or file integrity monitoring software installed, as they are appliances.

No policy/procedure or listing exists for unauthorized software (blacklisting). Policy/Procedure/Implement:There is no direct policy and procedure documentation for blacklisting or the review and updating of the list of unauthorized (blacklisted) software periodically but no less than annually. Implement: BCBSMA does not maintain a list of unauthorized (blacklisted) software via software or tooling.
DXC does not have an explicit policy or procedure which states that tools for maintenance are approved, controlled, monitored and periodically checked. No controls pertaining to preventative maintenance were tested in the DXC SOC 2.DXC does not have an explicit policy or procedure which states that tools for maintenance are approved, controlled, monitored and periodically checked. No controls pertaining to preventative maintenance were tested in the DXC SOC 2. Policy/Procedure/Implement:There is no explicit policy or procedure which states that tools for maintenance are approved, controlled, monitored and periodically checked. No controls pertaining to preventative maintenance were tested in the DXC SOC 2.
Enterprise Data Warehouse (EDW) rollback procedures are not always documented based on sample testing. Implement: Of the sampled changes, 0/25 (100%) of EDW changes had rollback procedures documented. Ref. BCBSMA 2023 Change Management Testing Table
The technical vulnerability management program is evaluated less frequently than HiTrust requires (HITrust requires quarterly). Implement: Noted the technical vulnerability management program is evaluated on an annual basis. Baseline requires this to be quarterly.

Policies and procdures do not include reviewing historic audit logs to determine if high vulnerability scan findings identified in the information system have been previously exploited. Policy/Procedure/Implement:There is no document that specifically calls out reviewing historic audit logs to determine if high vulnerability scan findings identified in the information system have been previously exploitedAssessment team noted that the organization does not review historic audit logs to determine if high vulnerability scan findings identified in the information system have been previously exploited.
Policy and standard documents do not list specifics required by HiTrust regarding commonly used passwords The following points are not covered in any of the BCBSMA Policy and Standard documents: The organization maintains a list of commonly-used, expected, or compromised passwords, and updates the list (i) at least every 180 days (ii) when organizational passwords are suspected to have been compromised (either directly or indirectly); employs automated tools to assist the user in selecting strong passwords and authenticators; and verifies, when users create or update passwords, that the passwords are not found on the organization-defined list of commonly-used, expected, or compromised passwords.
There is not a process implemented to confirm authorized use of shared accounts Implement: Only 1 account of 25 sampled had documented approval of use - there is not a process implemented to confirm authorized use of shared accounts.
There is no policy to provide incident response and contingency training to information systems users consistent with assigned roles and responsibilities and to provide additional training required due to information system changes. Policy/Procedure/Implement:There is no policy to determine whether the organization provides incident response and contingency training to information systems users consistent with assigned roles and responsibilities: (ii) when required by information system changes. Implement: Additional training is not required due to information system changes
There is no explicit policy or procedure for training senior executives for their specific roles and responsibilities. There is no specialized training for the senior executives in their specific roles and responsibilities outside of the scheduled tabletop exercises. Policy/Procedure/Implement:There is no explicit policy or procedure to define that the organization ensures that the senior executives have been trained in their specific roles and responsibilities.Noted the organization does not provide specialized training for the senior executives in their specific roles and responsibilities within the organization outside of the scheduled tabletop exercises.

Implement: A specific specialized and formal role-specific training program does not exist beyond the annual compliance training. Implement: A specific specialized and formal role-specific training program does not exist beyond the annual compliance training.
Additional Data Center controls are required to ensure HiTrust recertification. (CAP52) Implement: The assessment team noted no formal training that workforce members are aware of how to properly respond to perimeter security alarms. (CAP59) Policy/Procedure/Implement:• There is no policy or procedure mandating that a duress alarm is provided whereby a person under duress can indicate such problems and responded to accordingly by the organization. Per inspection of the Markley SOC 2 report, the assessment team noted that the independent assessor did not test for the functioning of duress alarms in the facility. (CAP72) Implement: There is no control tested pertaining to the frequency at which physical access devices are inventoried from Markley and DXC. (CAP73) Implement: No controls pertaining to automated alarms for perimeter doors were tested in the Markley SOC 2. (CAP74) Implement: No controls pertaining to automated alarms for perimeter doors were tested in the Markley SOC 2. (CAP75) Implement: The Markley and DXC SOC2 reports do not explicitly identify a process for testing alarms. (CAP76) Implement: No controls pertaining to automated alarms for perimeter doors were tested in the Markley SOC 2. DXC does not test the logging of automated alarms. (CAP78) Policy/Procedure/Implement:There is no explicit policy or procedure stating that any security threats presented by neighboring premises are identified.No threats regarding neighboring premises were specifically identified.
Security engineering principles are not documented or implemented to the level required by HiTrust. Implement: Noted that the documentation around security engineering principles is not documented or implemented to the level required of this requirement statement for the following IPs: (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns, as well as compensating controls and design patterns needed to mitigate risk; and, (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions.

There is no explicit policy or process which states that specifications for the security control requirements state automated controls will be incorporated in the information system, supplemented by manual controls as needed, as evidenced throughout the SDLC. Implement: • No relevant procedures exist detailing the specific control responsibilities for developers of the information system. • The assessment team noted that the following were not formally defined in our sampled change: (i) a description of the functional properties of the security controls to be employed (ii) design and implementation information for the security controls to be employed that includes: security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces and high-level design documentation at sufficient detail to prove the security control implementation.
No relevant procedures exist detailing the specific control responsibilities for developers of the information system. The following were not formally defined in the sampled change: (i) a description of the functional properties of the security controls to be employed (ii) design and implementation information for the security controls to be employed that includes: security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces and high-level design documentation at sufficient detail to prove the security control implementation. Implement: • No relevant procedures exist detailing the specific control responsibilities for developers of the information system. • The assessment team noted that the following were not formally defined in our sampled change: (i) a description of the functional properties of the security controls to be employed (ii) design and implementation information for the security controls to be employed that includes: security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces and high-level design documentation at sufficient detail to prove the security control implementation.
The DXC SOC2 report does not have a dedicated control related to the repair or modification of the physical components of the facility. Implement: The DXC SOC2 does not have a dedicated control related to the repair or modification of the physical components of the facility
No controls pertaining to automated alarms notifying the authorities were tested in the DXC SOC 2. Implement: No controls pertaining to automated alarms notifying the authorities were tested in the DXC SOC 2.

There is no documented process for data retention to verify the data includes at least (c) secure deletion of data when no longer needed for legal, regulatory, or business reasons, and (d) a process for identifying and securely deleting stored data that exceeds defined retention requirements. Implement: There is no documented process for the (i.c) or (i.d) CSF elements. See baseline testing workplan.
need separate action plans for policy and implement Policy/Procedure/Implement:• The following points were not identified: i. Organization documents and maintains records (PII) that are subject to access by individuals. ii. Titles of the persons or office responsible for receiving and processing requests for access by individuals as organizational records for a period of six years.The assessment team noted that BCBSMA does not hold records that are subject to access by individuals and the titles of the persons or office responsible for receiving and processing requests for access by individuals as organizational records for a period of six years
Additional controls at DXCs data center are required to ensure HiTrust recertification. (CAP71) Implement: No controls pertaining to automated alarms for doors to internal secure areas were tested in the DXCSOC 2. (CAP72) Implement: There is no control tested pertaining to the frequency at which physical access devices are inventoried from Markley and DXC. (CAP75) Implement: The Markley and DXC SOC2 reports do not explicitly identify a process for testing alarms. (CAP76) Implement: No controls pertaining to automated alarms for perimeter doors were tested in the Markley SOC 2. DXC does not test the logging of automated alarms. (CAP77) Implement: No controls pertaining to fire prevention training were tested in the Markley or DXC SOC 2s.
Global Group (GG) user reviewed their own access (Q1 2023) The reviewer of user access groups GG-ClaimOpsAdmin and GG-ClaimOpsPAM reviewed their own access in Q1 2023 recertification.

Informatica (DAL) access provisioning process not implemented User Transfers and Access recertifications are not currently performed for Informatica console users.
DAL AD group inventory is not maintained ET does not currently have a centralized inventory of AD groups with Access to the DAL
Solutions Development recertification users not removed timely For one (1) of 4 Solutions Development recertification users requested to be removed as part of the June 2023 recertification, access to the global group was not removed timely.

Review of DAL transferred users not completed timely and user was not included in the review For two (2) of four (4) total DAL transferred users, the reviews of access following the users' transfer was not completed within 30 days of the transfer date. For one (1) of four (4) total DAL transferred users, the DAL access was not included in the review performed by the manager.
User not removed timely for Salesforce access recertification For one (1) of 13 users sampled where access was requested to be modified or removed as part of the Salesforce access recertification, access was not removed timely.
A precise review was not performed AMS recertified users For three (3) AMS recertified users, a precise review was not performed.

Manager delegated review of associates' access to incorrect person For two (2) of 50 users sampled, one (1) manager delegated their review of their associates' access to the incorrect person.
DW QEDM & DAL Access Recertification System Accounts For the Q3 recertification, 44 accounts with access to the DW, QEDM and DAL applications were not initially recertified as part of the Q3 review.
No direct policy that changes to information assets are controlled and archived. There is no direct policy in place mandating that changes to information assets, including systems, networks, and network services, are controlled and archived.
Global Group (GG) user reviewed their own access (Q4 2023) The reviewer of the GG-ClaimOpsAdmin and GG-ClaimOpsPAM groups has access to those global groups and as a result the reviewer reviewed their own access in Q4 2023 recertification.
Laptops not recovered for termed employees For six (6) of 25 individuals, laptops were not recovered upon termination.
Lack of Quality Control for Non-Standard Contract Terms A formal quality control process is not in place for contracts with non-standard terms and where manual workarounds are needed for settlement calculations.

3 users with DW,QEDM and DAL access, their access was not recertified For three users with DW,QEDM and DAL access, their access was not recertified as part of the initial recertification process.
No evidence of region progression for Blackline During Q4.23 Change management audit, IA could not find evidence of lower region testing for ServiceNow Prod ticket CHG0112950. IA was told IBM performed was responsible for the and it followed their standard change process. However, IA was not able to find any evidence of region progression.
In Q4'23, 21 accounts with Salesforce access not included in the recert 21 accounts with Salesforce access (20 system accounts, 1 human account) were not included in the recertification.
Edifecs Segregation of Duties (SoD) One (1) of a total of 17 users were identified as having inappropriate access to the Edifecs production environment.

6 Informatica service accounts and 1 user account not reviewed for Q1'24 review Six (6) Informatica service accounts and one (1) individual account were not initially reviewed as part of the Q1 2024 review.
74 individuals with the ability to deploy DAL changes have development responsibilities. For the period October 2023 - April 2024, 74 individuals with the ability to deploy DAL changes manually outside of the pipeline have development responsibilities, creating a segregation of duties concern.

Two (2) of 23 transferred users with access to FEP did not have their access reviewed timely. Two (2) of 23 transferred users with access to FEP did not have their access reviewed timely.
Region progression not followed on 3 Tumbleweed Unix servers. IA recently requested for Tumbleweed servers to be included as part of quarterly patch testing beginning from Q2'24(for internal review only). IA identified that region progression was not followed on 2 packages affecting 3 Tumbleweed production servers namely bstep03vr,bstep04vr, and bstpp03vr.

Access not reviewed for 1 Salesforce Transfer
For two (2) of 7 Salesforce Commerce transfer users sampled for the period, access review for Salesforce Commerce access was not reviewed.

For 1 critical vendor, risks not remediated within the defined SLA For 1 out of 19 Critical Vendors, risks were identified as part of the assessment and were not remediated within the defined SLA.
For 1 of 4 users, temporary admin access was not removed timely For 1 of 4 users (100% of the population) that were provisioned temporary admin access, temporary admin access was not removed timely (within 30 days).
Badge access not suspended in a timely manner For 1 of 25 terminated users with badge access, the badge access was not suspended in a timely manner (30 days).
For 9 of 25 terminated users, the users' assets were not recovered For 9 of 25 terminated users, the users' assets were not recovered by BCBSMA and the remote wipes, while initiated, were not completed.

DAL patch reports missing evidence (IPE) System generated evidence of DAL patching was not available for the 2024 testing period.
SF Sales access not granted in accordance with approved new access request For one (1) of 20 instances of new user access sampled during the period, the user's access was not granted in accordance with the approved new access request.
Q4'24 Solutions Development review was not completed timely For the October 2024 Solutions Development monthly review performed, the review was not completed in a timely manner.
Pharmacy Dispensing Fee Calculation Discrepancy SBG found that NEJE achieved an overall dispensing fee performance overage across all distribution channels and networks, totaling $516,843, which was greater than CVSH’s calculated overage of $399,395. Since the dispensing fee guarantees were exceeded, there is no amount due to NEJE. Variance caused by: There were some differences in the inclusion/exclusion methodology used by CVSH. The claims data used by SBG contained approximately 42,000 more claims that the data used by CVSH.

Data sharing arrangements with vendors - process gaps exist with respect to identifying, evaluating, and approving arrangements or changes. Data Governance policies and controls were not sufficient to detect this change. Data feeds to vendor Oral Eye were changed to include PHI/PII. This was not communicated to procurement. legal or info security at the time of change or at contract renewal.
There are no technical controls in place to monitor and track PHI/PII sent to vendors or track changes to data sent to vendors During the review of the vendor Oral Eye's offshoring risks, several process gaps were identified including the lack of controls to detect unauthorized changes in data sharing arrangements with vendors.
DBA/Admin/Priv account activity for the DAL and associated PostgresDBs are currently not being or reviewed periodically Current logging only captures up to three (3) days of logs and isn't configured to log DBA/admin/priv account activity to the level of expectations by the InfoSec group. Since logging is not configured or maintained appropriately, the associated review cannot be performed on a periodic basis in accordance with the documented procedures
Discrepant Specialty Pricing for Commercial Claims (ESI) PwC identified 1,873 discrepant specialty claims that were not cleared in the initial inquiry to ESI. A sample of these claims have been sent to ESI for follow up research. The claims in question were filled at BCBSMA’s custom specialty pharmacies and were subject to a custom specialty guarantee. The total shortfall for these claims is $481,481.

During the PBM migration, member disruption letters were sent to the subscriber's address on file as opposed to the member's alternate address on file due to incorrect logic that was used on an MHK script. This incident has resulted in data breaches and HIPAA violations. During the PBM migration, member disruption letters were sent to the subscriber's address on file as opposed to the member's alternate address on file due to incorrect logic that was used on an MHK script. This incident has resulted in data breaches and HIPAA violations.
Member Touchpoint Measures (MTM) 2022 Since 2021 there has been a steady decline in MTM measures related to member and provider service (inquiry accuracy - manual, inquiry timeliness, and first call resolution). In 2022, the Plan's score hovered close to the 80 point threshold that requires further BCBS Association oversight.
Data Governance frameworks are not clearly understood across the enterprise, creating risk of data misuse and breaches. Data Governance frameworks are not clearly understood across the enterprise, creating risk of data misuse and breaches. Privacy incidents continue to occur (12 incidents in last 18 months).

Enterprise Data Warehouse (EDW) and RTMS changes did not have sufficient testing documentation, approvals, risk analysis and/or rollback procedures based on sample testing.
Implement: The assessment team obtained and inspected a sample of 25 change records from both EDW and RTMS. Of these changes, 16/25 (64%) of EDW changes were not appropriately tested. In addition, 1/25 (4%) of EDW and 1/25 (4%) of RTMS changes were approved by a qualified reviewer. In addition, 0/25 (0%) of EDW changes did have a risk analysis performed prior to implementation. Rollback analysis was not present on certain samples.
Ref. BCBSMA 2023 Change Management Testing Table

BCBSMA does not formally outline an approved application store for mobile devices accessing the in-scope systems.
Policy/Procedure: the organization does not formally outline an approved application store for mobile devices accessing the in-scope systems.

RTMS and EDW asset inventory did not include backup information, license information, business value, or portable/personal device. Implement: The assessment team noted that the RTMS and EDW inventory did not include backup information, license information, business value, or portable/personal device.
There is no direct policy identifying common vulnerabilities and mandating secure coding guidelines to the degree of specificity required by HiTrust. Policy/Procedure/Implement:There is no direct policy identifying common vulnerabilities to the degree of specificity outlined in the illustrative procedures of the baseline.• Implement: There is no direct policy in place mandating that developed applications are based on secure coding guidelines to prevent common coding vulnerabilities in software development processes including but not limited to: i. injection flaws, particularly SQL injection. (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.); ii. buffer overflow (Validate buffer boundaries and truncate input strings) iii. insecure cryptographic storage (Prevent cryptographic flaws) iv. insecure communications (Properly encrypt all authenticated and sensitive communications); v. improper error handling (Do not leak information via error messages); vi. broken authentication/sessions (Prevent unauthorized individuals from compromising legitimate account credentials, keys or session tokens that would otherwise enable an intruder to assume the identify of an authorized user); vii. cross-site scripting (XSS), e.g., validate all parameters before inclusion, utilize context-sensitive escaping, etc.); viii. improper access control, such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access functions (e.g., properly authenticate users and sanitize input, and do not expose internal object references to users); ix. cross-site request forgery (CSRF), e.g., do not reply on authorization credentials and tokens automatically submitted by browsers; and x. any other input-validation vulnerability listed in the OWASP top 10. Applications that are not developed using secure coding guidelines undergo automatic or manual input validation checks during testing and annually thereafter, and such checks include: i. dual input or other input checks, such as boundary checking or limiting fields to specific ranges of input data, to detect the following errors: 1. out-of-range values

There was no configuration shown to require immediate selection of a new password upon account recovery for the active directory. Implement: There was no configuration shown to require immediate selection of a new password upon account recovery for the active directory.
BCBSMA does not have a review and approval process implemented for shared accounts explicitly. Implement: The assessment team obtained a list of all group accounts (>250) with access to EDW and selected a sample of 25 shared group accounts and inspected 165_03282023_EDW Shared Group Accounts Sample to determine that 1/25 of the sampled shared/group accounts are reviewed of any requests and approved by the appropriate personnel.
Privileged access reviews are not occurring every 60 days as required by HiTrust. They currently occur every 90 days. Implement: The assessment team noted that privileged access reviews are not occurring every 60 days.
Networking sessions are not configured to close after 30 minutes of inactivity. Implement: The GPO is not configured to close the network session after 30 minutes of inactivity.
List of auditable events: Policy documentation doesnt explicitly specify that a listing of auditable events are reviewed and updated periodically within 365 days, including rationale for the list being adequate to support investigations or monitoring. Policy/Procedure/Implement:Policy documentation doesn't explicitly specify that the organization provides the listing of auditable events and supporting rationale are reviewed and updated periodically within 365 days.
RTMS and EDW application changes were not appropriately tested and/or approved by a qualified reviewer. Implement: The assessment team obtained and inspected a sample of 25 change records from both EDW and RTMS. Of these changes, 16/25 (64%) of EDW changes were not appropriately tested. In addition, 1/25 (4%) of EDW and 1/25 (4%) of RTMS changes were approved by a qualified reviewer. In addition, 0/25 (0%) of EDW changes did not have a risk analysis performed prior to implementation. In addition, of these changes, 0/25 (100%) of EDW changes had rollback procedures documented. Ref. BCBSMA 2023 Change Management Testing Table

Change Advisory Board (CAB) Enhancement Needed The Change Advisory Board (CAB) may not review a solution before changes are approved, and risk determination of changes do not consider information security risks.
Lack of consistent implementation of access provisioning and deprovisioning controls Lack of consistent implementation of access provisioning and deprovisioning controls: For two Active Directory (AD) groups reviewed, approximately 100 users were added without leader approval. In addition, an AD removal request was on hold for a month pending the leader's approval. Although the removal request was on hold, offshore vendor access was disabled timely as Palo Alto logs evidenced the firewall policy configuration was updated timely.
Lack of explicit and consistent AD group remote access management Lack of explicit and consistent AD group remote access management: 1). There is no periodic access review of users within AD groups; 2). Users were set up with both VPN and VDI access; and 3). BYOD users were observed with VPN access.
Lack of Different Information Security Risk Considerations for Onshore vs. Offshore Associates or Contractors in ET, InfoSec, and Third Party Vendor Management Policies and Standards Associate Remote Access Standard does not have different information security risk considerations or requirements for onshore vs. offshore associates or contractors.

Segregation of duties (SoD) is not enforced for changes to the DAL.
For two DAL (2) of 25 changes sampled, the same individual was both the change developer and the approver.

DAL System Changes are not logged and monitored.
For the Q1 - Q3 2023 period, the completeness of the population of changes for the Data Access Layer (DAL) application from the ticketing system could not be validated for the period as evidence to reconcile the manually created tickets to the production source was not available which could result in an incomplete or inaccurate population. For the Q4 2023 period, the completeness of the population of manually deployed changes for the Data Access Layer (DAL), outside of the pipeline, could not be validated for the period as evidence to reconcile the manually created ticket to the production source was not available which could result in an incomplete or inaccurate population.

Update: For the Q4 2023 - Q1 2024 period, the completeness of the population of manually deployed changes for the Data Access Layer (DAL), outside of the pipeline, could not be validated for the period as evidence to reconcile the manually created ticket to the production source was not available which could result in an incomplete or inaccurate population.

There is insufficient vendor oversight relating to data sharing of participant data, creating risk of inaccurate financial reporting.

There is insufficient vendor oversight relating to data sharing of participant data, creating risk of inaccurate financial reporting.

Lack of formal review over QEDM configuration with contract terms

There is no formal process in place to ensure that QEDM is configured correctly to reflect the latest contract terms, especially when contracts are renegotiated or amended.

Pricing Update Process Gap There was a finding in the FEP Overpayment Self-Assessment Pricing Update testing which uncovered a process gap. The update requested to terminate pricing for a provider in May 2023. The pricing was not updated until November 2023 upon request by Network Management. No one submitted a request to reprocess the claims which paid between May and November 2023 (aka a recovery request), so many claims were paying in-network when they should have been paying out-of-network.
Access was not requested and approved for 1 user within the listings QEDM & DW For one (1) of 26 users sampled, access was not requested and approved at the application level.
BQ access role was not recertified in Q4'23 For one user with BQ access, their BQ access role was not recertified as part of the initial recertification process. For one user with BQI access, their BQI access role was not recertified as part of the initial recertification process.
Discrepancy in ESI Specialty Pricing for Commercial Business During the Commercial Claims Audit, the external auditors identified 7,551 claims that adjudicated below the per claim specialty AWP pricing guarantee. The shortfall amount estimated for these claims totals $2,865,379.
Server OS Service Accounts Access Cert Service accounts with access to server operating systems are not certified on a recuring basis.

DAL prod access missing request and approval One (1) of XX users sampled was provisioned DAL production environment access without a documented request and approval for the production environment access.
3 Ataccama service accounts not reviewed for Q1'24 review. Three (3) Ataccama service accounts were not reviewed as part of the Q1 2024 review.
1 account with BQI access was not included in the recertification. 1 account with BQI access was not included in the recertification.
IPE for AWS S3 buckets AWS S3 buckets do not have sufficient reporting and archive data to support audit requirements.

Twelve (12) users identified having access to both the pipeline admin role and the developer role for pipeline changes Twelve (12) users were identified having access to both the pipeline admin role and the developer role for pipeline changes for the period through 6/20/2024.
Six (6) Abacus accounts were not included in the Q1 2024 review. Six (6) Abacus accounts were not included in the Q1 2024 review.

C&A not validated - Tumbleweed WebApp Changes Incomplete IPE for change reporting. The evidence for completeness of the population of the Axway Tumbleweed (SFTP) WebApp changes could not be validated.
One Salesforce Commerce account was not included in the Q2 2024 review. One Salesforce Commerce account was not included in the Q2 2024 review.
One (1) userwas not removed as part of the Q2 2024 recertification. One (1) user whose access was requested to be removed was not removed as part of the Q2 2024 recertification.
User did not have their access revoked timely - Q1 2024 1 user identified as part of the walkthrough sample did not have their access revoked timely as part of the Q1 2024 review.
Three (3) Ataccama accounts were not reviewed as part of the Q2 2024 review Three (3) Ataccama accounts were not reviewed as part of the Q2 2024 review.

One (1) user was provisioned access to a BQ role that did not correspond to access requested One (1) of XX users sampled was provisioned access to a BQ role that did not correspond to the role that was requested and approved.
Specialty Discount Discrepancy (MAPD) SBG identified 417 claims that adjudicated below the per claim specialty AWP discounts with an estimated shortfall amount of $508,718.
1 user was provisioned DW prod access without request and approval One (1) of XX users sampled was provisioned Data Warehouse production environment access without a documented request and approval for the production environment access.
Access to DAL ADH S3 Buckets Accounts with access to DAL ADH S3 buckets are not certified for appropriateness on a recurring basis.
DAL AWS Group Access AWS Roles with the naming convention of 'RO' for 'Read-Only' have edit access to AWS assets.

OM#4 - The Plan inadvertently charged FEP for administrative costs for FERM captive.
During the review of transactions with affiliated Plan organizations, it was noted that the Plan allocated to FEP as administrative cost $11,723.00 for FERM Captive and there was no documentary evidence that profit was removed, or that the charges met all the terms of an exception that would allow the Plan to charge an amount greater than cost to the Program.

2 of 25 recertified RTMS users, access marked appropriate despite the accounts being inactive (Sept 2024) For 2 of 25 recertified users sampled from the Summer 2024 recertification, the access for the accounts was marked as appropriate by the application owner despite the accounts being inactive accounts.
5 of 25 vulnerabilities were not resolved within the determined SLAs. For 5 of 25 vulnerabilities identified, the vulnerabilities were not resolved within the determined SLAs.
DAL AWS RDS patching reporting not retained Patching evidence (i.e. patch reporting) is not retained for DAL AWS RDS
AWS Operating System (OS) security configurations AWS OS security configurations are not reviewed to ensure alignment with BCBSMA policies and standards.

Improvement opportunity noted to confirm the authorized signer listings are complete and accurate for all banks BCBSMA has a relationship.

Currently, there is no formalized process to confirm that the authorized signer listing is complete and accurate for all banking institutions BCBSMA has a relationship. This was discovered in the MBA/Indigo review and applies to all bank relationships. Bank signatories are granted authority from each legal entity's governing body and the signatories on file at each bank are updated using bank specific documentation. Note that intercompany transfers from these entities are approved internally by Finance Management and processed via bank web portals by Cash Management associates. Bank signatories are needed to sign banking documents. However, this still may result in unauthorized individuals performing banking transactions, leading to potential fraud, or operational disruptions.

DW transfer access Q4'24
For nine (9) of 31 instances of transferred users' access sampled during the period, the users' access was not reviewed within 30 days.

For 12 out of 25 samples, ASCBE Errors were not worked in a timely manner.
Because ASCBE Errors were not worked in a timely manner, ASC billings and receivables may be inaccurate, incomplete, and untimely.

MLR Survey Results - Missed Package

An automated process that retrieves Medical Loss Ratio (MLR) survey results from a third-party vendor failed to process one of the monthly update files, as the file received was in a non-standard format and didn't meet the agreed upon specifications. This prompted the need for manual intervention/error resolution where the appropriate steps were not followed, resulting in group size records not being updated in timely.

Incorrect categorization of Rx claims for rebate guarantees and discounts (no financial impact)

Rebate guarantees and discounts were calculated incorrectly by CVS Health due to a classification error relating to Retail90 claims. CVSH re-performed the calculations, which led to increases in the guaranteed rebates and discount amounts; however, since the actual amounts earned by BCBSMA were higher than the recalculated guaranteed amounts, there was no financial impact. SBG recommends that CVSH implement appropriate corrective measures to ensure that the correct Retail90 logic is applied to BCBSMA's pricing reconciliation and as well as the correct application of claim inclusion and exclusion.

Application Change Management consistency, manual controls

Management has not documented existing change management processes across BCBSMA and determined future state controls to remediate root causes of 2023 audit findings communicated in Q4 2023. Management was engaging a vendor to assess in 2024/2025. New audit issues have occurred for MAR audit in 2024; no evidence to support testing prior to production for Blue Quote.

Active Directory Group Ownership

There is no inventory of Active Directory (AD) groups and their purposes, or periodic review of appropriateness of users in most AD groups. Lack of clarity over the purpose of certain groups has created issues with recertifying access of desktop administrators and created issues in which certain developers had inappropriate access in 2023 (SOC audit and offshore Palo Alto developer audit).

Logical Access - CVS provisioning Observation: CVS requires up to 2 weeks to provision certain access, which can result in users being deleted by BCBSMA's automated weekly process to remove access if all requested access does not agree with access provisioned.
Access Recertification - Leader review Leaders across BCBSMA do not always apply required level of rigor in responding to application access recertification requests.
Application Change Management and Monitoring DAL ODH changes could not be validated as complete, creating SOC 1 and SOC 2 audit issues in 2024.
Segregation of Duties - Edifecs There is currently no logging and monitoring of changes to Edifecs by system administrators.
Cloud Disaster Recovery Plan Not all aspects of BCBSMA's cloud environment are included in BCBSMA's Disaster Recovery / Crisis Response Plans. Enterprise Technology continues to execute on the plan to include the remainder of the environment.
Solutions Development Recertification not timely For the February 2025 Solutions Development monthly review, one user did not have their access reviewed timely and did not have their access removed timely (within the specified month).
MFA/2FA not enabled for IICS MFA/2FA and VPN are not required for user authentication to the IICS application.
DAL ADH Multi-Region Failure Data Access Layer Analytic Data Hub (ADH) does not have a Disaster Recovery or Business Continuity Plan in place which contemplates a potential multi-region failure. In the immediate term, the EDW may be used as a data source if DAL ADH is unavailable. The risk will increase if a plan isn’t implemented prior to the deprecation of the EDW.

Segregation of Duties - Salesforce instances Segregation of duties controls are not yet implemented in Salesforce instances. SOD is an area of increasing interest from external auditors, and an area with past issues from the 2024 audit (IICS, Edifecs). A recommendation was made in 2024 to revisit this across the ET organization.
Multi-Factor Authentication (MFA) not enabled for Informatica Intelligent Cloud Solutions (IICS) Multi-Factor Authentication (MFA) and VPN are not required for user authentication to the IICS application.
Pharmacy Discount Performance Calculation Discrepancy SBG found that NEJE achieved an overall AWP discount performance overage across all distribution channels and networks, totaling $9,160,178. Although SBG's amount was significantly greater than CVSH's $7,994,741 calculation, both represent overall guarantee overages, therefore no amounts are due to NEJE. Variance caused by: CVSH applied an incorrect rate to Specialty Chain Preferred Claims (Rates are applied at the aggregate level, so no member liability impacts). The claims data used by SBG contained approximately 42,000 more claims that the data used by CVSH.
Special Discount Rate Change With No Notification to NEJE Based on the Agreement provided for the audit, SBG identified 4,937 specialty claims filled at network specialty pharmacies that did not achieve the guaranteed per-claim rates. SBG sent a sample of fifteen claims to CVSH to research the cause of the variance. CVSH responded that guaranteed rates were changed on May 1, 2023. CVSH was unable to provide any documentation to show the validity of the new rates as they made the adjustments to the contracted rates without notifying NEJE. SBG recommends that NEJE ensures that CVSH notify them in advance of any adjustments to contracted rates. CVSH did not provide a reconciliation for the overall effective specialty discount and dispensing fee performances at network pharmacies; however, SBG found that CVSH exceeded the contracted 21.25% discount rate and met the $0.00 dispensing fee guarantee.
Pharmacy Package Size Violations SBG determined that no material package size violations occurred during the audit period. SBG identified eighteen claims where the package size did not align with the metric quantity dispensed. These errors may be attributed to pharmacist error at the point of sale. The monetary impact of these errors was immaterial, however SBG recommends that CVSH implements edits to ensure that the metric quantity aligns with the package size available for the given NDC.
Snowflake Role Definitions Snowflake DAL role definitions are missing or incorrect.

EDW Netezza ETL Access Recert Access re-certifications are not performed for EDW Netezza ETL ("Netezza Transformation")
BCBSMA account receivable does not reconcile with the account payable amounts from the Federal Employee Program Directors Office From 2019 FEP CPR Audit Finding: FAM Volume 3, Chapter 3 – FEP Benefit Payable Confirmation, states, “On a quarterly basis, Plans must confirm the Plan’s general ledger receivable, and identify variances with the FEP Director’s Office Benefit Expenses Payable Account. The purpose of this reconciliation is to identify and categorize the variance between the Plan’s FEP benefits receivable balance and the FEP benefits payable balance recorded at the FEP Director’s Office. The FEP Benefit Payable Confirmation of Balances Statement of Procedures contains the following instructions for differences due to timing, “All amounts recorded as timing should reverse during the following quarter and not carry over to additional quarters. Plans should identify the amounts and reasons for their timing differences and provide documentation supporting these amounts.”
DAL is not included in current enterprise DRP or BCP Application does not have a Disaster Recovery or Business Continuity Plan in place (migration to new AWS cloud hosting vendor completed May 2022).

There are no systematic timestamps that are required when updating or quality-checking MyPBM pharmacy benefits, which may lead to benefit changes that are not quality-checked and ultimately inaccurate MyPBM is a critical CVS system to manage and exchange benefits between BCBSMA and CVS. Identified through the PBM implementation engagement, IA notes that benefits within MyPBM can be edited after the original quality check upon entry. This may result in inaccurate benefit set-up and configuration.
BARs is not always used as source of truth for benefits due to known system and reporting limitations. Additionally, there is no direct QC of BAR's benefits which may to benefits that are configured but do not match the Sales and UW-approved benefits This risk has been realized in the issue with PillarRx benefits per I#356 and I#357, which notes that there is no QC or systematic reporting or QC regarding accounts and members which should have the Pillar Rx benefit.
Operations was not notified of an issue with accumulation rules feeds and had this occurred post 1/1/23, it could have led to inaccurate accumulation data being extracted from NASCO and sent to the PBM. As a part of the PBM engagement, IA notes that accumulation rules feeds are important for NASCO to know which accumulation information to extract and send to the PBM. Without proper notification and remediation, this could lead to inaccurate accumulation data being extracted from NASCO and sent to the PBM.

Observation 1: A sample of Medicare Secondary Payer (MSP) claims were not reprocessed by CVS on behalf of the New England Joint Enterprise (NEJE). NEJE disagrees with this observation. OHI (Other Health Insurance) information was received after the date of fill and after claims were processed for some members. The claims were not yet reprocessed with Medicare as the Secondary Payer as the retrospective gathering of information is required through confirmation and outreach from the beneficiary's other payer was still in process. CVS Caremark cannot reprocess the claims to correct the payer order without receiving the necessary information from the other payer. While this process may exceed beyond the date of annual PDE reconciliation, CVS Caremark previously triggered the outreach process to the other payers in following receipt of the COBC records and continues to send outreach to the other payers bimonthly to seek resolution of the claims. Of note, COBC records can be received for months after the applicable coverage, including beyond the PDE reconciliation date.
Finding 1: MSLC asserts The Plan did not report DIR associated with pharmacy benefit manager (PBM) payments related to pharmacy contractual guaranteed rates for drug pricing for 2021. NEJE disagrees with this finding. CMS Auditors (Myers and Stauffer) reviewed the contracts in place between the Plan and their downstream entities, and the contracts in place between the PBM and any of their downstream entities, for contractual provisions that may result in financial exchanges that qualify as DIR. This includes provisions in place between the PBM and the pharmacy that result in additional payments to or from the pharmacy that are not already included in the negotiated price of the drugs dispensed, as reported in the PDE data. The Plan did not report DIR associated with PBM payments related to pharmacy contractual guaranteed rates for drug pricing for 2021, as these payments are on a book of business level between CVS and pharmacies and do not change the cost to the Plan. The auditors assert that this should have been included as DIR.
Finding 2: MSLC asserts The Plan did not report DIR associated with pharmacy benefit manager (PBM) payments related to pharmacy contractual guaranteed rates for drug pricing for 2021. NEJE disagrees with the finding. CMS auditors (Myers and Stauffer) noted: As part of our procedures, we attempted to reconcile the total amounts of the Performance Network Rebates amounts down to the contract-PBP level. Per CVS Caremark, “The Plan decides which portions of its business will be participating in the PNR program. CVS does not decide this on behalf of the Plan. Currently, CVS tracks the following carriers as PNR-participants: 8580, 8582, 8584, 8586, 8588, 8590, 8592, and 8594. Understanding that not all these carriers conform to a contract-PBP that is under the scope of the audit.” The Plan is made up the following carriers: 8582, 8586, 8590, and 8594. As the PNR is collected for additional carriers aside from the Plan, we worked to verify the allocation from how the PNR is calculated, and how that amount flows to the amounts reported at the Contract-PBP level. CVS provided detail to support the amount of PNR that was reported at the Contract-PBP, but CVS did not provide sufficient information to reconcile the amount reported to the amount calculated at the overall collection amount for PNR.

The security policy doesn't include specific elements required by HiTrust. Policy/Procedure: Policy does not note explicitly iv) the latest controls, compliance and assurance requirements and arrangements of national bodies and of new legislation or regulation; (v) the latest guidance and recommendations from professional associations and from information privacy commissioners regarding the protection of covered information; (vi) the results of legal cases tested in courts that thereby establish or cancel precedents and established practices. Implement: The assessment team noted that the results of legal cases are not explicitly considered in the development of the security policy.
Bluetooth file sharing and peer to peer networking protocols are not disabled on workstations. Implement: Bluetooth file sharing was not disabled on workstations. We noted that the organization allows for the use of Bluetooth from computer peripherals but intends to lock down Bluetooth file sharing abilities in the future.
The policy for inventories of IT assets did not include specific information required by HiTrust. Policy/Procedure/Implement: • The assessment team noted that the policy does not talk about xii. operational status; xiii. primary and secondary administrators; and xiv. primary user.The assessment team noted that the RTMS inventory did not include backup information, license information, business value, or portable/personal device. The assessment team noted that "025_03162023_Endpoints Population" did not include: vi. presence of virtual machines vii. application software version/license information ix. logical location (e.g., IP address, position with the IS architecture) x. Media access control (MAC) address xii. operational status xiii. primary and secondary administrators
BCBSMA does not have a review and approval process implemented for shared accounts explicitly. Implement: The assessment team obtained a list of all group accounts with access to EDW and selected a sample of 25 shared group accounts and inspected 165_03282023_EDW Shared Group Accounts Sample to determine that 1/25 of the sampled shared/group accounts are reviewed of any requests and approved by the appropriate personnel. It was noted that BCBSMA does not have a approval review process implemented for shared accounts explicitly.

Insufficient Data Validation Process During RIT Plan Record Keeper Transition from TELUS to Fidelity On 1/1/24, the record-keeping responsibilities for the RIT plan transitioned from TELUS to Fidelity. As part of the transition, TELUS collaborated with Fidelity directly to ensure data migration was completed. However, there was no formalized, centralized process within BCBSMA to validate the accuracy and completeness of participant data transferred from TELUS to Fidelity. This lack of a validation process creates potential risks to the integrity of the RIT plan's data. Inaccuracies in participant demographics, account balances, elections and/or any other critical data elements may lead to participant and compliance issues, or errors in BCBSMA's financial reporting.
It could not be determined that the amounts reported on Line 2 of the FEP Benefit Payable Confirmations for the quarters indicated are properly identified and supported. FAM Volume 3, Chapter 3 – FEP Benefit Payable Confirmation, states, "On a quarterly basis, Plans must confirm the Plan's general ledger receivable, and identify variances with the FEP Director's Office Benefit Expenses Payable Account. The purpose of this reconciliation is to identify and categorize the variance between the Plan's FEP benefits receivable balance and the FEP benefits payable balance recorded at the FEP Director's Office. The FEP Benefit Payable Confirmation of Balances Statement of Procedures contains the following instructions for differences due to timing, "All amounts recorded as timing should reverse during the following quarter and not carry over to additional quarters. Plans should identify the amounts and reasons for their timing differences and provide documentation supporting these amounts."
FEP Contract Non-Compliance Due to Provider Recoupment Letters Not Sent When FEP overpayments are recuperated by A/R offsets, BCBSMA does not send the FEP contractually required provider recoupment reminder letters at exactly 30, 60, and then 90 days. Instead, letters are not sent until around 45 days after A/R creation. Due to the greater level of scrutiny on contract adherence under new Office of Personnel Management (OPM) leadership, we are not in compliance with the contract.
For one (1) of 27 changes sampled, approval not available For one (1) of 27 changes sampled, documented approval for the change prior to implementation was not available.

Lack of Quality Control for Group Measures Signed Post 12/1

A formal quality control process is not in place to track Provider Organizations that signed their agreement after the 12/1 notices are sent. This notice provides the final measure set for performance determination for the following year, e.g. 12/1/24 notices provide the measure sets for the 2025 measurement period.

Title (Issue)
Backup monitoring and remediation policy does not exist for Data Access Layer
MHK faxes going to error folder instead of inventory
Salesforce New Access - 1 PCMS user was provisioned without proper approval in Q1 2023.

Incident ticket not resolved within established service level timeframe in Q4 2022.
Change tickets closed without verification
ADP user access review for Q1 2023 excluded 1 user
Salesforce transferred users not reviewed timely.

User reviewed their own access to system backup schedules.
Risk Designations are not assigned for all positions and reviewed annually
Enterprise Data Warehouse (EDW) Cloudpak applicances (CP4D) do not have antivirus, firewalls, or file integrity monitoring software installed, as they are appliances.

No policy/procedure or listing exists for unauthorized software (blacklisting).
DXC does not have an explicit policy or procedure which states that tools for maintenance are approved, controlled, monitored and periodically checked. No controls pertaining to preventative maintenance were tested in the DXC SOC 2.DXC does not have an explicit policy or procedure which states that tools for maintenance are approved, controlled, monitored and periodically checked. No controls pertaining to preventative maintenance were tested in the DXC SOC 2.
Enterprise Data Warehouse (EDW) rollback procedures are not always documented based on sample testing.
The technical vulnerability management program is evaluated less frequently than HiTrust requires (HITrust requires quarterly).

Policies and procdures do not include reviewing historic audit logs to determine if high vulnerability scan findings identified in the information system have been previously exploited.
Policy and standard documents do not list specifics required by HiTrust regarding commonly used passwords
There is not a process implemented to confirm authorized use of shared accounts
There is no policy to provide incident response and contingency training to information systems users consistent with assigned roles and responsibilities and to provide additional training required due to information system changes.
There is no explicit policy or procedure for training senior executives for their specific roles and responsibilities. There is no specialized training for the senior executives in their specific roles and responsibilities outside of the scheduled tabletop exercises.

Implement: A specific specialized and formal role-specific training program does not exist beyond the annual compliance training.
Additional Data Center controls are required to ensure HiTrust recertification.
Security engineering principles are not documented or implemented to the level required by HiTrust.

There is no explicit policy or process which states that specifications for the security control requirements state automated controls will be incorporated in the information system, supplemented by manual controls as needed, as evidenced throughout the SDLC.
No relevant procedures exist detailing the specific control responsibilities for developers of the information system. The following were not formally defined in the sampled change: (i) a description of the functional properties of the security controls to be employed (ii) design and implementation information for the security controls to be employed that includes: security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces and high-level design documentation at sufficient detail to prove the security control implementation.
The DXC SOC2 report does not have a dedicated control related to the repair or modification of the physical components of the facility.
No controls pertaining to automated alarms notifying the authorities were tested in the DXC SOC 2.

There is no documented process for data retention to verify the data includes at least (c) secure deletion of data when no longer needed for legal, regulatory, or business reasons, and (d) a process for identifying and securely deleting stored data that exceeds defined retention requirements.
need separate action plans for policy and implement
Additional controls at DXCs data center are required to ensure HiTrust recertification.
Global Group (GG) user reviewed their own access (Q1 2023)

Informatica (DAL) access provisioning process not implemented
DAL AD group inventory is not maintained
Solutions Development recertification users not removed timely

Review of DAL transferred users not completed timely and user was not included in the review
User not removed timely for Salesforce access recertification
A precise review was not performed AMS recertified users

Manager delegated review of associates' access to incorrect person
DW QEDM & DAL Access Recertification System Accounts
No direct policy that changes to information assets are controlled and archived.
Global Group (GG) user reviewed their own access (Q4 2023)
Laptops not recovered for termed employees
Lack of Quality Control for Non-Standard Contract Terms

3 users with DW,QEDM and DAL access, their access was not recertified
No evidence of region progression for Blackline
In Q4'23, 21 accounts with Salesforce access not included in the recert
Edifecs Segregation of Duties (SoD)

6 Informatica service accounts and 1 user account not reviewed for Q1'24 review
74 individuals with the ability to deploy DAL changes have development responsibilities.

Two (2) of 23 transferred users with access to FEP did not have their access reviewed timely.
Region progression not followed on 3 Tumbleweed Unix servers.

Access not reviewed for 1 Salesforce Transfer

For 1 critical vendor, risks not remediated within the defined SLA
For 1 of 4 users, temporary admin access was not removed timely
Badge access not suspended in a timely manner
For 9 of 25 terminated users, the users' assets were not recovered

DAL patch reports missing evidence (IPE)
SF Sales access not granted in accordance with approved new access request
Q4'24 Solutions Development review was not completed timely
Pharmacy Dispensing Fee Calculation Discrepancy

Data sharing arrangements with vendors - process gaps exist with respect to identifying, evaluating, and approving arrangements or changes. Data Governance policies and controls were not sufficient to detect this change.
There are no technical controls in place to monitor and track PHI/PII sent to vendors or track changes to data sent to vendors
DBA/Admin/Priv account activity for the DAL and associated PostgresDBs are currently not being or reviewed periodically
Discrepant Specialty Pricing for Commercial Claims (ESI)

During the PBM migration, member disruption letters were sent to the subscriber's address on file as opposed to the member's alternate address on file due to incorrect logic that was used on an MHK script. This incident has resulted in data breaches and HIPAA violations.
Member Touchpoint Measures (MTM) 2022
Data Governance frameworks are not clearly understood across the enterprise, creating risk of data misuse and breaches.

Enterprise Data Warehouse (EDW) and RTMS changes did not have sufficient testing documentation, approvals, risk analysis and/or rollback procedures based on sample testing.
BCBSMA does not formally outline an approved application store for mobile devices accessing the in-scope systems.

RTMS and EDW asset inventory did not include backup information, license information, business value, or portable/personal device.
There is no direct policy identifying common vulnerabilities and mandating secure coding guidelines to the degree of specificity required by HiTrust.

There was no configuration shown to require immediate selection of a new password upon account recovery for the active directory.
BCBSMA does not have a review and approval process implemented for shared accounts explicitly.
Privileged access reviews are not occurring every 60 days as required by HiTrust. They currently occur every 90 days.
Networking sessions are not configured to close after 30 minutes of inactivity.
List of auditable events: Policy documentation doesnt explicitly specify that a listing of auditable events are reviewed and updated periodically within 365 days, including rationale for the list being adequate to support investigations or monitoring.
RTMS and EDW application changes were not appropriately tested and/or approved by a qualified reviewer.

Change Advisory Board (CAB) Enhancement Needed
Lack of consistent implementation of access provisioning and deprovisioning controls
Lack of explicit and consistent AD group remote access management
Lack of Different Information Security Risk Considerations for Onshore vs. Offshore Associates or Contractors in ET, InfoSec, and Third Party Vendor Management Policies and Standards

Segregation of duties (SoD) is not enforced for changes to the DAL.

DAL System Changes are not logged and monitored.

There is insufficient vendor oversight relating to data sharing of participant data, creating risk of inaccurate financial reporting.
Lack of formal review over QEDM configuration with contract terms

Pricing Update Process Gap
Access was not requested and approved for 1 user within the listings QEDM & DW
BQ access role was not recertified in Q4'23
Discrepancy in ESI Specialty Pricing for Commercial Business
Server OS Service Accounts Access Cert

DAL prod access missing request and approval
3 Ataccama service accounts not reviewed for Q1'24 review.
1 account with BQI access was not included in the recertification.
IPE for AWS S3 buckets

Twelve (12) users identified having access to both the pipeline admin role and the developer role for pipeline changes
Six (6) Abacus accounts were not included in the Q1 2024 review.

C&A not validated - Tumbleweed WebApp Changes
One Salesforce Commerce account was not included in the Q2 2024 review.
One (1) userwas not removed as part of the Q2 2024 recertification.
User did not have their access revoked timely - Q1 2024
Three (3) Ataccama accounts were not reviewed as part of the Q2 2024 review

One (1) user was provisioned access to a BQ role that did not correspond to access requested
Specialty Discount Discrepancy (MAPD)
1 user was provisioned DW prod access without request and approval
Access to DAL ADH S3 Buckets
DAL AWS Group Access

OM#4 - The Plan inadvertently charged FEP for administrative costs for FERM captive.

2 of 25 recertified RTMS users, access marked appropriate despite the accounts being inactive (Sept 2024)
5 of 25 vulnerabilities were not resolved within the determined SLAs.
DAL AWS RDS patching reporting not retained
AWS Operating System (OS) security configurations

Improvement opportunity noted to confirm the authorized signer listings are complete and accurate for all banks BCBSMA has a relationship.

DW transfer access Q4'24

For 12 out of 25 samples, ASCBE Errors were not worked in a timely manner.

MLR Survey Results - Missed Package
Incorrect categorization of Rx claims for rebate guarantees and discounts (no financial impact)
Application Change Management consistency, manual controls
Active Directory Group Ownership

Logical Access - CVS provisioning
Access Recertification - Leader review
Application Change Management and Monitoring
Segregation of Duties - Edifecs
Cloud Disaster Recovery Plan
Solutions Development Recertification not timely
MFA/2FA not enabled for IICS
DAL ADH Multi-Region Failure

Segregation of Duties - Salesforce instances
Multi-Factor Authentication (MFA) not enabled for Informatica Intelligent Cloud Solutions (IICS)
Pharmacy Discount Performance Calculation Discrepancy
Special Discount Rate Change With No Notification to NEJE
Pharmacy Package Size Violations
Snowflake Role Definitions

EDW Netezza ETL Access Recert
BCBSMA account receivable does not reconcile with the account payable amounts from the Federal Employee Program Directors Office
DAL is not included in current enterprise DRP or BCP

There are no systematic timestamps that are required when updating or quality-checking MyPBM pharmacy benefits, which may lead to benefit changes that are not quality-checked and ultimately inaccurate
BARs is not always used as source of truth for benefits due to known system and reporting limitations. Additionally, there is no direct QC of BAR's benefits which may to benefits that are configured but do not match the Sales and UW-approved benefits
Operations was not notified of an issue with accumulation rules feeds and had this occurred post 1/1/23, it could have led to inaccurate accumulation data being extracted from NASCO and sent to the PBM.

Observation 1: A sample of Medicare Secondary Payer (MSP) claims were not reprocessed by CVS on behalf of the New England Joint Enterprise (NEJE). NEJE disagrees with this observation.
Finding 1: MSLC asserts The Plan did not report DIR associated with pharmacy benefit manager (PBM) payments related to pharmacy contractual guaranteed rates for drug pricing for 2021. NEJE disagrees with this finding.
Finding 2: MSLC asserts The Plan did not report DIR associated with pharmacy benefit manager (PBM) payments related to pharmacy contractual guaranteed rates for drug pricing for 2021. NEJE disagrees with the finding.

The security policy doesn’t include specific elements required by HiTrust.
Bluetooth file sharing and peer to peer networking protocols are not disabled on workstations.
The policy for inventories of IT assets did not include specific information required by HiTrust.
BCBSMA does not have a review and approval process implemented for shared accounts explicitly.

Insufficient Data Validation Process During RIT Plan Record Keeper Transition from TELUS to Fidelity
It could not be determined that the amounts reported on Line 2 of the FEP Benefit Payable Confirmations for the quarters indicated are properly identified and supported.
FEP Contract Non-Compliance Due to Provider Recoupment Letters Not Sent
For one (1) of 27 changes sampled, approval not available

Lack of Quality Control for Group Measures Signed Post 12/1

* Issue Description
There is currently not a process or documented policy to monitor and address backup failures as of the date of our review for DAL and associated Postgres DBs in the AWS platform.
Based on an early review of all inbound faxes, it is believed that ~ 1-2% of total faxes received from 8/22/2022-2/17/2023 failed to enter the fax queue due to a code defect. Due to the delay in processing these faxes there is a potential of late authorization decisions. If the fax in the failed-fax folder is identified as a new request and the received date is prior to the received date for the case currently in the system, it could result in cases being decisioned past the due date.
For one (1) Salesforce PCMS new user sampled for the period, access was provisioned without the appropriate approval.

One Q4 2022 problem/incident ticket tested was not resolved within established service level timelines.
Corp Change Management area closes tickets as successful without verification if the ticket has been open over a certain time limit
For the Q1 2023 access review, one user was not included in the access review despite having access to ADP.
Two Salesforce Provider Contracting (PCMS) transferred users in Q1 2023 were not reviewed within 30 days of transfer. Control exceptions were also noted in 2022.

User access to the Tivoli Workload Scheduler and Avamar is performed annually to ensure access is restricted to authorized individuals. As part of the Avamar annual recertification, a user reviewed and recertified their own access.
Policy/Procedure: The policy and procedure documents do not include any information on user roles and responsibilities and determine whether the organization assigns risk designations to all organizational positions as appropriate and review and revise designations every 365 days.
Enterprise Data Warehouse (EDW) Cloudpak applicances (CP4D) do not have antivirus, firewalls, or file integrity monitoring software installed, as they are appliances.

Policy/Procedure/Implement:There is no direct policy and procedure documentation for blacklisting or the review and updating of the list of unauthorized (blacklisted) software periodically but no less than annually. Implement: BCBSMA does not maintain a list of unauthorized (blacklisted) software via software or tooling.
Policy/Procedure/Implement:There is no explicit policy or procedure which states that tools for maintenance are approved, controlled, monitored and periodically checked. No controls pertaining to preventative maintenance were tested in the DXC SOC 2.
Implement: Of the sampled changes, 0/25 (100%) of EDW changes had rollback procedures documented. Ref. BCBSMA 2023 Change Management Testing Table
Implement: Noted the technical vulnerability management program is evaluated on an annual basis. Baseline requires this to be quarterly.

Policy/Procedure/Implement:There is no document that specifically calls out reviewing historic audit logs to determine if high vulnerability scan findings identified in the information system have been previously exploitedAssessment team noted that the organization does not review historic audit logs to determine if high vulnerability scan findings identified in the information system have been previously exploited.
The following points are not covered in any of the BCBSMA Policy and Standard documents: The organization maintains a list of commonly-used, expected, or compromised passwords, and updates the list (i) at least every 180 days (ii) when organizational passwords are suspected to have been compromised (either directly or indirectly); employs automated tools to assist the user in selecting strong passwords and authenticators; and verifies, when users create or update passwords, that the passwords are not found on the organization-defined list of commonly-used, expected, or compromised passwords.
Implement: Only 1 account of 25 sampled had documented approval of use - there is not a process implemented to confirm authorized use of shared accounts.
Policy/Procedure/Implement:There is no policy to determine whether the organization provides incident response and contingency training to information systems users consistent with assigned roles and responsibilities: (ii) when required by information system changes. Implement: Additional training is not required due to information system changes
Policy/Procedure/Implement:There is no explicit policy or procedure to define that the organization ensures that the senior executives have been trained in their specific roles and responsibilities.Noted the organization does not provide specialized training for the senior executives in their specific roles and responsibilities within the organization outside of the scheduled tabletop exercises.

Implement: A specific specialized and formal role-specific training program does not exist beyond the annual compliance training.
(CAP52) Implement: The assessment team noted no formal training that workforce members are aware of how to properly respond to perimeter security alarms. (CAP59) Policy/Procedure/Implement:• There is no policy or procedure mandating that a duress alarm is provided whereby a person under duress can indicate such problems and responded to accordingly by the organization. Per inspection of the Markley SOC 2 report, the assessment team noted that the independent assessor did not test for the functioning of duress alarms in the facility. (CAP72) Implement: There is no control tested pertaining to the frequency at which physical access devices are inventoried from Markley and DXC. (CAP73) Implement: No controls pertaining to automated alarms for perimeter doors were tested in the Markley SOC 2. (CAP74) Implement: No controls pertaining to automated alarms for perimeter doors were tested in the Markley SOC 2. (CAP75) Implement: The Markley and DXC SOC2 reports do not explicitly identify a process for testing alarms. (CAP76) Implement: No controls pertaining to automated alarms for perimeter doors were tested in the Markley SOC 2. DXC does not test the logging of automated alarms. (CAP78) Policy/Procedure/Implement:There is no explicit policy or procedure stating that any security threats presented by neighboring premises are identified.No threats regarding neighboring premises were specifically identified.
Implement: Noted that the documentation around security engineering principles is not documented or implemented to the level required of this requirement statement for the following IPs: (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns, as well as compensating controls and design patterns needed to mitigate risk; and, (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions.

Implement: • No relevant procedures exist detailing the specific control responsibilities for developers of the information system. • The assessment team noted that the following were not formally defined in our sampled change: (i) a description of the functional properties of the security controls to be employed (ii) design and implementation information for the security controls to be employed that includes: security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces and high-level design documentation at sufficient detail to prove the security control implementation.
Implement: • No relevant procedures exist detailing the specific control responsibilities for developers of the information system. • The assessment team noted that the following were not formally defined in our sampled change: (i) a description of the functional properties of the security controls to be employed (ii) design and implementation information for the security controls to be employed that includes: security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces and high-level design documentation at sufficient detail to prove the security control implementation.
Implement: The DXC SOC2 does not have a dedicated control related to the repair or modification of the physical components of the facility
Implement: No controls pertaining to automated alarms notifying the authorities were tested in the DXC SOC 2.

Implement: There is no documented process for the (i.c) or (i.d) CSF elements. See baseline testing workplan.
Policy/Procedure/Implement:• The following points were not identified: i. Organization documents and maintains records (PII) that are subject to access by individuals. ii. Titles of the persons or office responsible for receiving and processing requests for access by individuals as organizational records for a period of six years.The assessment team noted that BCBSMA does not hold records that are subject to access by individuals and the titles of the persons or office responsible for receiving and processing requests for access by individuals as organizational records for a period of six years
(CAP71) Implement: No controls pertaining to automated alarms for doors to internal secure areas were tested in the DXCSOC 2. (CAP72) Implement: There is no control tested pertaining to the frequency at which physical access devices are inventoried from Markley and DXC. (CAP75) Implement: The Markley and DXC SOC2 reports do not explicitly identify a process for testing alarms. (CAP76) Implement: No controls pertaining to automated alarms for perimeter doors were tested in the Markley SOC 2. DXC does not test the logging of automated alarms. (CAP77) Implement: No controls pertaining to fire prevention training were tested in the Markley or DXC SOC 2s.
The reviewer of user access groups GG-ClaimOpsAdmin and GG-ClaimOpsPAM reviewed their own access in Q1 2023 recertification.

User Transfers and Access recertifications are not currently performed for Informatica console users.
ET does not currently have a centralized inventory of AD groups with Access to the DAL
For one (1) of 4 Solutions Development recertification users requested to be removed as part of the June 2023 recertification, access to the global group was not removed timely.

For two (2) of four (4) total DAL transferred users, the reviews of access following the users' transfer was not completed within 30 days of the transfer date. For one (1) of four (4) total DAL transferred users, the DAL access was not included in the review performed by the manager.
For one (1) of 13 users sampled where access was requested to be modified or removed as part of the Salesforce access recertification, access was not removed timely.
For three (3) AMS recertified users, a precise review was not performed.

For two (2) of 50 users sampled, one (1) manager delegated their review of their associates' access to the incorrect person.
For the Q3 recertification, 44 accounts with access to the DW, QEDM and DAL applications were not initially recertified as part of the Q3 review.
There is no direct policy in place mandating that changes to information assets, including systems, networks, and network services, are controlled and archived.
The reviewer of the GG-ClaimOpsAdmin and GG-ClaimOpsPAM groups has access to those global groups and as a result the reviewer reviewed their own access in Q4 2023 recertification.
For six (6) of 25 individuals, laptops were not recovered upon termination.
A formal quality control process is not in place for contracts with non-standard terms and where manual workarounds are needed for settlement calculations.

For three users with DW,QEDM and DAL access, their access was not recertified as part of the initial recertification process.
During Q4.23 Change management audit, IA could not find evidence of lower region testing for ServiceNow Prod ticket CHG0112950. IA was told IBM performed was responsible for the and it followed their standard change process. However, IA was not able to find any evidence of region progression.
21 accounts with Salesforce access (20 system accounts, 1 human account) were not included in the recertification.
One (1) of a total of 17 users were identified as having inappropriate access to the Edifecs production environment.

Six (6) Informatica service accounts and one (1) individual account were not initially reviewed as part of the Q1 2024 review.
For the period October 2023 - April 2024, 74 individuals with the ability to deploy DAL changes manually outside of the pipeline have development responsibilities, creating a segregation of duties concern.

Two (2) of 23 transferred users with access to FEP did not have their access reviewed timely.
IA recently requested for Tumbleweed servers to be included as part of quarterly patch testing beginning from Q2'24(for internal review only). IA identified that region progression was not followed on 2 packages affecting 3 Tumbleweed production servers namely bstep03vr,bstep04vr, and bstpp03vr.

For two (2) of 7 Salesforce Commerce transfer users sampled for the period, access review for Salesforce Commerce access was not reviewed.

For 1 out of 19 Critical Vendors, risks were identified as part of the assessment and were not remediated within the defined SLA.
For 1 of 4 users (100% of the population) that were provisioned temporary admin access, temporary admin access was not removed timely (within 30 days).
For 1 of 25 terminated users with badge access, the badge access was not suspended in a timely manner (30 days).
For 9 of 25 terminated users, the users' assets were not recovered by BCBSMA and the remote wipes, while initiated, were not completed.

System generated evidence of DAL patching was not available for the 2024 testing period.
For one (1) of 20 instances of new user access sampled during the period, the user's access was not granted in accordance with the approved new access request.
For the October 2024 Solutions Development monthly review performed, the review was not completed in a timely manner.
SBG found that NEJE achieved an overall dispensing fee performance overage across all distribution channels and networks, totaling $516,843, which was greater than CVSH's calculated overage of $399,395. Since the dispensing fee guarantees were exceeded, there is no amount due to NEJE. Variance caused by: There were some differences in the inclusion/exclusion methodology used by CVSH. The claims data used by SBG contained approximately 42,000 more claims that the data used by CVSH.

Data feeds to vendor Oral Eye were changed to include PHI/PII. This was not communicated to procurement. legal or info security at the time of change or at contract renewal.
During the review of the vendor Oral Eye's offshoring risks, several process gaps were identified including the lack of controls to detect unauthorized changes in data sharing arrangements with vendors.
Current logging only captures up to three (3) days of logs and isn't configured to log DBA/admin/priv account activity to the level of expectations by the InfoSec group. Since logging is not configured or maintained appropriately, the associated review cannot be performed on a periodic basis in accordance with the documented procedures
PwC identified 1,873 discrepant specialty claims that were not cleared in the initial inquiry to ESI. A sample of these claims have been sent to ESI for follow up research. The claims in question were filled at BCBSMA’s custom specialty pharmacies and were subject to a custom specialty guarantee. The total shortfall for these claims is $481,481.

During the PBM migration, member disruption letters were sent to the subscriber's address on file as opposed to the member's alternate address on file due to incorrect logic that was used on an MHK script. This incident has resulted in data breaches and HIPAA violations.
Since 2021 there has been a steady decline in MTM measures related to member and provider service (inquiry accuracy - manual, inquiry timeliness, and first call resolution). In 2022, the Plan's score hovered close to the 80 point threshold that requires further BCBS Association oversight.
Data Governance frameworks are not clearly understood across the enterprise, creating risk of data misuse and breaches. Privacy incidents continue to occur (12 incidents in last 18 months).

Implement: The assessment team obtained and inspected a sample of 25 change records from both EDW and RTMS. Of these changes, 16/25 (64%) of EDW changes were not appropriately tested. In addition, 1/25 (4%) of EDW and 1/25 (4%) of RTMS changes were approved by a qualified reviewer. In addition, 0/25 (0%) of EDW changes did have a risk analysis performed prior to implementation. Rollback analysis was not present on certain samples.
Ref. BCBSMA 2023 Change Management Testing Table

Policy/Procedure: the organization does not formally outline an approved application store for mobile devices accessing the in-scope systems.

Implement: The assessment team noted that the RTMS and EDW inventory did not include backup information, license information, business value, or portable/personal device.
Policy/Procedure/Implement:There is no direct policy identifying common vulnerabilities to the degree of specificity outlined in the illustrative procedures of the baseline.• Implement: There is no direct policy in place mandating that developed applications are based on secure coding guidelines to prevent common coding vulnerabilities in software development processes including but not limited to: i. injection flaws, particularly SQL injection. (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.); ii. buffer overflow (Validate buffer boundaries and truncate input strings) iii. insecure cryptographic storage (Prevent cryptographic flaws) iv. insecure communications (Properly encrypt all authenticated and sensitive communications); v. improper error handling (Do not leak information via error messages); vi. broken authentication/sessions (Prevent unauthorized individuals from compromising legitimate account credentials, keys or session tokens that would otherwise enable an intruder to assume the identify of an authorized user); vii. cross-site scripting (XSS), e.g., validate all parameters before inclusion, utilize context-sensitive escaping, etc.); viii. improper access control, such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access functions (e.g., properly authenticate users and sanitize input, and do not expose internal object references to users); ix. cross-site request forgery (CSRF), e.g., do not reply on authorization credentials and tokens automatically submitted by browsers; and x. any other input-validation vulnerability listed in the OWASP top 10. Applications that are not developed using secure coding guidelines undergo automatic or manual input validation checks during testing and annually thereafter, and such checks include: i. dual input or other input checks, such as boundary checking or limiting fields to specific ranges of input data, to detect the following errors: 1. out-of-range values 2. invalid characters in data fields 3. missing or incomplete data

Implement: There was no configuration shown to require immediate selection of a new password upon account recovery for the active directory.
Implement: The assessment team obtained a list of all group accounts (>250) with access to EDW and selected a sample of 25 shared group accounts and inspected 165_03282023_EDW Shared Group Accounts Sample to determine that 1/25 of the sampled shared/group accounts are reviewed of any requests and approved by the appropriate personnel.
Implement: The assessment team noted that privileged access reviews are not occurring every 60 days.
Implement: The GPO is not configured to close the network session after 30 minutes of inactivity.
Policy/Procedure/Implement:Policy documentation doesn't explicitly specify that the organization provides the listing of auditable events and supporting rationale are reviewed and updated periodically within 365 days.
Implement: The assessment team obtained and inspected a sample of 25 change records from both EDW and RTMS. Of these changes, 16/25 (64%) of EDW changes were not appropriately tested. In addition, 1/25 (4%) of EDW and 1/25 (4%) of RTMS changes were approved by a qualified reviewer. In addition, 0/25 (0%) of EDW changes did not have a risk analysis performed prior to implementation. In addition, of these changes, 0/25 (100%) of EDW changes had rollback procedures documented. Ref. BCBSMA 2023 Change Management Testing Table

The Change Advisory Board (CAB) may not review a solution before changes are approved, and risk determination of changes do not consider information security risks.
Lack of consistent implementation of access provisioning and deprovisioning controls: For two Active Directory (AD) groups reviewed, approximately 100 users were added without leader approval. In addition, an AD removal request was on hold for a month pending the leader's approval. Although the removal request was on hold, offshore vendor access was disabled timely as Palo Alto logs evidenced the firewall policy configuration was updated timely.
Lack of explicit and consistent AD group remote access management: 1). There is no periodic access review of users within AD groups; 2). Users were set up with both VPN and VDI access; and 3). BYOD users were observed with VPN access.
Associate Remote Access Standard does not have different information security risk considerations or requirements for onshore vs. offshore associates or contractors.

For two DAL (2) of 25 changes sampled, the same individual was both the change developer and the approver.

For the Q1 - Q3 2023 period, the completeness of the population of changes for the Data Access Layer (DAL) application from the ticketing system could not be validated for the period as evidence to reconcile the manually created tickets to the production source was not available which could result in an incomplete or inaccurate population. For the Q4 2023 period, the completeness of the population of manually deployed changes for the Data Access Layer (DAL), outside of the pipeline, could not be validated for the period as evidence to reconcile the manually created ticket to the production source was not available which could result in an incomplete or inaccurate population.

Update: For the Q4 2023 - Q1 2024 period, the completeness of the population of manually deployed changes for the Data Access Layer (DAL), outside of the pipeline, could not be validated for the period as evidence to reconcile the manually created ticket to the production source was not available which could result in an incomplete or inaccurate population.

There is insufficient vendor oversight relating to data sharing of participant data, creating risk of inaccurate financial reporting.

There is no formal process in place to ensure that QEDM is configured correctly to reflect the latest contract terms, especially when contracts are renegotiated or amended.

There was a finding in the FEP Overpayment Self-Assessment Pricing Update testing which uncovered a process gap. The update requested to terminate pricing for a provider in May 2023. The pricing was not updated until November 2023 upon request by Network Management. No one submitted a request to reprocess the claims which paid between May and November 2023 (aka a recovery request), so many claims were paying in-network when they should have been paying out-of-network.
For one (1) of 26 users sampled, access was not requested and approved at the application level.
For one user with BQ access, their BQ access role was not recertified as part of the initial recertification process. For one user with BQI access, their BQI access role was not recertified as part of the initial recertification process.
During the Commercial Claims Audit, the external auditors identified 7,551 claims that adjudicated below the per claim specialty AWP pricing guarantee. The shortfall amount estimated for these claims totals $2,865,379.
Service accounts with access to server operating systems are not certified on a recuring basis.

One (1) of XX users sampled was provisioned DAL production environment access without a documented request and approval for the production environment access.
Three (3) Ataccama service accounts were not reviewed as part of the Q1 2024 review.
1 account with BQI access was not included in the recertification.
AWS S3 buckets do not have sufficient reporting and archive data to support audit requirements.

Twelve (12) users were identified having access to both the pipeline admin role and the developer role for pipeline changes for the period through 6/20/2024.
Six (6) Abacus accounts were not included in the Q1 2024 review.

Incomplete IPE for change reporting. The evidence for completeness of the population of the Axway Tumbleweed (SFTP) WebApp changes could not be validated.
One Salesforce Commerce account was not included in the Q2 2024 review.
One (1) user whose access was requested to be removed was not removed as part of the Q2 2024 recertification.
1 user identified as part of the walkthrough sample did not have their access revoked timely as part of the Q1 2024 review.
Three (3) Ataccama accounts were not reviewed as part of the Q2 2024 review.

One (1) of XX users sampled was provisioned access to a BQ role that did not correspond to the role that was requested and approved.
SBG identified 417 claims that adjudicated below the per claim specialty AWP discounts with an estimated shortfall amount of $508,718.
One (1) of XX users sampled was provisioned Data Warehouse production environment access without a documented request and approval for the production environment access.
Accounts with access to DAL ADH S3 buckets are not certified for appropriateness on a recurring basis.
AWS Roles with the naming convention of 'RO' for 'Read-Only' have edit access to AWS assets.

During the review of transactions with affiliated Plan organizations, it was noted that the Plan allocated to FEP as administrative cost $11,723.00 for FERM Captive and there was no documentary evidence that profit was removed, or that the charges met all the terms of an exception that would allow the Plan to charge an amount greater than cost to the Program.

For 2 of 25 recertified users sampled from the Summer 2024 recertification, the access for the accounts was marked as appropriate by the application owner despite the accounts being inactive accounts.
For 5 of 25 vulnerabilities identified, the vulnerabilities were not resolved within the determined SLAs.
Patching evidence (i.e. patch reporting) is not retained for DAL AWS RDS
AWS OS security configurations are not reviewed to ensure alignment with BCBSMA policies and standards.

Currently, there is no formalized process to confirm that the authorized signer listing is complete and accurate for all banking institutions BCBSMA has a relationship. This was discovered in the MBA/Indigo review and applies to all bank relationships. Bank signatories are granted authority from each legal entity's governing body and the signatories on file at each bank are updated using bank specific documentation. Note that intercompany transfers from these entities are approved internally by Finance Management and processed via bank web portals by Cash Management associates. Bank signatories are needed to sign banking documents. However, this still may result in unauthorized individuals performing banking transactions, leading to potential fraud, or operational disruptions.

For nine (9) of 31 instances of transferred users' access sampled during the period, the users' access was not reviewed within 30 days.
Because ASCBE Errors were not worked in a timely manner, ASC billings and receivables may be inaccurate, incomplete, and untimely.

An automated process that retrieves Medical Loss Ratio (MLR) survey results from a third-party vendor failed to process one of the monthly update files, as the file received was in a non-standard format and didn't meet the agreed upon specifications. This prompted the need for manual intervention/error resolution where the appropriate steps were not followed, resulting in group size records not being updated in timely.
Rebate guarantees and discounts were calculated incorrectly by CVS Health due to a classification error relating to Retail90 claims. CVSH re-performed the calculations, which led to increases in the guaranteed rebates and discount amounts; however, since the actual amounts earned by BCBSMA were higher than the recalculated guaranteed amounts, there was no financial impact. SBG recommends that CVSH implement appropriate corrective measures to ensure that the correct Retail90 logic is applied to BCBSMA's pricing reconciliation and as well as the correct application of claim inclusion and exclusion.
Management has not documented existing change management processes across BCBSMA and determined future state controls to remediate root causes of 2023 audit findings communicated in Q4 2023. Management was engaging a vendor to assess in 2024/2025. New audit issues have occurred for MAR audit in 2024; no evidence to support testing prior to production for Blue Quote.
There is no inventory of Active Directory (AD) groups and their purposes, or periodic review of appropriateness of users in most AD groups. Lack of clarity over the purpose of certain groups has created issues with recertifying access of desktop administrators and created issues in which certain developers had inappropriate access in 2023 (SOC audit and offshore Palo Alto developer audit).

Observation: CVS requires up to 2 weeks to provision certain access, which can result in users being deleted by BCBSMA's automated weekly process to remove access if all requested access does not agree with access provisioned.
Leaders across BCBSMA do not always apply required level of rigor in responding to application access recertification requests.
DAL ODH changes could not be validated as complete, creating SOC 1 and SOC 2 audit issues in 2024.
There is currently no logging and monitoring of changes to Edifecs by system administrators.
Not all aspects of BCBSMA's cloud environment are included in BCBSMA's Disaster Recovery / Crisis Response Plans. Enterprise Technology continues to execute on the plan to include the remainder of the environment.
For the February 2025 Solutions Development monthly review, one user did not have their access reviewed timely and did not have their access removed timely (within the specified month).
MFA/2FA and VPN are not required for user authentication to the IICS application.
Data Access Layer Analytic Data Hub (ADH) does not have a Disaster Recovery or Business Continuity Plan in place which contemplates a potential multi-region failure. In the immediate term, the EDW may be used as a data source if DAL ADH is unavailable. The risk will increase if a plan isn’t implemented prior to the deprecation of the EDW.

Segregation of duties controls are not yet implemented in Salesforce instances. SOD is an area of increasing interest from external auditors, and an area with past issues from the 2024 audit (IICS, Edifecs). A recommendation was made in 2024 to revisit this across the ET organization.
Multi-Factor Authentication (MFA) and VPN are not required for user authentication to the IICS application.
SBG found that NEJE achieved an overall AWP discount performance overage across all distribution channels and networks, totaling $9,160,178. Although SBG's amount was significantly greater than CVSH's $7,994,741 calculation, both represent overall guarantee overages, therefore no amounts are due to NEJE. Variance caused by: CVSH applied an incorrect rate to Specialty Chain Preferred Claims (Rates are applied at the aggregate level, so no member liability impacts). The claims data used by SBG contained approximately 42,000 more claims that the data used by CVSH.
Based on the Agreement provided for the audit, SBG identified 4,937 specialty claims filled at network specialty pharmacies that did not achieve the guaranteed per-claim rates. SBG sent a sample of fifteen claims to CVSH to research the cause of the variance. CVSH responded that guaranteed rates were changed on May 1, 2023. CVSH was unable to provide any documentation to show the validity of the new rates as they made the adjustments to the contracted rates without notifying NEJE. SBG recommends that NEJE ensures that CVSH notify them in advance of any adjustments to contracted rates. CVSH did not provide a reconciliation for the overall effective specialty discount and dispensing fee performances at network pharmacies; however, SBG found that CVSH exceeded the contracted 21.25% discount rate and met the $0.00 dispensing fee guarantee.
SBG determined that no material package size violations occurred during the audit period. SBG identified eighteen claims where the package size did not align with the metric quantity dispensed. These errors may be attributed to pharmacist error at the point of sale. The monetary impact of these errors was immaterial, however SBG recommends that CVSH implements edits to ensure that the metric quantity aligns with the package size available for the given NDC.
Snowflake DAL role definitions are missing or incorrect.

Access re-certifications are not performed for EDW Netezza ETL ("Netezza Transformation")
From 2019 FEP CPR Audit Finding: FAM Volume 3, Chapter 3 – FEP Benefit Payable Confirmation, states, “On a quarterly basis, Plans must confirm the Plan’s general ledger receivable, and identify variances with the FEP Director’s Office Benefit Expenses Payable Account. The purpose of this reconciliation is to identify and categorize the variance between the Plan’s FEP benefits receivable balance and the FEP benefits payable balance recorded at the FEP Director’s Office. The FEP Benefit Payable Confirmation of Balances Statement of Procedures contains the following instructions for differences due to timing, “All amounts recorded as timing should reverse during the following quarter and not carry over to additional quarters. Plans should identify the amounts and reasons for their timing differences and provide documentation supporting these amounts.”
Application does not have a Disaster Recovery or Business Continuity Plan in place (migration to new AWS cloud hosting vendor completed May 2022).

MyPBM is a critical CVS system to manage and exchange benefits between BCBSMA and CVS. Identified through the PBM implementation engagement, IA notes that benefits within MyPBM can be edited after the original quality check upon entry. This may result in inaccurate benefit set-up and configuration.
This risk has been realized in the issue with PillarRx benefits per I#356 and I#357 , which notes that there is no QC or systematic reporting or QC regarding accounts and members which should have the Pillar Rx benefit.
As a part of the PBM engagement, IA notes that accumulation rules feeds are important for NASCO to know which accumulation information to extract and send to the PBM. Without proper notification and remediation, this could lead to inaccurate accumulation data being extracted from NASCO and sent to the PBM.

OHI (Other Health Insurance) information was received after the date of fill and after claims were processed for some members. The claims were not yet reprocessed with Medicare as the Secondary Payer as the retrospective gathering of information is required through confirmation and outreach from the beneficiary's other payer was still in process. CVS Caremark cannot reprocess the claims to correct the payer order without receiving the necessary information from the other payer. While this process may exceed beyond the date of annual PDE reconciliation, CVS Caremark previously triggered the outreach process to the other payers in following receipt of the COBC records and continues to send outreach to the other payers bimonthly to seek resolution of the claims. Of note, COBC records can be received for months after the applicable coverage, including beyond the PDE reconciliation date.
CMS Auditors (Myers and Stauffer) reviewed the contracts in place between the Plan and their downstream entities, and the contracts in place between the PBM and any of their downstream entities, for contractual provisions that may result in financial exchanges that qualify as DIR. This includes provisions in place between the PBM and the pharmacy that result in additional payments to or from the pharmacy that are not already included in the negotiated price of the drugs dispensed, as reported in the PDE data. The Plan did not report DIR associated with PBM payments related to pharmacy contractual guaranteed rates for drug pricing for 2021, as these payments are on a book of business level between CVS and pharmacies and do not change the cost to the Plan. The auditors assert that this should have been included as DIR.
CMS auditors (Myers and Stauffer) noted: As part of our procedures, we attempted to reconcile the total amounts of the Performance Network Rebates amounts down to the contract-PBP level. Per CVS Caremark, “The Plan decides which portions of its business will be participating in the PNR program. CVS does not decide this on behalf of the Plan. Currently, CVS tracks the following carriers as PNR-participants: 8580, 8582, 8584, 8586, 8588, 8590, 8592, and 8594. Understanding that not all these carriers conform to a contract-PBP that is under the scope of the audit.” The Plan is made up the following carriers: 8582, 8586, 8590, and 8594. As the PNR is collected for additional carriers aside from the Plan, we worked to verify the allocation from how the PNR is calculated, and how that amount flows to the amounts reported at the Contract-PBP level. CVS provided detail to support the amount of PNR that was reported at the Contract-PBP, but CVS did not provide sufficient information to reconcile the amount reported to the amount calculated at the overall collection amount for PNR.

Policy/Procedure: Policy does not note explicitly iv) the latest controls, compliance and assurance requirements and arrangements of national bodies and of new legislation or regulation; (v) the latest guidance and recommendations from professional associations and from information privacy commissioners regarding the protection of covered information; (vi) the results of legal cases tested in courts that thereby establish or cancel precedents and established practices. Implement: The assessment team noted that the results of legal cases are not explicitly considered in the development of the security policy.
Implement: Bluetooth file sharing was not disabled on workstations. We noted that the organization allows for the use of Bluetooth from computer peripherals but intends to lock down Bluetooth file sharing abilities in the future.
Policy/Procedure/Implement: • The assessment team noted that the policy does not talk about xii. operational status; xiii. primary and secondary administrators; and xiv. primary user.The assessment team noted that the RTMS inventory did not include backup information, license information, business value, or portable/personal device. The assessment team noted that "025_03162023_Endpoints Population" did not include: vi. presence of virtual machines vii. application software version/license information ix. logical location (e.g., IP address, position with the IS architecture) x. Media access control (MAC) address xii. operational status xiii. primary and secondary administrators
Implement: The assessment team obtained a list of all group accounts with access to EDW and selected a sample of 25 shared group accounts and inspected 165_03282023_EDW Shared Group Accounts Sample to determine that 1/25 of the sampled shared/group accounts are reviewed of any requests and approved by the appropriate personnel. It was noted that BCBSMA does not have a approval review process implemented for shared accounts explicitly.

On 1/1/24, the record-keeping responsibilities for the RIT plan transitioned from TELUS to Fidelity. As part of the transition, TELUS collaborated with Fidelity directly to ensure data migration was completed. However, there was no formalized, centralized process within BCBSMA to validate the accuracy and completeness of participant data transferred from TELUS to Fidelity. This lack of a validation process creates potential risks to the integrity of the RIT plan's data. Inaccuracies in participant demographics, account balances, elections and/or any other critical data elements may lead to participant and compliance issues, or errors in BCBSMA's financial reporting.
FAM Volume 3, Chapter 3 – FEP Benefit Payable Confirmation, states, "On a quarterly basis, Plans must confirm the Plan's general ledger receivable, and identify variances with the FEP Director's Office Benefit Expenses Payable Account. The purpose of this reconciliation is to identify and categorize the variance between the Plan's FEP benefits receivable balance and the FEP benefits payable balance recorded at the FEP Director's Office. The FEP Benefit Payable Confirmation of Balances Statement of Procedures contains the following instructions for differences due to timing, "All amounts recorded as timing should reverse during the following quarter and not carry over to additional quarters. Plans should identify the amounts and reasons for their timing differences and provide documentation supporting these amounts."
When FEP overpayments are recuperated by A/R offsets, BCBSMA does not send the FEP contractually required provider recoupment reminder letters at exactly 30, 60, and then 90 days. Instead, letters are not sent until around 45 days after A/R creation. Due to the greater level of scrutiny on contract adherence under new Office of Personnel Management (OPM) leadership, we are not in compliance with the contract.
For one (1) of 27 changes sampled, documented approval for the change prior to implementation was not available.

A formal quality control process is not in place to track Provider Organizations that signed their agreement after the 12/1 notices are sent. This notice provides the final measure set for performance determination for the following year, e.g. 12/1/24 notices provide the measure sets for the 2025 measurement period.

Test Section	Cycle	Entity	Process	Subprocess
	ITGC IT General Controls	COOIT Chief Operating Officer	LA Logical Access	LA.NEW New Access

	ITGC IT General Controls	CORPIT Corporate	SOC2 SOC 2	SOC2.SYSOPS System Operations
	ITGC IT General Controls	FINIT Finance	CM Change Management	CM.MIGR Migration Approval
	ITGC IT General Controls	HRIT Chief Human Resources	LA Logical Access	LA.RECERT Recertification of Access
	ITGC IT General Controls	COOIT Chief Operating Officer	LA Logical Access	LA.TRANS Transfer Access

	ITGC IT General Controls	CORPIT Corporate	SOC2 SOC 2	SOC2.PI Processing Integrity

	ITGC IT General Controls	ARMIT Audit & Risk Management	LA Logical Access	LA.RECERT Recertification of Access

	ITGC IT General Controls	COOIT Chief Operating Officer	LA Logical Access	LA.PRIV Privileged Access
	ITGC IT General Controls	ARMIT Audit & Risk Management	LA Logical Access	LA.RECERT Recertification of Access

	ITGC IT General Controls	COOIT Chief Operating Officer	LA Logical Access	LA.TRANS Transfer Access
	ITGC IT General Controls	COOIT Chief Operating Officer	LA Logical Access	LA.RECERT Recertification of Access
	ITGC IT General Controls	FINIT Finance	LA Logical Access	LA.RECERT Recertification of Access

	ITGC IT General Controls	ARMIT Audit & Risk Management	LA Logical Access	LA.RECERT Recertification of Access
	ITGC IT General Controls	ARMIT Audit & Risk Management	LA Logical Access	LA.RECERT Recertification of Access
	ITGC IT General Controls	CORPIT Corporate	SOC2 SOC 2	SOC2.ACC Access and Security

	ITGC IT General Controls	ARMIT Audit & Risk Management	LA Logical Access	LA.RECERT Recertification of Access
	ITGC IT General Controls	SALESIT Sales, Marketing, & Product	LA Logical Access	LA.RECERT Recertification of Access
	ITGC IT General Controls	COOIT Chief Operating Officer	CM Change Management	CM.SoD Segregation of Duties

	ITGC IT General Controls	COOIT Chief Operating Officer	LA Logical Access	LA.PRIV Privileged Access
	ITGC IT General Controls	FINIT Finance	CM Change Management	CM.SoD Segregation of Duties

	ITGC IT General Controls	COOIT Chief Operating Officer	LA Logical Access	LA.TRANS Transfer Access
Walkthrough	ITGC IT General Controls	COOIT Chief Operating Officer	CM Change Management	CM.TEST Testing

	ITGC IT General Controls	ARMIT Audit & Risk Management	LA Logical Access	LA.TRANS Transfer Access

	ITGC IT General Controls	CORPIT Corporate	SOC2 SOC 2	SOC2.ORG Organization and Mgmt
	ITGC IT General Controls	ARMIT Audit & Risk Management	LA Logical Access	LA.NEW New Access
	ITGC IT General Controls	CORPIT Corporate	SOC2 SOC 2	SOC2.ACC Access and Security
	ITGC IT General Controls	CORPIT Corporate	SOC2 SOC 2	SOC2.ACC Access and Security

	ITGC IT General Controls	COOIT Chief Operating Officer	CM Change Management	CM.TEST Testing
	ITGC IT General Controls	SALESIT Sales, Marketing, & Product	LA Logical Access	LA.NEW New Access
	ITGC IT General Controls	ARMIT Audit & Risk Management	LA Logical Access	LA.RECERT Recertification of Access

	ITGC IT General Controls	COOIT Chief Operating Officer	CM Change Management	CM.SoD Segregation of Duties

	ITGC IT General Controls	COOIT Chief Operating Officer	CM Change Management	CM.POL Policy or Methodology

	ITGC IT General Controls	ARMIT Audit & Risk Management	LA Logical Access	LA.NEW New Access
	ITGC IT General Controls	ARMIT Audit & Risk Management	LA Logical Access	LA.RECERT Recertification of Access
	ITGC IT General Controls	COOIT Chief Operating Officer	LA Logical Access	LA.PRIV Privileged Access

	ITGC IT General Controls	ARMIT Audit & Risk Management	LA Logical Access	LA.NEW New Access
	ITGC IT General Controls	COOIT Chief Operating Officer	LA Logical Access	LA.PRIV Privileged Access
	ITGC IT General Controls	SALESIT Sales, Marketing, & Product	LA Logical Access	LA.RECERT Recertification of Access
	ITGC IT General Controls	COOIT Chief Operating Officer	CM Change Management	CM.POL Policy or Methodology

	ITGC IT General Controls	FINIT Finance	CM Change Management	CM.SoD Segregation of Duties
	ITGC IT General Controls	COOIT Chief Operating Officer	LA Logical Access	LA.PRIV Privileged Access

	ITGC IT General Controls	COOIT Chief Operating Officer	CM Change Management	CM.REQS Requirements and Approval
	ITGC IT General Controls	ARMIT Audit & Risk Management	LA Logical Access	LA.RECERT Recertification of Access
	ITGC IT General Controls	ARMIT Audit & Risk Management	LA Logical Access	LA.RECERT Recertification of Access
Walkthrough	ITGC IT General Controls	ARMIT Audit & Risk Management	LA Logical Access	LA.RECERT Recertification of Access
	ITGC IT General Controls	COOIT Chief Operating Officer	LA Logical Access	LA.PRIV Privileged Access

	ITGC IT General Controls	ARMIT Audit & Risk Management	LA Logical Access	LA.NEW New Access
	ITGC IT General Controls	ARMIT Audit & Risk Management	LA Logical Access	LA.NEW New Access
	ITGC IT General Controls	COOIT Chief Operating Officer	LA Logical Access	LA.PRIV Privileged Access

	ITGC IT General Controls	ARMIT Audit & Risk Management	LA Logical Access	LA.RECERT Recertification of Access
	ITGC IT General Controls	CORPIT Corporate	SOC2 SOC 2	SOC2.ERM Risk Mgmt
	ITGC IT General Controls	COOIT Chief Operating Officer	CM Change Management	CM.TEST Testing
	ITGC IT General Controls	CORPIT Corporate	SOC2 SOC 2	SOC2.CTRL Control Activities

	ITGC IT General Controls	COOIT Chief Operating Officer	LA Logical Access	LA.TRANS Transfer Access
Walkthrough	BP Business Process	FIN Finance	ASC ASC BILLING	ASC.ASC ASC BILLING

	ITGC IT General Controls	CORPIT Corporate	SOC2 SOC 2	SOC2.ACC Access and Security

	ITGC IT General Controls	ARMIT Audit & Risk Management	LA Logical Access	LA.RECERT Recertification of Access

	ITGC IT General Controls	FINIT Finance	CM Change Management	CM.MIGR Migration Approval

	BP Business Process	COO Chief Operating Officer	AQC AQC PAYMENTS /SETTLEMENTS	AQC.AQC AQC PAYMENTS /SETTLEMENTS

UID	Category	Audit Title
67	Operations	DAL Operational Readiness Assessment

124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023

124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023

124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023

124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023

124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023

124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023

124	Security	HITRUST CAPS 2023

249	Compliance	PBM Claims, Rebates, Mail Order - 2023 NEJE

81	Security	Data Offshoring (Oral Eye)
81	Security	Data Offshoring (Oral Eye)
67	Operations	DAL Operational Readiness Assessment
CRC21	Operations	PBM Claims, Rebates, Mail Order - 2021 Commercial

119	Operations	Member Rights Database (Alternate Addresses)

124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023

124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023

124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023

130	Security	Palo Alto / Offshore Contractor Remote Access
130	Security	Palo Alto / Offshore Contractor Remote Access
130	Security	Palo Alto / Offshore Contractor Remote Access
130	Security	Palo Alto / Offshore Contractor Remote Access

FEPO23	Compliance	FEP Overpayment Self Assessment (2023)
CRC22	Operations	PBM Claims, Rebates, Mail Order - 2022 Commercial

178	Compliance	PBM Claims, Rebates, Mail Order - MAPD 2022

164	Operations	2024 FEP Control Performance Review (CPR)

246	Compliance	PBM Claims, Rebates, Mail Order - 2023 MAPD

249	Compliance	PBM Claims, Rebates, Mail Order - 2023 NEJE
249	Compliance	PBM Claims, Rebates, Mail Order - 2023 NEJE
249	Compliance	PBM Claims, Rebates, Mail Order - 2023 NEJE

16	Operations	FEP IPA 2021
67	Operations	DAL Operational Readiness Assessment

45	Operations	Pharmacy Benefit Manager (PBM) Implementation (1.1.23)
45	Operations	Pharmacy Benefit Manager (PBM) Implementation (1.1.23)
45	Operations	Pharmacy Benefit Manager (PBM) Implementation (1.1.23)

114	Operations	CMS Financial Audit S2893-801
114	Operations	CMS Financial Audit S2893-801
114	Operations	CMS Financial Audit S2893-801

124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023
124	Security	HITRUST CAPS 2023

164	Operations	2024 FEP Control Performance Review (CPR)
FEPO24	Compliance	FEP Overpayment Self Assessment (2024)

Work Step	Status (Work Step)	Control
Backup error monitoring and resolution	Complete	
		COOIT.LA.NEW.LA6.06 New Access Request_Salesforce Provider Ops Access to BCBSMA LAN and application data is approved by the associate's leader. The Security Administrators work with the business leaders to validate the access request and ensure that the application access is in accordance with job responsibilities, and that the request is authorized by the leader (includes Privilege Access).

		CORPIT.SOC2.SYSOPS.CC7.3_02 System Issue/Incident Tracking A system issue or incident affecting multiple users (five or more) is entered, tracked, researched, and resolved in a help desk ticket using a system-generated tracking number. Incidents that cannot be resolved immediately are escalated according to limits defined in the Service Level Agreement (SLA) and, if appropriate, workarounds are provided.
		FINIT.CM.MIGR.CM05.01 Leader Approval_Finance Business or ET leaders approve changes prior to the program being placed into production.
		HRIT.LA.RECERT.LA3.08 Access Recert_ADP Access is recertified on a quarterly basis for all users.
		COOIT.LA.TRANS.LA4.06 Transferred User Access_Salesforce Provider Ops [Deprecated - Control to be deleted] Application access is revalidated by security administration upon an associates job transfer.

		CORPIT.SOC2.PI.PI1.3_01 Tivoli Workload Scheduler Access Access to modify batch and backup schedules in the Tivoli Workload Scheduler and Avamar is restricted to authorized individuals and is revalidated on an annual basis.
CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	

CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	

CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	

CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	

CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	

CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	
		ARMIT.LA.RECERT.LA3.01 Access Recert_IAM For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.

		COOIT.LA.PRIV.LA2.01 Privileged Access Recert_SD DB Privileged access to servers and databases is revalidated on a periodic basis to determine whether continued access is appropriate: - On premise servers and databases: quarterly - DAL servers and databases: at least annually
		ARMIT.LA.RECERT.LA3.01 Access Recert_IAM For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.

		COOIT.LA.TRANS.LA4.03 Transferred User Access_Enterprise Technology Application access is revalidated by security administration upon an associate's job transfer.
		COOIT.LA.RECERT.LA3.06 Access Recert_Salesforce Provider Ops For the key business applications, the IAM Team and Security Administrators, with the assistance of business leaders, revalidate access levels for end users on at least an annual basis.
		FINIT.LA.RECERT.LA3.02 Access Recert_BARS_AMS For the key business applications, the IAM Team and Security Administrators, with the assistance of business leaders, revalidate access levels for end users on at least an annual basis.

		ARMIT.LA.RECERT.LA3.01 Access Recert_IAM For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.
		ARMIT.LA.RECERT.LA3.01 Access Recert_IAM For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.
CAPS and Workplan (Scoring Results) for 2023	Open	
		CORPIT.SOC2.ACC.CC6.4_03 Laptop Retrieval The company recovers physical devices upon the employee/contractor termination process. For cases in which physical devices cannot be recovered, network administrators remotely delete data from the device.

		ARMIT.LA.RECERT.LA3.01 Access Recert_IAM For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.
		SALESIT.LA.RECERT.LA3.05 Access Recert_BQ/BQi/SF For the key business applications, the IAM Team and Security Administrators, with the assistance of business leaders, revalidate access levels for end users on at least an annual basis.
		COOIT.CM.SoD.CM03.02 Change Monitoring and SoD_ Enterprise Technology The Company has established change management monitoring and segregation of duties controls over changes made in the production environments.

		COOIT.LA.PRIV.LA2.01 Privileged Access Recert_SD DB Privileged access to servers and databases is revalidated on a periodic basis to determine whether continued access is appropriate: - On premise servers and databases: quarterly - DAL servers and databases: at least annually
		FINIT.CM.SoD.CM03.01 Change Monitoring and SoD_ Finance The Company has established change management monitoring and segregation of duties controls over changes made in the production environments.

		COOIT.LA.TRANS.LA4.03 Transferred User Access_Enterprise Technology Application access is revalidated by security administration upon an associate's job transfer.
		COOIT.CM.TEST.CM04.02 Tested Before Prod_Enterprise Technology Program changes are tested before being placed into production.

		ARMIT.LA.TRANS.LA4.01 Transferred User Access_IAM Application access is revalidated by security administration upon an associate’s job transfer.

		CORPIT.SOC2.ORG.CC1.4_02 Annual Vendor Review Critical vendors are reviewed on an annual basis.
		ARMIT.LA.NEW.LA6.01 New Access Request_IAM Access to BCBSMA LAN and application data is approved by the associate's leader. The Security Administrators work with the business leaders to validate the access request and ensure that the application access is in accordance with job responsibilities, and that the request is authorized by the leader.
		CORPIT.SOC2.ACC.CC6.4_01 Daily Phys Term from TIM/TAM Daily Workday Email and TIM/TAM Report
		CORPIT.SOC2.ACC.CC6.4_03 Laptop Retrieval The company recovers physical devices upon the employee/contractor termination process. For cases in which physical devices cannot be recovered, network administrators remotely delete data from the device.

		COOIT.CM.TEST.CM04.04 Patch Testing System patch changes are tested before being placed into production.
		SALESIT.LA.NEW.LA6.04 New Access Request_BQ/BQi/SF All new access is requested and approved prior to being granted.
		ARMIT.LA.RECERT.LA3.01 Access Recert_IAM For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.
Claims Findings	Open	

The vendor intake and review process was completed in line with the process and accurately.	Complete	
BCBSMA data is maintained onshore and is not accessible to offshore resources without appropriate technical controls to prevent access and/or downloading of BCBSMA data.	Open	
Administrator/Priv Access Monitoring	Open	
Review Findings	Reviewed	

Narrative, Flowchart, Meeting Notes	Open	

CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	

CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	

CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	

Engagement Summary	Reviewed	
Engagement Summary	Reviewed	
Engagement Summary	Reviewed	
Engagement Summary	Reviewed	

		COOIT.CM.SoD.CM03.02 Change Monitoring and SoD_ Enterprise Technology The Company has established change management monitoring and segregation of duties controls over changes made in the production environments.

		COOIT.CM.POL.CM01.02 Program Change Policy/Methodology_Enterprise Technology Program changes follow an established process, policy, or methodology for documenting system change: - Change Request Form - Test Plan - User Acceptance and Manager Approval - Production Control Staging

Test Samples	Complete	
		ARMIT.LA.NEW.LA6.01 New Access Request_IAM Access to BCBSMA LAN and application data is approved by the associate's leader. The Security Administrators work with the business leaders to validate the access request and ensure that the application access is in accordance with job responsibilities, and that the request is authorized by the leader.
		ARMIT.LA.RECERT.LA3.01 Access Recert_IAM For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.
Review Findings	Open	
		COOIT.LA.PRIV.LA2.01 Privileged Access Recert_SD DB Privileged access to servers and databases is revalidated on a periodic basis to determine whether continued access is appropriate: - On premise servers and databases: quarterly - DAL servers and databases: at least annually

		ARMIT.LA.NEW.LA6.01 New Access Request_IAM Access to BCBSMA LAN and application data is approved by the associate's leader. The Security Administrators work with the business leaders to validate the access request and ensure that the application access is in accordance with job responsibilities, and that the request is authorized by the leader.
		COOIT.LA.PRIV.LA2.01 Privileged Access Recert_SD DB Privileged access to servers and databases is revalidated on a periodic basis to determine whether continued access is appropriate: - On premise servers and databases: quarterly - DAL servers and databases: at least annually
		SALESIT.LA.RECERT.LA3.05 Access Recert_BQ/BQi/SF For the key business applications, the IAM Team and Security Administrators, with the assistance of business leaders, revalidate access levels for end users on at least an annual basis.
		COOIT.CM.POL.CM01.02 Program Change Policy/Methodology_Enterprise Technology Program changes follow an established process, policy, or methodology for documenting system change: - Change Request Form - Test Plan - User Acceptance and Manager Approval - Production Control Staging

		FINIT.CM.SoD.CM03.01 Change Monitoring and SoD_ Finance The Company has established change management monitoring and segregation of duties controls over changes made in the production environments.
		COOIT.LA.PRIV.LA2.01 Privileged Access Recert_SD DB Privileged access to servers and databases is revalidated on a periodic basis to determine whether continued access is appropriate: - On premise servers and databases: quarterly - DAL servers and databases: at least annually

		COOIT.CM.REQS.CM02.02 Change Approvals_Enterprise Technology Appropriate business or ET area management approves any new or modified program change requests before work is initiated.
		ARMIT.LA.RECERT.LA3.01 Access Recert_IAM For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.
		ARMIT.LA.RECERT.PBM.IT.LA.03 Access Recertification (CVS Systems) For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, revalidate access levels for end users on at least an annual basis.
		ARMIT.LA.RECERT.LA3.01 Access Recert_IAM For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.
		COOIT.LA.PRIV.LA2.01 Privileged Access Recert_SD DB Privileged access to servers and databases is revalidated on a periodic basis to determine whether continued access is appropriate: - On premise servers and databases: quarterly - DAL servers and databases: at least annually

		ARMIT.LA.NEW.LA6.01 New Access Request_IAM Access to BCBSMA LAN and application data is approved by the associate's leader. The Security Administrators work with the business leaders to validate the access request and ensure that the application access is in accordance with job responsibilities, and that the request is authorized by the leader.
Claims Findings	Open	
		ARMIT.LA.NEW.LA6.01 New Access Request_IAM Access to BCBSMA LAN and application data is approved by the associate's leader. The Security Administrators work with the business leaders to validate the access request and ensure that the application access is in accordance with job responsibilities, and that the request is authorized by the leader.
		COOIT.LA.PRIV.LA2.01 Privileged Access Recert_SD DB Privileged access to servers and databases is revalidated on a periodic basis to determine whether continued access is appropriate: - On premise servers and databases: quarterly - DAL servers and databases: at least annually

IR#22 Admin - Services Acquired from Plan Organizations	Under Review (R)	

		ARMIT.LA.RECERT.LA3.01 Access Recert_IAM For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.
		CORPIT.SOC2.ERM.CC3.2_05 Internal Vulnerability Scanning BCBSMA performs Internal Vulnerability scanning on a weekly basis.
		COOIT.CM.TEST.CM04.04 Patch Testing System patch changes are tested before being placed into production.
		CORPIT.SOC2.CTRL.CC5.3_01 OS Security Configuration Mid-tier operating system security configuration settings are controlled via quarterly automated scripts that are run against Company Security Policy and Standards. All results are reviewed by IT Infrastructure Management.

		COOIT.LA.TRANS.LA4.03 Transferred User Access_Enterprise Technology Application access is revalidated by security administration upon an associate's job transfer.
		FIN.ASC.ASC.ASC.KC.12 ASCBE Error Control claim errors generated from Oracle during the ASC billing process are investigated and claims errors are researched and resolved on a timely basis.

Rebates Findings	Open	

		CORPIT.SOC2.ACC.CC6.1_06 MFA External access by BCBSMA employees and contractors is restricted to methods that require two-factor authentication.

Claims Findings	Open	
Claims Findings	Open	
Claims Findings	Open	

		ARMIT.LA.RECERT.LA3.01 Access Recert_IAM For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.
Issue	Open	
DRP and BCP	Complete	

Flowchart(s)	Reviewed	
Flowchart(s)	Reviewed	
Narrative	Reviewed	

Issues	Open	
Issues	Open	
Issues	Open	

CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	
CAPS and Workplan (Scoring Results) for 2023	Open	

IR#8 Cash Management Benefits Payable	Open	
C.1 SWCR and UCM Recovery Testing	Complete	
		FINIT.CM.MIGR.CM05.01 Leader Approval_Finance Business or ET leaders approve changes prior to the program being placed into production.

		COO.AQC.AQC.AQC.KC.02 AQC Settlement Quality A Quality Control program validates the completeness and accuracy of AQC Actuarial projections. Management maintains evidence that Quality control was performed. (PEER REVIEW)

Control UID	Title (Control)	Description
COOIT.LA.NEW.LA6.06	New Access Request_Salesforce Provider Ops	Access to BCBSMA LAN and application data is approved by the associate's leader. The Security Administrators work with the business leaders to validate the access request and ensure that the application access is in accordance with job responsibilities, and that the request is authorized by the leader (includes Privilege Access).

CORPIT.SOC2.SYSOPS.CC 7.3_02	System Issue/Incident Tracking	A system issue or incident affecting multiple users (five or more) is entered, tracked, researched, and resolved in a help desk ticket using a system-generated tracking number. Incidents that cannot be resolved immediately are escalated according to limits defined in the Service Level Agreement (SLA) and, if appropriate, workarounds are provided.
FINIT.CM.MIGR.CM05.01	Leader Approval_Finance	Business or ET leaders approve changes prior to the program being placed into production.
HRIT.LA.RECERT.LA3.08	Access Recert_ADP	Access is recertified on a quarterly basis for all users.
COOIT.LA.TRANS.LA4.06	Transferred User Access_Salesforce Provider Ops	[Deprecated - Control to be deleted] Application access is revalidated by security administration upon an associates job transfer.

CORPIT.SOC2.PI.PI1.3_01	Tivoli Workload Scheduler Access	Access to modify batch and backup schedules in the Tivoli Workload Scheduler and Avamar is restricted to authorized individuals and is revalidated on an annual basis.

ARMIT.LA.RECERT.LA3.01	Access Recert_IAM	For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.

COOIT.LA.PRIV.LA2.01	Privileged Access Recert_SD DB	Privileged access to servers and databases is revalidated on a periodic basis to determine whether continued access is appropriate: - On premise servers and databases: quarterly - DAL servers and databases: at least annually
ARMIT.LA.RECERT.LA3.01	Access Recert_IAM	For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.

COOIT.LA.TRANS.LA4.03	Transferred User Access_Enterprise Technology	Application access is revalidated by security administration upon an associate's job transfer.
COOIT.LA.RECERT.LA3.06	Access Recert_Salesforce Provider Ops	For the key business applications, the IAM Team and Security Administrators, with the assistance of business leaders, revalidate access levels for end users on at least an annual basis.
FINIT.LA.RECERT.LA3.02	Access Recert_BARS_AMS	For the key business applications, the IAM Team and Security Administrators, with the assistance of business leaders, revalidate access levels for end users on at least an annual basis.

ARMIT.LA.RECERT.LA3.01	Access Recert_IAM	For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.
ARMIT.LA.RECERT.LA3.01	Access Recert_IAM	For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.
CORPIT.SOC2.ACC.CC6.4_03	Laptop Retrieval	The company recovers physical devices upon the employee/contractor termination process. For cases in which physical devices cannot be recovered, network administrators remotely delete data from the device.

ARMIT.LA.RECERT.LA3.01	Access Recert_IAM	For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.
SALESIT.LA.RECERT.LA3.05	Access Recert_BQ/BQi/SF	For the key business applications, the IAM Team and Security Administrators, with the assistance of business leaders, revalidate access levels for end users on at least an annual basis.
COOIT.CM.SoD.CM03.02	Change Monitoring and SoD_ Enterprise Technology	The Company has established change management monitoring and segregation of duties controls over changes made in the production environments.

COOIT.LA.PRIV.LA2.01	Privileged Access Recert_SD DB	Privileged access to servers and databases is revalidated on a periodic basis to determine whether continued access is appropriate: - On premise servers and databases: quarterly - DAL servers and databases: at least annually
FINIT.CM.SoD.CM03.01	Change Monitoring and SoD_ Finance	The Company has established change management monitoring and segregation of duties controls over changes made in the production environments.

COOIT.LA.TRANS.LA4.03	Transferred User Access_Enterprise Technology	Application access is revalidated by security administration upon an associate's job transfer.
COOIT.CM.TEST.CM04.02	Tested Before Prod_Enterprise Technology	Program changes are tested before being placed into production.

ARMIT.LA.TRANS.LA4.01	Transferred User Access_IAM	Application access is revalidated by security administration upon an associate's job transfer.

CORPIT.SOC2.ORG.CC1.4_02	Annual Vendor Review	Critical vendors are reviewed on an annual basis.
ARMIT.LA.NEW.LA6.01	New Access Request_IAM	Access to BCBSMA LAN and application data is approved by the associate's leader. The Security Administrators work with the business leaders to validate the access request and ensure that the application access is in accordance with job responsibilities, and that the request is authorized by the leader.
CORPIT.SOC2.ACC.CC6.4_01	Daily Phys Term from TIM/TAM	Daily Workday Email and TIM/TAM Report
CORPIT.SOC2.ACC.CC6.4_03	Laptop Retrieval	The company recovers physical devices upon the employee/contractor termination process. For cases in which physical devices cannot be recovered, network administrators remotely delete data from the device.

COOIT.CM.TEST.CM04.04	Patch Testing	System patch changes are tested before being placed into production.
SALESIT.LA.NEW.LA6.04	New Access Request_BQ/BQi/SF	All new access is requested and approved prior to being granted.
ARMIT.LA.RECERT.LA3.01	Access Recert_IAM	For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.

COOIT.CM.SoD.CM03.02	Change Monitoring and SoD_ Enterprise Technology	The Company has established change management monitoring and segregation of duties controls over changes made in the production environments.

COOIT.CM.POL.CM01.02	Program Change Policy/Methodology_Enterprise Technology	Program changes follow an established process, policy, or methodology for documenting system change: - Change Request Form - Test Plan - User Acceptance and Manager Approval - Production Control Staging

ARMIT.LA.NEW.LA6.01	New Access Request_IAM	Access to BCBSMA LAN and application data is approved by the associate's leader. The Security Administrators work with the business leaders to validate the access request and ensure that the application access is in accordance with job responsibilities, and that the request is authorized by the leader.
ARMIT.LA.RECERT.LA3.01	Access Recert_IAM	For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.
COOIT.LA.PRIV.LA2.01	Privileged Access Recert_SD DB	Privileged access to servers and databases is revalidated on a periodic basis to determine whether continued access is appropriate: - On premise servers and databases: quarterly - DAL servers and databases: at least annually

ARMIT.LA.NEW.LA6.01	New Access Request_IAM	Access to BCBSMA LAN and application data is approved by the associate's leader. The Security Administrators work with the business leaders to validate the access request and ensure that the application access is in accordance with job responsibilities, and that the request is authorized by the leader.
COOIT.LA.PRIV.LA2.01	Privileged Access Recert_SD DB	Privileged access to servers and databases is revalidated on a periodic basis to determine whether continued access is appropriate: - On premise servers and databases: quarterly - DAL servers and databases: at least annually
SALESIT.LA.RECERT.LA3.05	Access Recert_BQ/BQi/SF	For the key business applications, the IAM Team and Security Administrators, with the assistance of business leaders, revalidate access levels for end users on at least an annual basis.
COOIT.CM.POL.CM01.02	Program Change Policy/Methodology_Enterprise Technology	Program changes follow an established process, policy, or methodology for documenting system change: - Change Request Form - Test Plan - User Acceptance and Manager Approval - Production Control Staging

FINIT.CM.SoD.CM03.01	Change Monitoring and SoD_ Finance	The Company has established change management monitoring and segregation of duties controls over changes made in the production environments.
COOIT.LA.PRIV.LA2.01	Privileged Access Recert_SD DB	Privileged access to servers and databases is revalidated on a periodic basis to determine whether continued access is appropriate: - On premise servers and databases: quarterly - DAL servers and databases: at least annually

COOIT.CM.REQS.CM02.02	Change Approvals_Enterprise Technology	Appropriate business or ET area management approves any new or modified program change requests before work is initiated.
ARMIT.LA.RECERT.LA3.01	Access Recert_IAM	For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.
ARMIT.LA.RECERT.PBM.IT.LA.03	Access Recertification (CVS Systems)	For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, revalidate access levels for end users on at least an annual basis.
ARMIT.LA.RECERT.LA3.01	Access Recert_IAM	For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.
COOIT.LA.PRIV.LA2.01	Privileged Access Recert_SD DB	Privileged access to servers and databases is revalidated on a periodic basis to determine whether continued access is appropriate: - On premise servers and databases: quarterly - DAL servers and databases: at least annually

ARMIT.LA.NEW.LA6.01	New Access Request_IAM	Access to BCBSMA LAN and application data is approved by the associate's leader. The Security Administrators work with the business leaders to validate the access request and ensure that the application access is in accordance with job responsibilities, and that the request is authorized by the leader.
ARMIT.LA.NEW.LA6.01	New Access Request_IAM	Access to BCBSMA LAN and application data is approved by the associate's leader. The Security Administrators work with the business leaders to validate the access request and ensure that the application access is in accordance with job responsibilities, and that the request is authorized by the leader.
COOIT.LA.PRIV.LA2.01	Privileged Access Recert_SD DB	Privileged access to servers and databases is revalidated on a periodic basis to determine whether continued access is appropriate: - On premise servers and databases: quarterly - DAL servers and databases: at least annually

ARMIT.LA.RECERT.LA3.01	Access Recert_IAM	For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.
CORPIT.SOC2.ERM.CC3.2_05	Internal Vulnerability Scanning	BCBSMA performs Internal Vulnerability scanning on a weekly basis.
COOIT.CM.TEST.CM04.04	Patch Testing	System patch changes are tested before being placed into production.
CORPIT.SOC2.CTRL.CC5.3_01	OS Security Configuration	Mid-tier operating system security configuration settings are controlled via quarterly automated scripts that are run against Company Security Policy and Standards. All results are reviewed by IT Infrastructure Management.

COOIT.LA.TRANS.LA4.03	Transferred User Access_Enterprise Technology	Application access is revalidated by security administration upon an associate's job transfer.
FIN.ASC.ASC.ASC.KC.12	ASCBE Error Control	claim errors generated from Oracle during the ASC billing process are investigated and claims errors are researched and resolved on a timely basis.

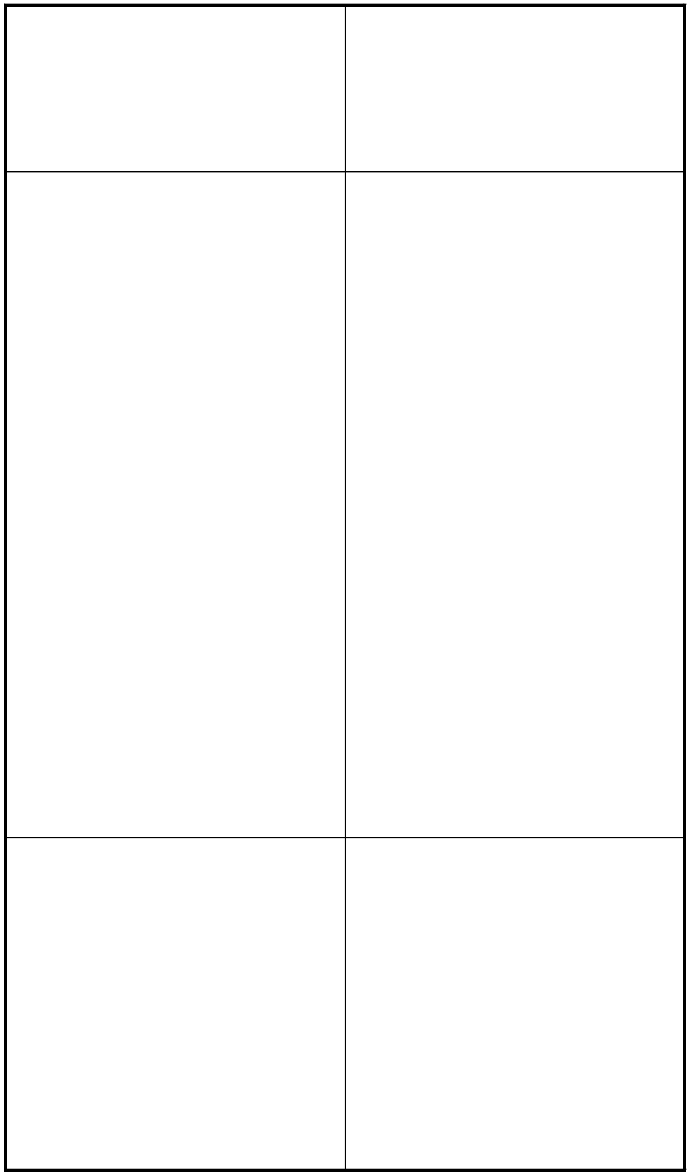
CORPIT.SOC2.ACC.CC6.1_06	MFA	External access by BCBSMA employees and contractors is restricted to methods that require two-factor authentication.

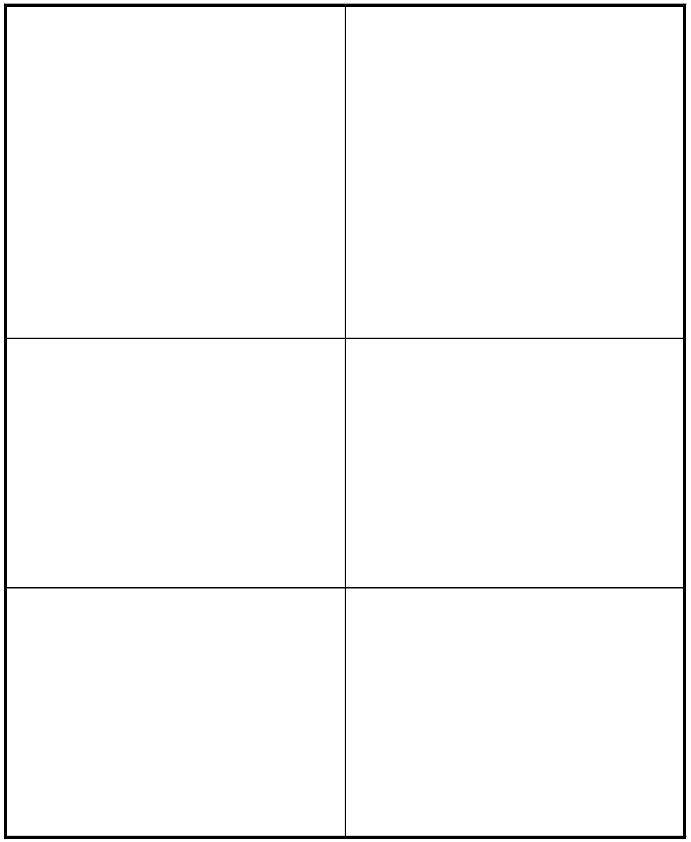
ARMIT.LA.RECERT.LA3.01	Access Recert_IAM	For the key business applications, the IAM team and Security Administrators, with the assistance of business leaders, re-validate access levels for end users on at least an annual basis.

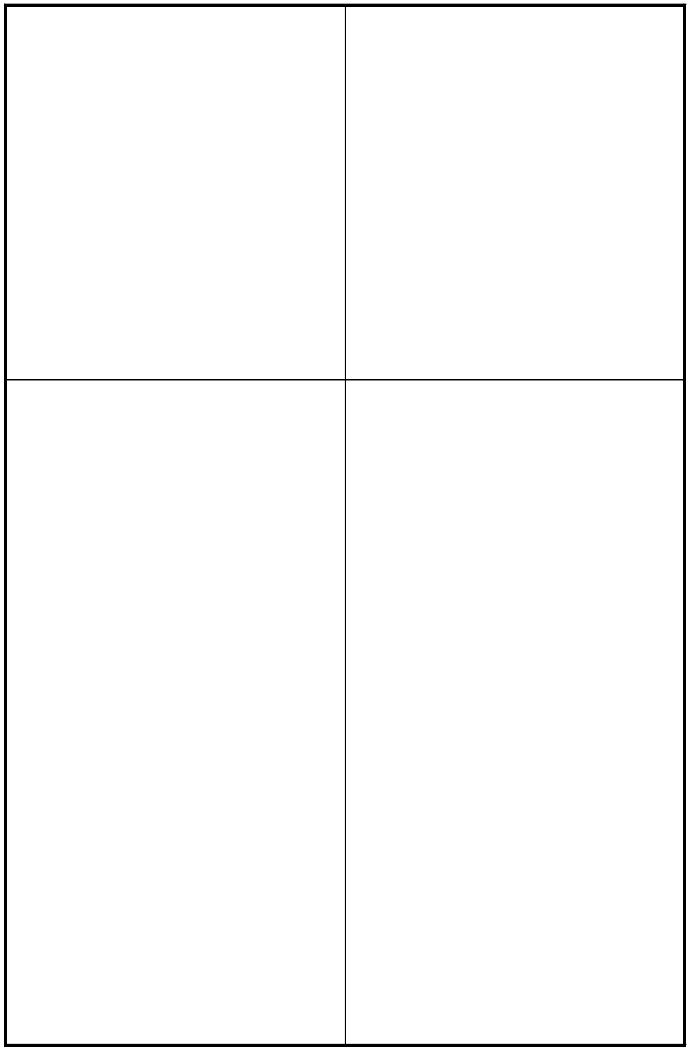
FINIT.CM.MIGR.CM05.01	Leader Approval_Finance	Business or ET leaders approve changes prior to the program being placed into production.

COO.AQC.AQC.AQC.KC.02	AQC Settlement Quality	A Quality Control program validates the completeness and accuracy of AQC Actuarial projections. Management maintains evidence that Quality control was performed. (PEER REVIEW)

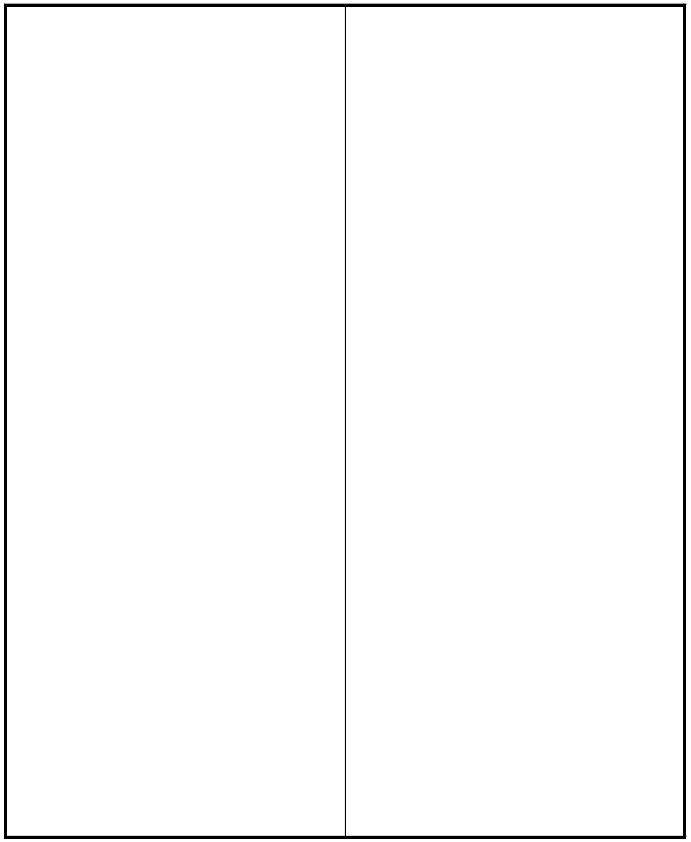
Status (Test)	Effectiveness

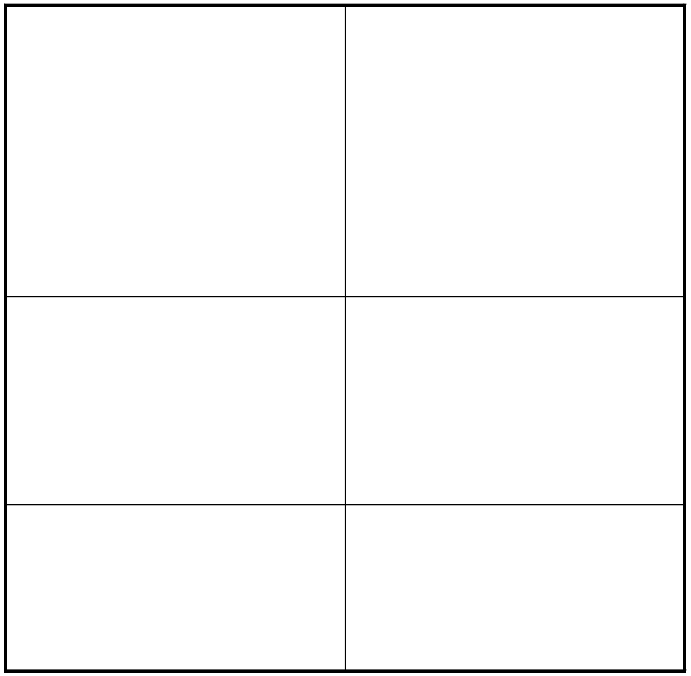


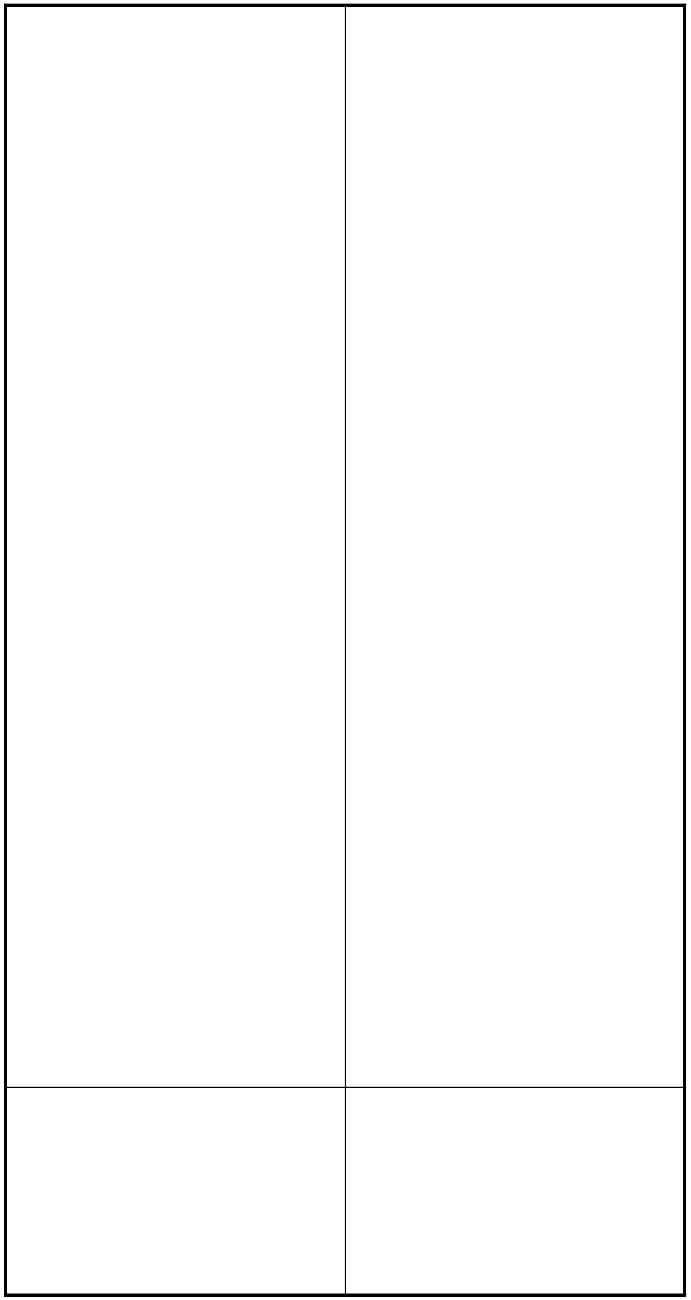


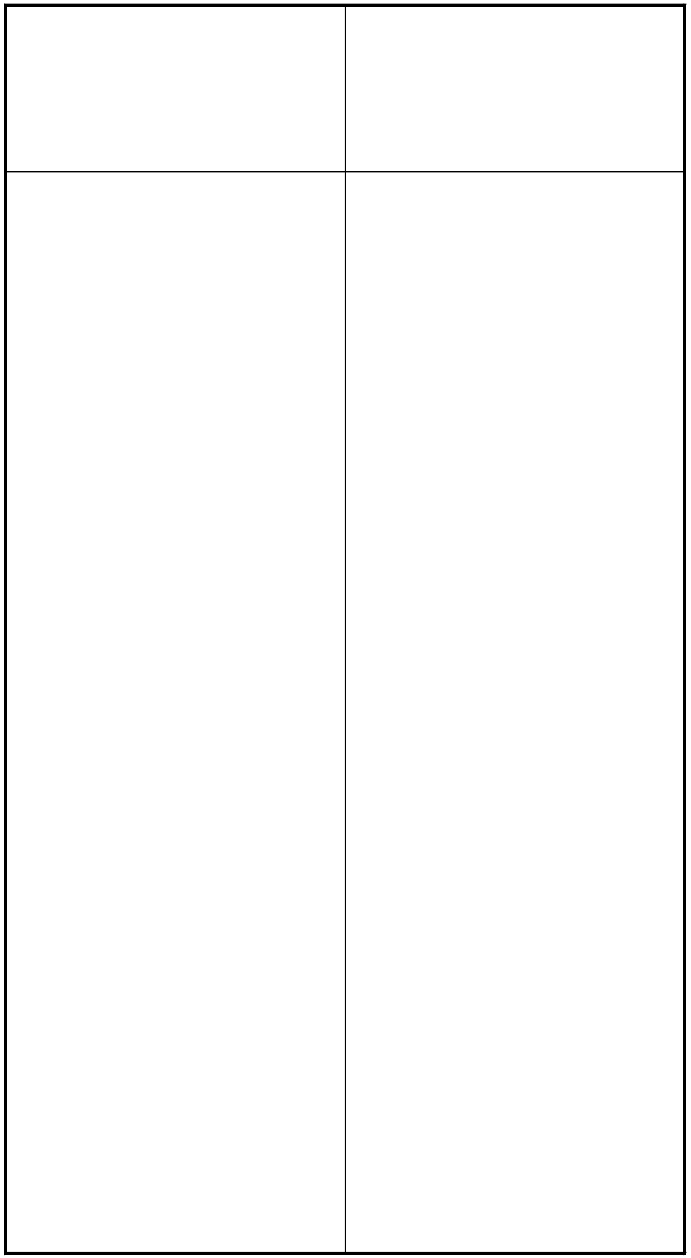


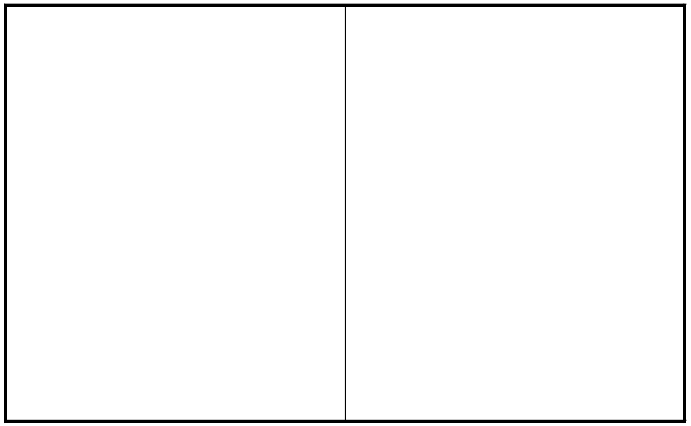
Not Started	Not Tested

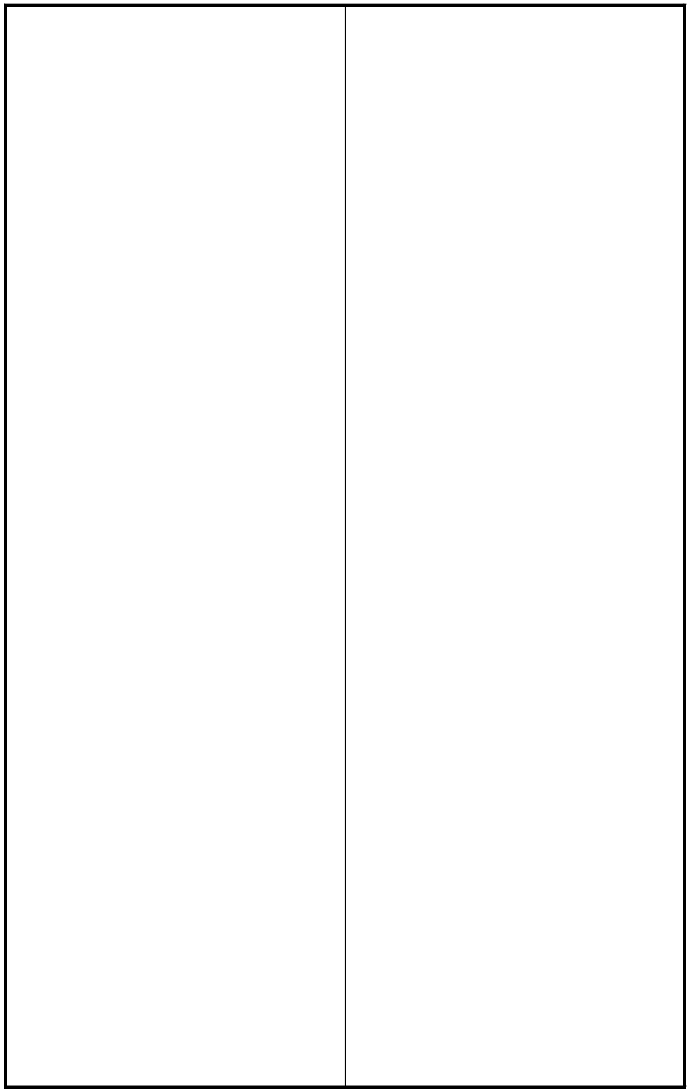


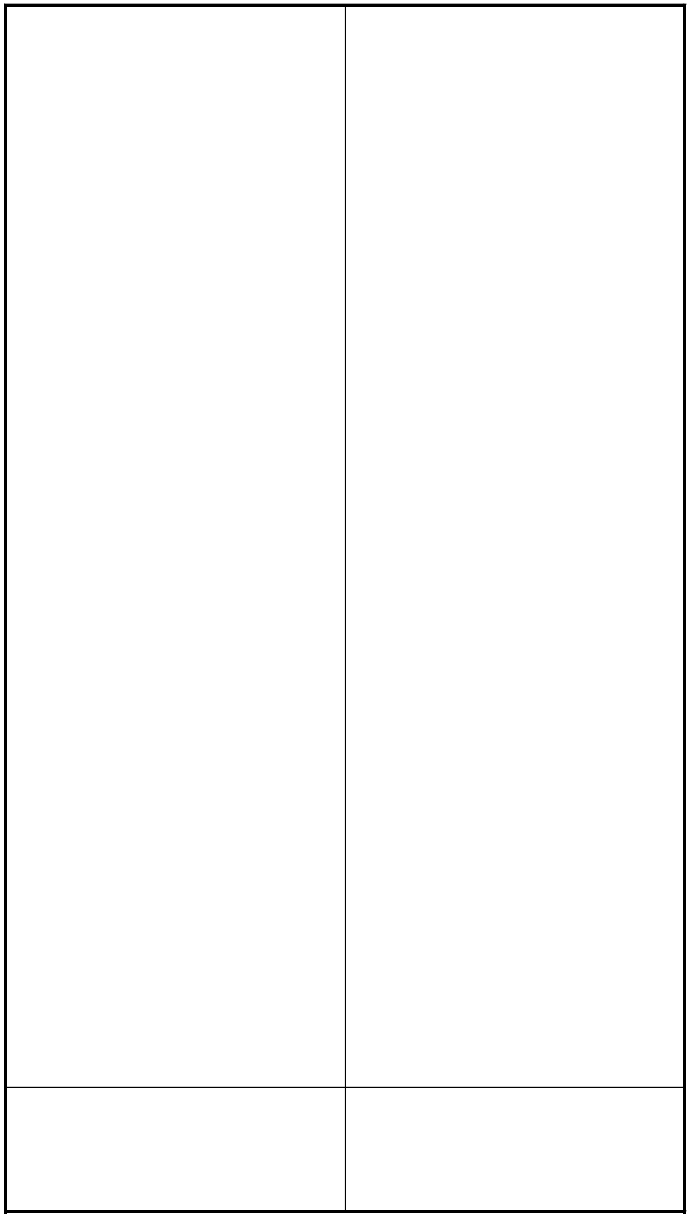


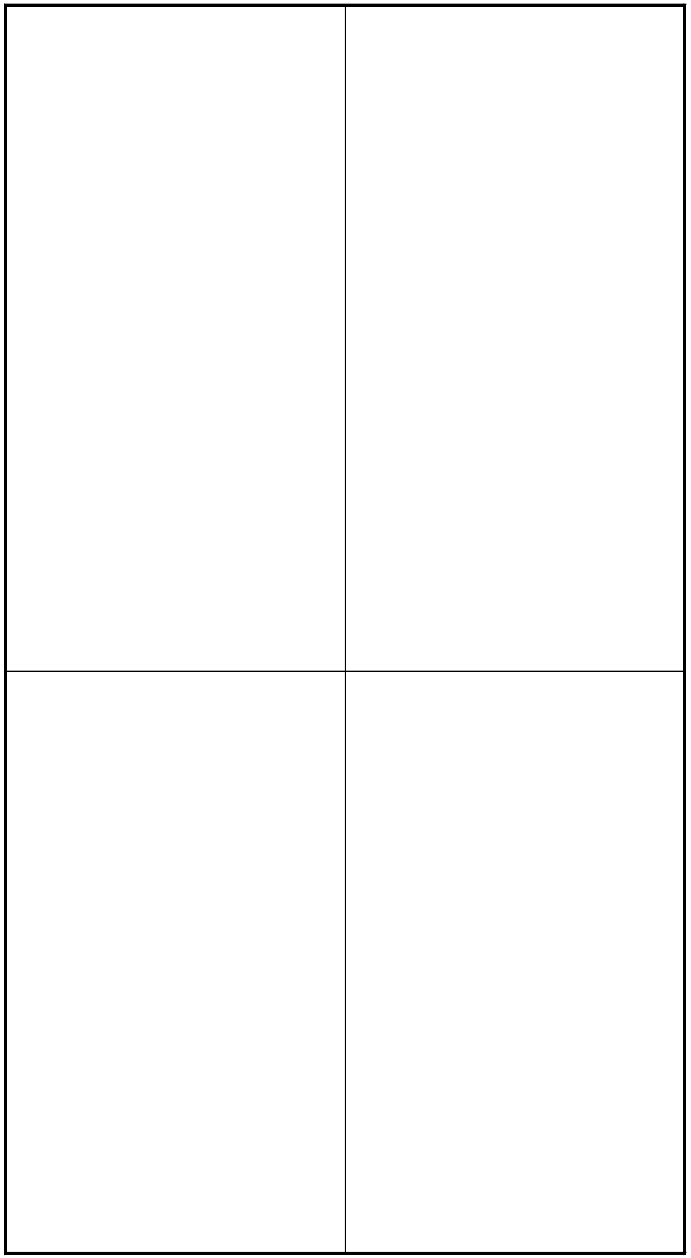




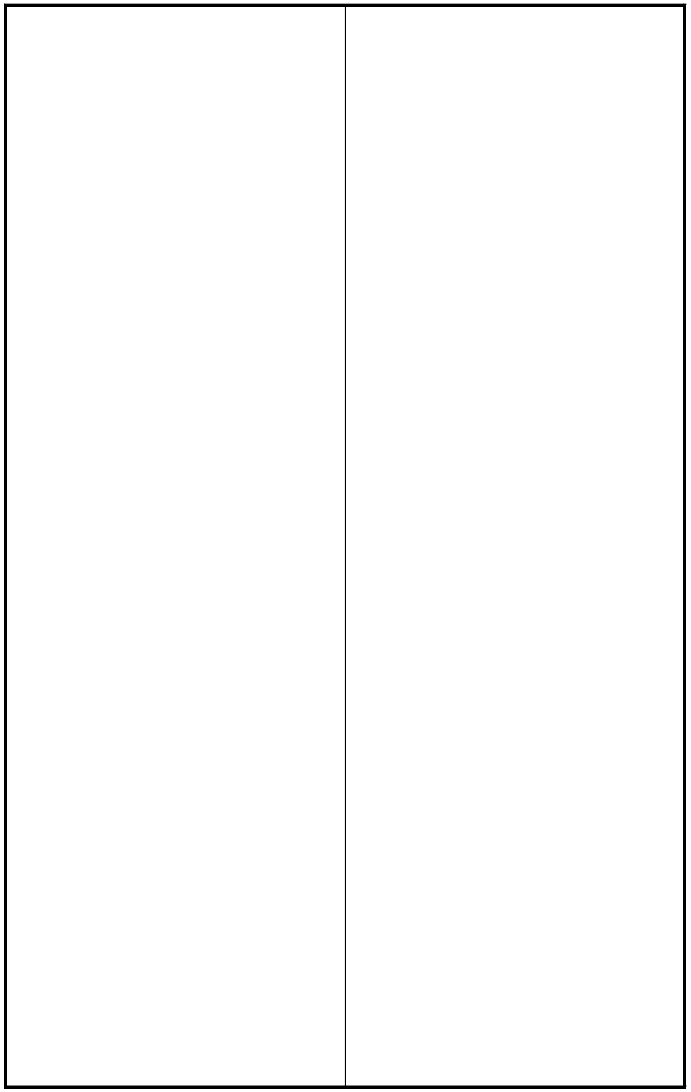


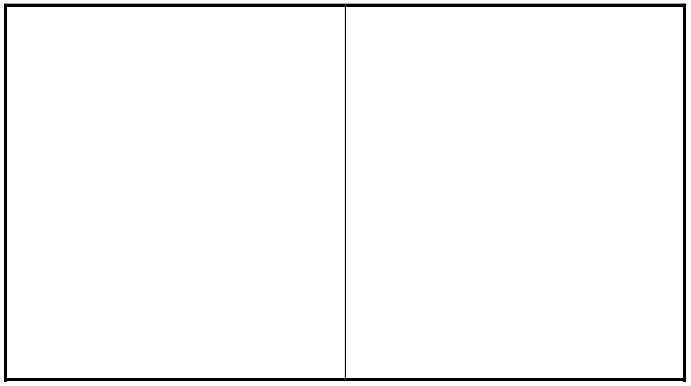




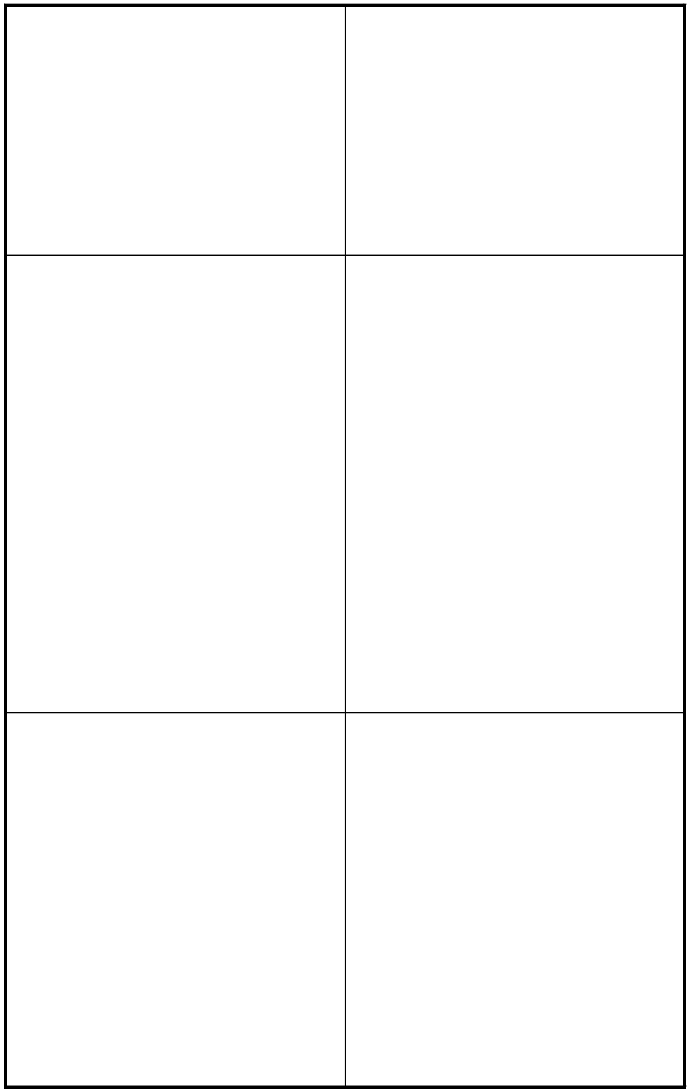


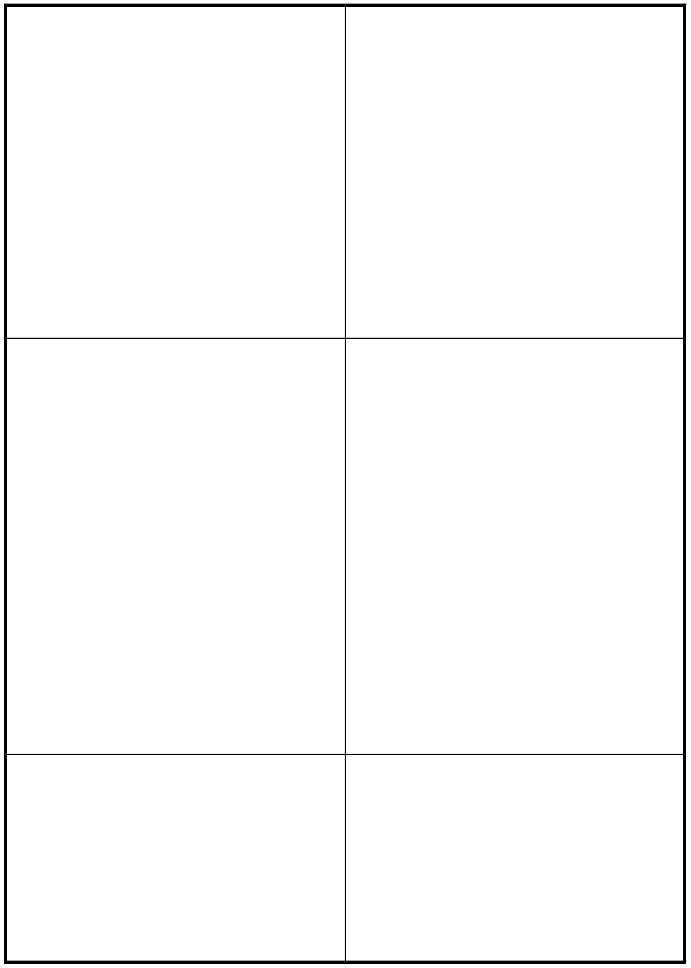
Not Started	Not Tested

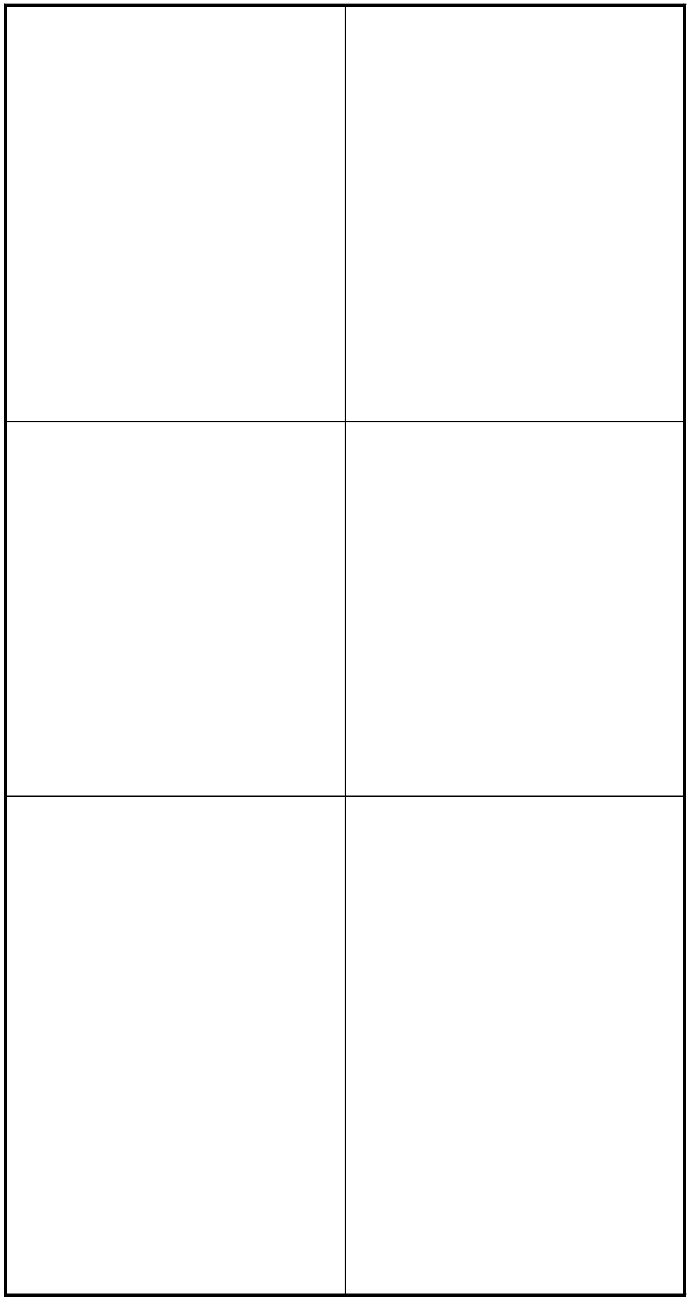


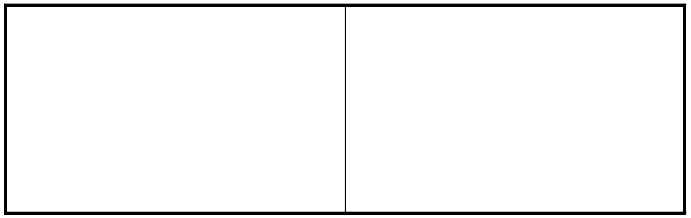


Not Started	Not Tested









Business Risk
Process and control as-is would fail an audit as currently tested. Moderate b/c it is a documentation gap, as no instances of a backup failure were noted as part of our testing or walkthrough. While this is not currently an issue, should failures become more frequent this could raise a significant risk in how to address these risks. Ensure all backups are complete in accordance with the application criticality and approved backup schedule.
Turnaround time and compliance impacts
Inappropriate access to applications; potential control failure if more issues are found.

Priority 1 and 2 Incident/problems are not researched and resolved timely.
Inaccurate populations of changes completed; potential SOC audit findings
Inappropriate access to payroll data.
Inappropriate access to system

Inappropriate system access
HiTrust CAP HiTrust Baseline requirement: Risk designations are assigned for all positions within the organization as appropriate, with commensurate screening criteria, and reviewed/revised every 365 days.
HiTrust CAP. CAP09 HiTrust Baseline: The organization maintains information systems according to a current baseline configuration and configures system security parameters to prevent misuse. Vendor supplied software used in operational systems is maintained at a level supported by the supplier and uses the latest version of web browsers on operational systems to take advantage of the latest security functions in the application. CAP10 HiTrust Baseline: The operating system has in place supporting technical controls such as antivirus, file integrity monitoring, host-based (personal) firewalls or port filtering tools, and logging as part of its baseline. CAP21 HiTrust Baseline: The organization (i) establishes and documents mandatory configuration settings for information technology products employed within the information system using the latest security configuration baselines; (ii) identifies, documents, and approves exceptions from the mandatory established configuration settings for individual components based on explicit operational requirements; and, (iii) monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. CAP27 HiTrust Baseline: A hardened configuration standard exists for all system and network components. CAP30 HiTrust Baseline: Systems are appropriately hardened (e.g., configured with only necessary and secure services, ports, and protocols enabled).

HITRUST CAP. CAP11 HiTrust Baseline: The organization identifies unauthorized (blacklisted) software on the information system, including servers, workstations and laptops, employs an allow-all, deny-by-exception policy to prohibit the execution of known unauthorized (blacklisted) software on the information system, and reviews and updates the list of unauthorized (blacklisted) software periodically but no less than annually. CAP12 HiTrust Baseline: The organization prevents program execution in accordance with the list of unauthorized (blacklisted) software programs and rules authorizing the terms and conditions of software program usage. CAP43 HiTrust Baseline: The organization identifies unauthorized (blacklisted) software on the information system, prevents program execution in accordance with a list of unauthorized (blacklisted) software programs, employs an allow-all, deny-by exception policy to prohibit execution of known unauthorized (blacklisted) software, and reviews and updates the list of unauthorized (blacklisted) software programs annually.
HiTrust CAP. HiTrust Baseline requiring that tools for maintenance are approved, controlled, monitored and periodically checked was not met
HiTrust CAP, HiTrust Baseline: Fallback procedures are defined and implemented, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.
Hitrust CAP, HiTrust Baseline: The technical vulnerability management program is evaluated on a quarterly basis.

HiTrust CAP, HiTrust Baseline: The organization reviews historic audit logs to determine if high vulnerability scan findings identified in the information system have been previously exploited.
HiTrust CAP, HiTrust Baseline: The organization maintains a list of commonly-used, expected, or compromised passwords, and updates the list (i) at least every 180 days and (ii) when organizational passwords are suspected to have been compromised (either directly or indirectly); allows users to select long passwords and passphrases, including spaces and all printable characters; employs automated tools to assist the user in selecting strong passwords and authenticators; and verifies, when users create or update passwords, that the passwords are not found on the organization-defined list of commonly-used, expected, or compromised passwords.
HiTrust CAP, HiTrust Baseline: Users are given a written statement of their access rights, which they are required to sign stating they understand the conditions of access. Guest/anonymous, shared/group, emergency and temporary accounts are specifically authorized and use monitored.
HiTrust CAP, HiTrust Baseline: The organization provides incident response and contingency training to information system users consistent with assigned roles and responsibilities within 90 days of assuming an incident response role or responsibility; when required by information system changes; and within every 365 days thereafter.
HiTrust CAP, HiTrust Baseline: The organization ensures that the senior executives have been trained in their specific roles and responsibilities.

HiTrust CAP, HiTrust Baseline: The organization provides specialized security and privacy education and training appropriate to the employee's roles/responsibilities, including organizational business unit security POCs and system/software developers.
HiTrust CAPS (CAP52) HiTrust Baseline: The organization trains workforce members on how to properly respond to perimeter security alarms. (CAP59) HiTrust Baseline: A duress alarm is provided whereby a person under duress can indicate such problems and responded to accordingly by the organization. (CAP72) HiTrust Baseline: Inventories of physical access devices are performed every 90 days. (CAP73) HiTrust Baseline: Intrusion detection systems (e.g., alarms and surveillance equipment) are installed on all external doors and accessible windows, the systems are monitored, and incidents/alarms are investigated. (CAP74) HiTrust Baseline: The organization actively monitors unoccupied areas at all times and sensitive and/or restricted areas in real time as appropriate for the area. (CAP75) HiTrust Baseline: The organization regularly tests alarms to ensure proper operation. (CAP76) HiTrust Baseline: The organization maintains an electronic log of alarm system events and regularly reviews the logs, no less than monthly. (CAP78) HiTrust Baseline: Any security threats presented by neighboring premises are identified.
HiTrust CAP, HiTrust Baseline: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of security requirements and controls in developed and acquired information systems.

HiTrust CAP, HiTrust Baseline: Specifications for the security control requirements state automated controls will be incorporated in the information system, supplemented by manual controls as needed, as evidenced throughout the SDLC.
HiTrust CAP, HiTrust Baseline: The organization requires the developer of the information system, system component, or information system service to provide specific control design and implementation information.
HiTrust CAP, HiTrust Baseline: Repairs or modifications to the physical components of a facility which are related to security (e.g., hardware, walls, doors and locks) are documented and retained in accordance with the organization's retention policy.
HiTrust CAP, HiTrust Baseline: Fire authorities are automatically notified when a fire alarm is activated.

HiTrust CAP, HiTrust Baseline: The organization's formal policies and procedures, other critical records and disclosures of individuals' protected health information made are retained for a minimum of six years; and, for electronic health records, the organization retains records of disclosures to carry out treatment, payment and health care operations for a minimum of three years.
HiTrust CAP, HiTrust Baseline: The organization documents and maintains (i) designated record sets that are subject to access by individuals, and (ii) titles of the persons or office responsible for receiving and processing requests for access by individuals as organizational records for a period of six years.
HiTrust CAP (CAP71) HiTrust Baseline: Doors to internal secure areas lock automatically, implement a door delay alarm, and are equipped with electronic locks. (CAP72) HiTrust Baseline: Inventories of physical access devices are performed every 90 days. (CAP75) HiTrust Baseline: The organization regularly tests alarms to ensure proper operation. (CAP76) HiTrust Baseline: The organization maintains an electronic log of alarm system events and regularly reviews the logs, no less than monthly. (CAP77) HiTrust Baseline: Fire prevention and suppression mechanisms, including workforce training, are provided.
Inappropriate access to system

Inappropriate system access
Inappropriate system access
Inappropriate system access

Inappropriate system access
Inappropriate system access
Inappropriate system access

Inappropriate system access
Inappropriate system access
HiTrust Baseline: Changes to information assets, including systems, networks, and network services, are controlled and archived.
Inappropriate access to system

Access to data is restricted to properly authorized personnel. Compensating controls exist to ensure access is appropriate.
Application system disruption
Inappropriate access to systems
Inappropriate system access

Inappropriate access to systems
Potential unauthorized changes to the system. Persons with both deploy and development responsibilities can create change to system without proper SOD.

Inappropriate system access
Not properly testing patches in a lower region can lead to unexpected vulnerabilities in the production environment potentially exposing PHI or lead to a malware attack.

Inappropriate access to systems

One high level vendor risk was not remediated in a timely manner.
Inappropriate access to systems.
Physical security access risk
Inappropriate access to company assets

Sensitive/confidential (PII/PHI) information is provided to vendor without the proper controls in place to mitigate the risks of member data being accessed in an unauthorized manner. The lack of knowing when a vendor has access to PII/PHI exposes BCBSMA and its members to unacceptable risk surrounding their data if IRM, InfoSec, Legal, and Internal Audit are unable to assess the controls and environment the vendor is ingesting and storing BCBSMA member data in. Ensure all vendors who have access to BCBSMA member PII/PHI have adequate controls in place to protect sensitive and confidential data.
Sending member data (PHI/PII) without proper approvals and ensuring technical controls are in place exposes BCBSMA to risk unauthorized access to member data, offshore data storage regulations, and member data exfiltration. All of these can result in reputational damage, fines, and compliance and/or audit issues. Any issue relating to member data, PHI/PII, and vendor data transfer warrants a "High" designation given the sensitive nature of the issue and need for immediate remediation. All member data (PHI/PII) sent to vendors is approved and adequate technical controls are in place to safeguard BCBSMA member data.
Without logging of dba/admin/priv account activity, BCBSMA is unable to research and investigate any unauthorized or historical activity that may impact system data, functionality, or availability adversely. Noted as high due to the current state being unable to pass an audit in the current state of the process and history maintained by the logging of the DAL and PostgresDB environments. All changes to data and systems are appropriate and authorized by DBAs, admins, and privileged users.
Moderate financial impact and potential for the same finding for 2022 claims if ESI has had incorrect system set up

Immature data governance structure over the Member Rights Database can result in data breaches and HIPAA violations. The number of privacy incidents and HIPAA violations have continued to increase over the past couple of years due to immature data governance around the Member Right's database. Timely and appropriate reconciliation of GL accounts
Member, Provider and Account impacts due to misinformation and lack of timeliness. At risk for BCBSA oversight. Failure to meet BCBSA performance standards for three key measures. Quality control to ensure accurate, complete and timely information provided to members and providers
Sharing of sensitive data not in accordance with established policies to prevent misuse and breaches can lead to a high risk of data misuse and breaches.

HiTrust CAP CAP06 HiTrust Baseline: Changes to equipment, software, and procedures are strictly and consistently managed. CAP08 HiTrust Baseline: Operational systems only hold approved programs or executable code. CAP13 HiTrust Baseline: Applications and operating systems are tested for usability, security, and impact prior to production. CAP14 HiTrust Baseline: A rollback strategy is in place before changes are implemented, and an audit log is maintained of all updates to operational program libraries. CAP15 HiTrust Baseline: Managers responsible for application systems are also responsible for the strict control (security) of the project or support environment and ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment. CAP16 HiTrust Baseline: The organization manages changes to mobile device operating systems, patch levels, and/or applications through a formal change management process. CAP18 HiTrust Baseline: The organization has developed, documented, and implemented a configuration management plan for the information system. CAP19 HiTrust Baseline: Changes are formally controlled, documented, and enforced in order to minimize the corruption of information systems. CAP20 HiTrust Baseline: Installation checklists and vulnerability scans are used to validate the configuration of servers, workstations, devices, and appliances, and ensure the configuration meets minimum standards.
HiTrust CAP, HiTrust Baseline: A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing entity (client) or cloud service provider-managed client data, and the use of unapproved application stores is prohibited for company-owned and BYOD mobile devices. Non-approved applications or approved applications not obtained through approved application stores are prohibited.

HiTrust CAP, HiTrust Baseline: An inventory of assets and services is maintained.

HiTrust CAP, HiTrust Baseline: Applications developed by the organization are based on secure coding guidelines to prevent common vulnerabilities or undergo appropriate testing.

HiTrust CAP, HiTrust Baseline: The organization changes passwords for default system accounts, whenever there is any indication of password compromise, at first logon following the issuance of a temporary password, and requires immediate selection of a new password upon account recovery.
HiTrust CAP, HiTrust Baseline: Group, shared or generic accounts and passwords (e.g., for first-time log-on) are not used.
HiTrust CAP, HiTrust Baseline: The organization reviews critical system accounts and privileged access rights every 60 days; all other accounts, including user access and changes to access authorizations, are reviewed every 90 days.
HiTrust CAP, HiTrust Baseline: A time-out mechanism (e.g., a screen saver) pauses the session screen after 15 minutes of inactivity, closes network sessions after 30 minutes of inactivity, and requires the user to reestablish authenticated access once the session has been paused or closed; or, if the system cannot be modified, a limited form of time-out that clears the screen but does not close down the application or network sessions is used.
HiTrust CAP, HiTrust Baseline: The organization provides a rationale for why the auditable events are deemed adequate to support after the fact investigations of security incidents and which events require auditing on a continuous basis in response to specific situations; and the listing of auditable events and supporting rational are reviewed and updated periodically within 365 days.
HiTrust CAP, HiTrust Baseline: When developing software or systems the organization performs thorough testing and verification during the development process.

The Change Advisory Board (CAB) meets weekly to review proposed changes that are risk-ranked above a certain category. oThe risk ranking is solely validated by ET, and the risk ranking categories are not clearly defined. This could lead to impactful changes not being reviewed by all relevant stakeholders. For the Palo Alto implementation, information security risk considerations were not included as criteria for the risk ranking. As a result, the InfoSec (CISO, if escalation needed) and IRM teams were not included as approvers for the Palo Alto changes that had security risk implications. oET noted that stakeholder approvals may occur before the proposed changes have been reviewed at a CAB meeting. This limits the value of the meeting, as approvals may be given without regard to important considerations that may be brought up at the CAB meeting.
AD group access controls are designed to ensure access to data is restricted to properly authorized personnel. Ineffective implementation of these controls as designed increase information security risks.
AD group access controls are designed to ensure access to data is restricted to properly authorized personnel. Insufficient design and ineffective implementation of these controls increase information security risks.
Relevant corporate policies and standards do not differentiate information security risk considerations or requirements for onshore versus offshore associates and contractors. This is important due to the heightened risks of potential unauthorized disclosure of sensitive data offshore.

Inappropriate system access due to unenforced Segregation of duties (SoD)

Without logging and monitoring of system changes, BCBSMA is unable to research and investigate any unauthorized or historical activity that may impact system data, functionality, or availability adversely

Inaccurate financial reporting
Inaccurate reporting on AQC Settlements

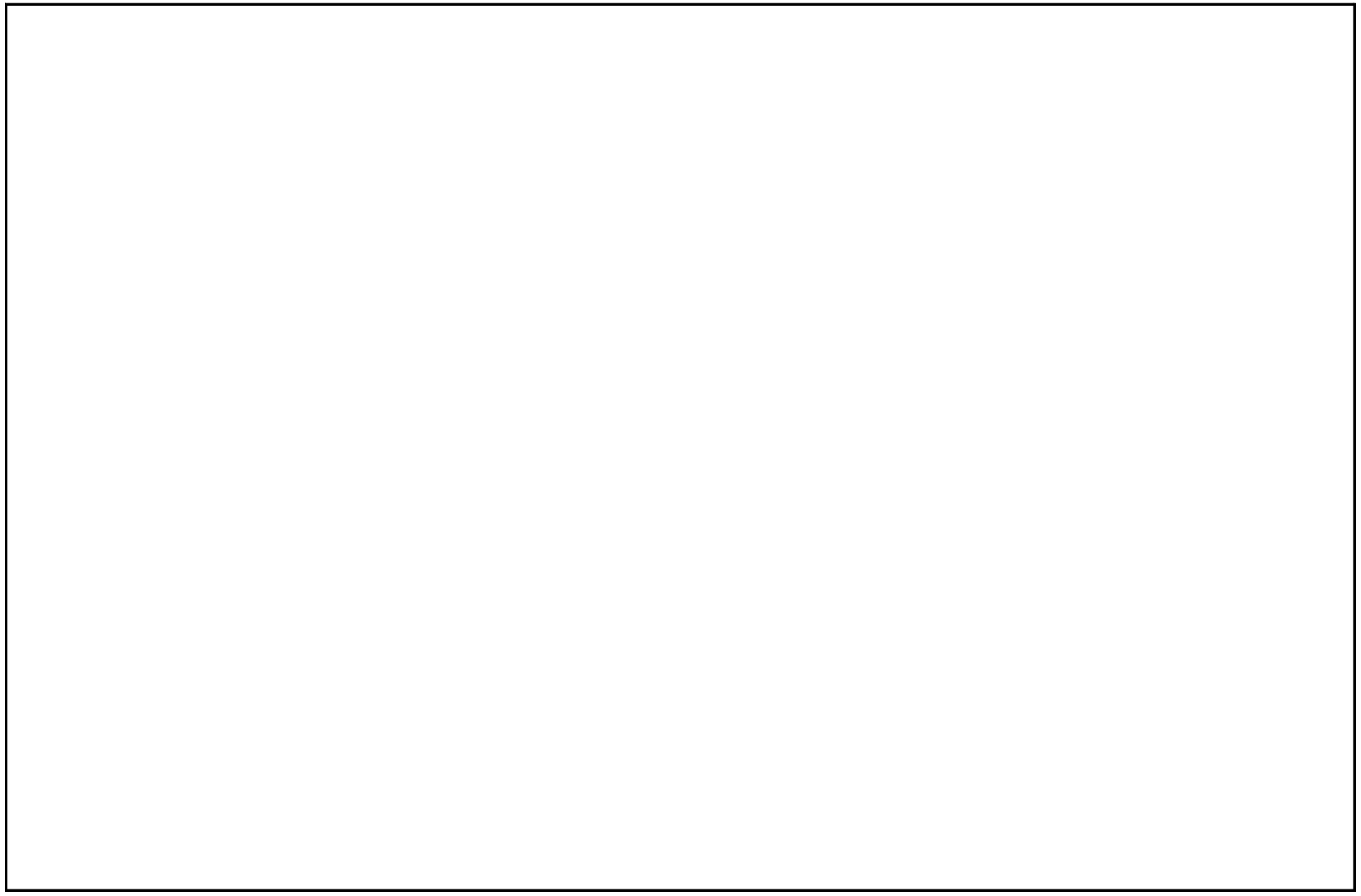
Risk of non-compliance if this happened in more than one sample in the FEP Self-Assessment testing.
Access to data is restricted to properly authorized personnel. Compensating controls exist to ensure access is appropriate.
Inappropriate access to systems
ESI processed thousands of specialty claims incorrectly, and they owe BCBSMA $2.9 million. There is no risk of ESI repeating this, as they are no longer our PBM, but there is a risk of CVS Health processing specialty claims incorrectly, and a risk of BCBSMA not receiving the money owed.
Inappropriate access to BCBSMA information systems and sensitive data

Access to data is not restricted to properly authorized personnel.
Inappropriate access to systems
Inappropriate access to systems
Inappropriate access to systems/ Inappropriate changes to systems

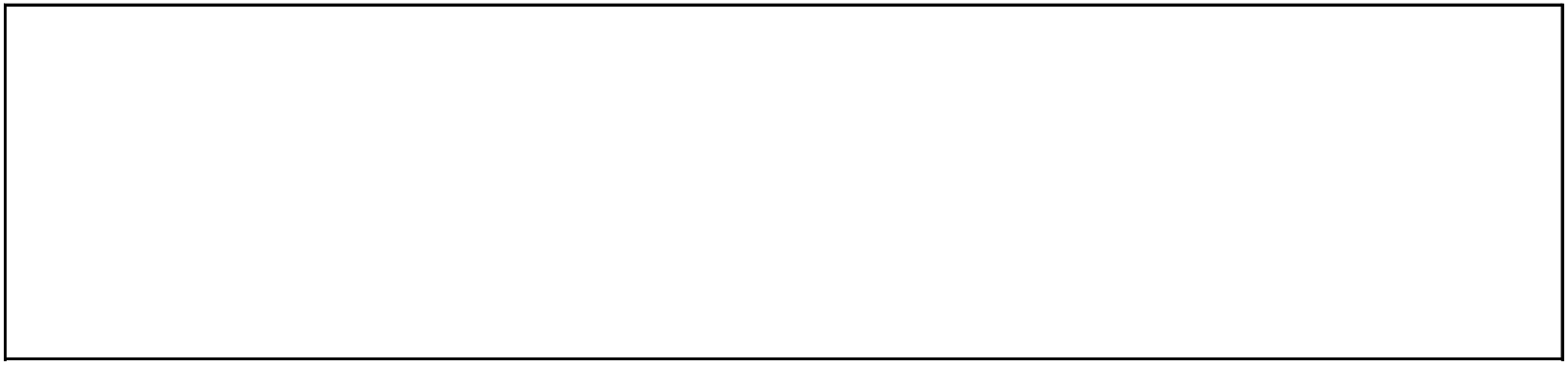
Potential unauthorized changes to the system. Persons with both pipeline admin role and development responsibilities can create change to system without proper SOD.
Potential inappropriate access to system. This control is meant to provide reasonable assurance that logical access to data is restricted to properly authorized personnel.

Incorrect change output from system could result in incomplete change management documentation, i.e. approvals, testing.
Access to data is restricted to properly authorized personnel.
Inappropriate access to system
Inappropriate access to systems
Inappropriate access to systems

Inappropriate access to systems
Access to data is not restricted to properly authorized personnel.



Access to data is restricted to properly authorized personnel.
Information Security



ASC billings and receivables may be inaccurate, incomplete, and untimely.

Could have resulted in financial impact
Inappropriate access; security risk

Loss of productivity
Audit issues, inappropriate access
inappropriate application changes
inappropriate system changes
Operational impacts
Unauthorized Access to Systems
Unauthorized access to data
Business disruption / inability to operate

Inappropriate access, potential processing issues

Identify and categorize the variance between the Plan's FEP benefits receivable balance and the FEP benefits payable balance recorded at the FEP Director's Office. We are not in compliance with FAM Volume 3, Chapter 3 requirements. The Plan is out of compliance with CS 1039 (Contract between The Federal Employee Program Directors Office and the Office of Personnel Management)
As currently tested, the controls for DRP and BCP would fail for the DAL application and AWS platform/environment. The inability to recover or continue operations for a key solution like DAL could cause significant disruptions if an adverse event were to happen or vendor were to experience a significant outage. Recover from business or environmental disruption or disaster within the BCBSMA timeline as indicated by the DRP and/or BCP.

Benefits changes not subject to a quality can lead to inaccurate benefit set-up at the account and/or group scale, potentially impacting a large number of members depending on the size of the account/group.
BARs should be the source of truth per Sales and UW approved-benefits. But other sources such as OLB and contracts are being used to determine which benefits (ex. Rx Co-pays) members should have. This may lead to configured benefits that are not UW or Sales approved. Impact could be at the account/group scale.
Incorrect accumulation information being sent to CVS may result in members who are overpaying or underpaying. Accum rules could impact numerous account, groups, and members. Note that there is a small subset of members

low member impact
CMS issues compliance letter to CVS
PNR going away in 2024

HiTrust CAP HiTrust baseline: The security policy reviews consider all appropriate elements that could impact the organization's risk profile.
HiTrust CAP HiTrust Baseline: File sharing is disabled on wireless-enabled devices. HiTrust Baseline: The organization disables Bluetooth and peer-to-peer networking protocols within the information system determined to be unnecessary or non-secure.
HiTrust CAP, HiTrust Baseline: Organizational inventories of IT assets are updated during installations, removals, and system changes, with full physical inventories performed for capital assets (at least annually) and for non-capital assets.
HiTrust CAP, HiTrust Baseline: Account types are identified (individual, shared/group, system, application, guest/anonymous, emergency and temporary), conditions for group and role membership are established, and, if used, shared/group account credentials are modified when users are removed from the group.

Non-compliance
Inappropriate changes to systems

Tester	Reviewer	Subscribers	Impacted Risks
James Farrell	Lisa George	Rich Trisoline	
Theresa Lynch	Kim Sok	Rich Trisoline	
Bernard Mumuluh	Alexander DeSimone	Sri Narasimhan;;Rich Trisoline	

Bernard Mumuluh	Alexander DeSimone	Rich Trisoline	
Bernard Mumuluh	James Farrell	Lisa George;;Rich Trisoline;;Mark Noonan	
Bernard Mumuluh	Alexander DeSimone	Richard Stinson	
Bernard Mumuluh	Alexander DeSimone	Sri Narasimhan;;Shafat Khan (Deleted);;Malar Vizhi Somasundaram;;Rich Trisoline	

Bernard Mumuluh	Alexander DeSimone	Rich Trisoline	
Korelle Foy	James Farrell	Alex Rodriguez	
Korelle Foy	Alexander DeSimone	Rich Trisoline	

Bernard Mumuluh	Alexander DeSimone	Rich Trisoline	
Korelle Foy	James Farrell	Wendy Ross-Atwood;;Rich Trisoline;;Salil Goel	
Korelle Foy	Alexander DeSimone	Hiren Thakkar;;Rich Trisoline	
Korelle Foy	James Farrell	Rich Trisoline	

Korelle Foy	James Farrell	Rich Trisoline	
Korelle Foy	James Farrell	Rich Trisoline	
Bernard Mumuluh	Alexander DeSimone	Hiren Thakkar;;Donna Price (no-access);;Rich Trisoline	
Korelle Foy	James Farrell	Rich Trisoline	
Korelle Foy	James Farrell	Rich Trisoline	

Korelle Foy	James Farrell	Rich Trisoline	
Korelle Foy	James Farrell	Rich Trisoline;;Wendy Ross-Atwood;;Salil Goel	
Korelle Foy	James Farrell	Rich Trisoline	

Bernard Mumuluh	Alexander DeSimone	Rich Trisoline;;Robert DiRamio	
Korelle Foy	James Farrell	Rich Trisoline;;Robert DiRamio	
Korelle Foy	James Farrell	Wendy Ross-Atwood;;Rich Trisoline;;Salil Goel	
Korelle Foy	James Farrell	Wendy Ross-Atwood;;Rich Trisoline;;Salil Goel	

Korelle Foy	James Farrell	Alex Rodriguez	
Korelle Foy	James Farrell	Alex Rodriguez	
Korelle Foy	James Farrell	Rich Trisoline;;Wendy Ross-Atwood;;Salil Goel	
Bernard Mumuluh	Alexander DeSimone	Sri Narasimhan;;Rich Trisoline	

Alexander DeSimone	James Farrell	Lisa George;;James Farrell;;Rich Trisoline;;Adeola Adebiyi	Inappropriate access to both member and group files/transactions and/or claims/eligibility processing systems could lead to data theft and data breaches
Alexander DeSimone	James Farrell	Lisa George;;James Farrell;;Rich Trisoline	
Bernard Mumuluh	Alexander DeSimone		

Bernard Mumuluh	Alexander DeSimone	Hiren Thakkar;;Donna Price (no-access);;Adeola Adebiyi	
Bernard Mumuluh	Alexander DeSimone	Shafat Khan (Deleted);;Malar Vizhi Somasundaram;;Rich Trisoline	
Bernard Mumuluh	Alexander DeSimone		

Bernard Mumuluh	Alexander DeSimone	Rich Trisoline	
Bernard Mumuluh	Alexander DeSimone	Adeola Adebiyi;;Rich Trisoline	
Bernard Mumuluh	Alexander DeSimone	James Farrell;;Rich Trisoline	
Bernard Mumuluh	Alexander DeSimone	Sri Narasimhan;;Rich Trisoline;;Adeola Adebiyi	
Bernard Mumuluh	Alexander DeSimone	James Farrell;;Rich Trisoline;;Walter Endyke	
Zachary Mucha	Nikita Sujan	Jackie Dillon;;Josephine Zhang	

Korelle Foy	Alexander DeSimone	Hiren Thakkar;;Rich Trisoline;;Mike Kane	
Bernard Mumuluh	Alexander DeSimone	Steven Thurber;;James Farrell	
Korelle Foy	Alexander DeSimone	James Farrell	
External Auditor (Deleted) (no-access)	Alexander DeSimone	Sureshkumar Chinnappan;;James Farrell	

External Auditor (Deleted) (no-access)	Alexander DeSimone	James Farrell	
Alexander DeSimone	James Farrell	James Farrell;;Humayun Shaik;;Pavan Anna;;Yeswanth Poolikunta;;Mike Kane	

Korelle Foy	Alexander DeSimone	James Farrell	
Bernard Mumuluh	Alexander DeSimone	Rich Trisoline	

Korelle Foy	Alexander DeSimone	James Farrell	

Korelle Foy	Alexander DeSimone	James Farrell	
Korelle Foy	Alexander DeSimone	James Farrell	
Korelle Foy	Alexander DeSimone	James Farrell	
Korelle Foy	Alexander DeSimone	James Farrell;;Rich Trisoline	

Alex Rodriguez	Alexander DeSimone	Yeswanth Poolikunta;;Rich Trisoline	
Bernard Mumuluh	Alexander DeSimone	Rashi Khanna;;James Farrell	
Bernard Mumuluh	Alexander DeSimone	Adeola Adebiyi;;James Farrell	
Melissa Trenholm	Theresa Lynch		

Jonathan St Vincent	Margaret Fu	Jennifer Read;;Carolyn Jose;;Pedro Ramos	
Jonathan St Vincent	Margaret Fu	Lisa George;;Jennifer Read;;Rich Trisoline;;Carolyn Jose;;Pedro Ramos	
Alexander DeSimone	James Farrell	Robert Lang;;Rich Trisoline;;Mark Noonan	
Melissa Trenholm	Theresa Lynch	Lisa George;;Timothy Bulman	

Nikita Sujan	Lisa George	Jen Abdel-Samed;;Prem Somasundaram;;Sri Narasimhan;;Himanshu Arora (Deleted) (no-access);;Steven Akeley	Inappropriate access to both member and group files/transactions and/or claims/eligibility processing systems could lead to data theft and data breaches
Theresa Tillmon	Lisa George		
Nikita Sujan	Lisa George	Himanshu Arora (Deleted) (no-access)	

Korelle Foy	James Farrell	Hiren Thakkar;;Donna Price (no-access);;Rich Trisoline	
Korelle Foy	James Farrell	Rich Trisoline	

Bernard Mumuluh	Alexander DeSimone	Rich Trisoline	
Korelle Foy	James Farrell	Hiren Thakkar;;Rich Trisoline	

Korelle Foy	James Farrell	Rich Trisoline;;Adeola Adebiyi;;Bessie Ezuma-Ngwu;;Charles Robertson;;Sandra Brown	
Korelle Foy	James Farrell	Hiren Thakkar;;Donna Price (no-access);;Rich Trisoline	
Bernard Mumuluh	Alexander DeSimone	Rich Trisoline	
Korelle Foy	James Farrell	Rich Trisoline	
Korelle Foy	James Farrell	Rich Trisoline	
Korelle Foy	James Farrell	Wendy Ross-Atwood;;Rich Trisoline;;Salil Goel	

Margaret Fu	James Farrell	Lisa George;;Mark Noonan;;Rich Trisoline	
Margaret Fu	James Farrell	Lisa George;;Adeola Adebiyi;;Rich Trisoline;;Bessie Ezuma-Ngwu;;Charles Robertson;;Sandra Brown	
Margaret Fu	James Farrell	Lisa George;;Adeola Adebiyi;;Rich Trisoline;;Bessie Ezuma-Ngwu;;Charles Robertson;;Sandra Brown	
Margaret Fu	James Farrell	Lisa George;;Rich Trisoline;;Carolyn Jose;;Pedro Ramos	

Bernard Mumuluh	Alexander DeSimone	Humayun Shaik;;Rich Trisoline;;Hiren Thakkar;;Adeola Adebiyi	

Bernard Mumuluh	Alexander DeSimone	Pavan Anna;;Humayun Shaik;;Dipen Gajaria;;Rich Trisoline;;Hiren Thakkar	

Zachary Mucha	Nikita Sujan	Zachary Mucha	
Zachary Mucha	Nikita Sujan	Jackie Dillon;;Josephine Zhang	

Melissa Trenholm	Theresa Lynch	Timothy Bulman	
Bernard Mumuluh	Alexander DeSimone	Hiren Thakkar;;Rich Trisoline;;Mike Kane;;Ryan Canney;;Yeswanth Poolikunta	
Korelle Foy	Alexander DeSimone		
Melissa Trenholm	Theresa Lynch	Timothy Bulman	
Bernard Mumuluh	Alexander DeSimone	James Farrell	

Alexander DeSimone	James Farrell	Donna Price (no-access);;James Farrell;;Mike Kane	
Alexander DeSimone	James Farrell	James Farrell;;Donna Price (no-access);;Mike Kane	
Korelle Foy	Alexander DeSimone	James Farrell	
Korelle Foy	Alexander DeSimone	James Farrell;;Rich Trisoline;;Humayun Shaik;;Yeswanth Poolikunta	

Korelle Foy	Alexander DeSimone	Humayun Shaik;;James Farrell;;Pavan Anna;;Mike Kane;;Yeswanth Poolikunta;;Rich Trisoline;;Ryan Canney	
Korelle Foy	Alexander DeSimone	James Farrell;;Mike Kane;;Yeswanth Poolikunta;;Ryan Canney	

Korelle Foy	Alexander DeSimone	James Farrell;;Robert Quick;;Rich Trisoline;;Humayun Shaik	
Korelle Foy	Alexander DeSimone	James Farrell	
Korelle Foy	Alexander DeSimone	James Farrell;;Donna Price (no-access);;Mike Kane	
Alexander DeSimone	James Farrell	James Farrell	
Korelle Foy	Alexander DeSimone	James Farrell;;Mike Kane;;Donna Price (no-access)	

Korelle Foy	Alexander DeSimone	James Farrell	
Melissa Trenholm	Theresa Lynch	Lisa George;;Timothy Bulman	
Korelle Foy	Alexander DeSimone	James Farrell;;Yeswanth Poolikunta;;Ryan Canney	
Alex Rodriguez	Alexander DeSimone	Yeswanth Poolikunta;;James Farrell;;MaheswaraReddy Talla;;Kapil Pahuja;;Pattabiraman Rajamannar;;Adeola Adebiyi;;Aravind Murugesh	
Alex Rodriguez	Alexander DeSimone	James Farrell;;MaheswaraReddy Talla;;Kapil Pahuja;;Pattabiraman Rajamannar;;Yeswanth Poolikunta;;Rich Trisoline	

Theresa Lynch			

Korelle Foy	Alexander DeSimone	James Farrell	
Korelle Foy	James Farrell	James Farrell	
Alex Rodriguez	Alexander DeSimone	James Farrell;;MaheswaraReddy Talla;;Yeswanth Poolikunta;;Dean Volungis	
Alex Rodriguez	Alexander DeSimone	Yeswanth Poolikunta;;MaheswaraReddy Talla	

Ollie Bodden	Zachary Mucha	Steven Thurber;;Martin Kelly	

Bernard Mumuluh	Alexander DeSimone	Pattabiraman Rajamannar;;James Farrell;;Yeswanth Poolikunta	
Kim Sok	Nikita Sujan		

Ollie Bodden	Zachary Mucha	Roger Proulx;;Jozef Nagy	
Melissa Trenholm	Theresa Lynch	Timothy Bulman	
Lisa George	James Farrell		
Lisa George	James Farrell	Rich Trisoline	

Lisa George	James Farrell	Rich Trisoline;;Adeola Adebiyi	
Lisa George	James Farrell	Adeola Adebiyi	
Lisa George	James Farrell		
Lisa George	James Farrell		
Lisa George	James Farrell	Mark Noonan;;Rich Trisoline;;Carl Thompson	
Alexander DeSimone	James Farrell	Sri Narasimhan;;Arunkumar Ramakrishnan;;Andrew Moore	
Bernard Mumuluh	Alexander DeSimone	James Farrell;;Rich Trisoline	
Alexander DeSimone	Lisa George	Kapil Pahuja;;Hiren Thakkar	

Alexander DeSimone	Lisa George	Rafael Garcia;;Merribeth Flaherty (no-access)	
Lisa George	Lisa George		
Melissa Trenholm	Theresa Lynch		
Melissa Trenholm	Theresa Lynch		
Melissa Trenholm	Theresa Lynch		
Korelle Foy	Alexander DeSimone	James Farrell;;Jensen Lugo Velez	

Bernard Mumuluh	Alexander DeSimone	Hiren Thakkar;;James Farrell;;Christopher Tomascak (no-access);;Diana Salvucci;;Pattabiraman Rajamannar	
Timothy Bulman	Lisa George		
Alexander DeSimone	James Farrell	Rich Trisoline;;Yeswanth Poolikunta;;Alexander DeSimone;;Scott Connell (no-access);;James Farrell;;Kapil Pahuja;;Mark Noonan;;Jensen Lugo Velez;;Carl Thompson	

Kim Sok	Nikita Sujan	Greg Buchanan	
Kim Sok	Nikita Sujan	Michele Bernache;;Greg Buchanan	
Kim Sok	Nikita Sujan	Richard Sarcia (no-access);;Natalya Belozerova (Deleted) (no-access);;Rich Trisoline	

Theresa Lynch		Rich Trisoline	
Theresa Lynch	Timothy Bulman		
Theresa Lynch	Timothy Bulman		

Korelle Foy	James Farrell	Rich Trisoline	
Korelle Foy	James Farrell	Rich Trisoline	
Bernard Mumuluh	Alexander DeSimone	Hiren Thakkar;;Rich Trisoline	
Korelle Foy	James Farrell	Hiren Thakkar;;Rich Trisoline	

Zachary Mucha	Nikita Sujan	Lesley Delaney (no-access)	
Theresa Lynch	Timothy Bulman		
Melissa Trenholm	Theresa Lynch	Timothy Bulman	
Bernard Mumuluh	Alexander DeSimone	James Farrell	

Ollie Bodden	Zachary Mucha	Carli Walsh;;Kellen Affleck;;Maura Feldman (no-access)	

Impacted Controls	Identified By
COOIT.CO.BU.CO3.01 Daily Backup Config;;CORPIT.SOC2.PI.PI1.3_03 Server/DB Daily Backups	Internal Audit
	Management
COOIT.LA.NEW.LA6.06 New Access Request_Salesforce Provider Ops	External Audit

CORPIT.SOC2.SYSOPS.CC7.3_02 System Issue/Incident Tracking	External Audit
FINIT.CM.MIGR.CM05.01 Leader Approval_Finance	Internal Audit
HRIT.LA.RECERT.LA3.08 Access Recert_ADP	External Audit
SALESIT.LA.TRANS.LA4.04 Transferred User Access_BQ/BQi/SF	External Audit

CORPIT.SOC2.PI.PI1.3_01 Tivoli Workload Scheduler Access	External Audit
	External Audit
	External Audit

	External Audit
	External Audit
	External Audit
	External Audit

	External Audit
	External Audit
	External Audit
	External Audit
	External Audit

	External Audit
	External Audit
	External Audit

	External Audit
	External Audit
	External Audit
	External Audit

	External Audit
	External Audit
	External Audit
ARMIT.LA.RECERT.LA3.01 Access Recert_IAM	External Audit

COOIT.LA.PRIV.LA2.01 Privileged Access Recert_SD DB	Internal Audit
COOIT.LA.PRIV.LA2.01 Privileged Access Recert_SD DB	Internal Audit
ARMIT.LA.RECERT.LA3.01 Access Recert_IAM	External Audit

COOIT.LA.TRANS.LA4.03 Transferred User Access_Enterprise Technology;;COOIT.LA.TRANS.LA4.03.a Transferred User Access_Enterprise Technology	External Audit
COOIT.LA.RECERT.LA3.06 Access Recert_Salesforce Provider Ops	External Audit
FINIT.LA.RECERT.LA3.02 Access Recert_BARS_AMS	External Audit

ARMIT.LA.RECERT.LA3.01 Access Recert_IAM	External Audit
ARMIT.LA.RECERT.LA3.01 Access Recert_IAM	External Audit
	External Audit
ARMIT.LA.RECERT.LA3.01 Access Recert_IAM	External Audit
	External Audit
COO.AQC.AQC.AQC.KC.01 AQC Settlement Efficiency	Internal Audit

ARMIT.LA.RECERT.LA3.01 Access Recert_IAM	External Audit
COOIT.CM.TEST.CM04.02 Tested Before Prod_Enterprise Technology	Internal Audit
SALESIT.LA.RECERT.LA3.05 Access Recert_BQ/BQi/SF	External Audit
COOIT.CM.SoD.CM03.02 Change Monitoring and SoD_ Enterprise Technology	External Audit

COOIT.LA.PRIV.LA2.01 Privileged Access Recert_SD DB	External Audit
COOIT.CM.SoD.CM03.02 Change Monitoring and SoD_ Enterprise Technology	External Audit

COOIT.LA.TRANS.LA4.03.b Transferred User Access_Enterprise Technology	External Audit
COOIT.CM.TEST.CM04.02 Tested Before Prod_Enterprise Technology	Internal Audit

SALESIT.LA.TRANS.LA4.04 Transferred User Access_BQ/BQi/SF	External Audit

CORPIT.SOC2.COMM.CC2.2_05 Vendor Risk Assessments	External Audit
ARMIT.LA.NEW.LA6.01 New Access Request_IAM	External Audit
CORPIT.SOC2.ACC.CC6.4_01 Daily Phys Term from TIM/TAM	External Audit
CORPIT.SOC2.ACC.CC6.4_03 Laptop Retrieval	External Audit

COOIT.CM.TEST.CM04.04 Patch Testing	Internal Audit
SALESIT.LA.NEW.LA6.04 New Access Request_BQ/BQi/SF	External Audit
ARMIT.LA.RECERT.LA3.01 Access Recert_IAM	External Audit
	External Audit

	Internal Audit
	Internal Audit
	Internal Audit
	External Audit

	Management
	Internal Audit
	Management

	External Audit
	External Audit

	External Audit
	External Audit

	External Audit
	External Audit
	External Audit
	External Audit
	External Audit
	External Audit

	Internal Audit
	Management
	Management
	Internal Audit

COOIT.CM.SoD.CM03.02 Change Monitoring and SoD_ Enterprise Technology	Internal Audit

COOIT.CM.REQS.CM02.02 Change Approvals_Enterprise Technology;;COOIT.CM.TEST.CM04.02 Tested Before Prod_Enterprise Technology;;COOIT.CM.POL.CM01.02 Program Change Policy/Methodology_Enterprise Technology;;COOIT.CM.SoD.CM03.02 Change Monitoring and SoD_ Enterprise Technology	Internal Audit

	External Audit
COO.AQC.AQC.AQC.KC.01 AQC Settlement Efficiency	Internal Audit

	Internal Audit
ARMIT.LA.NEW.LA6.01 New Access Request_IAM	External Audit
ARMIT.LA.RECERT.LA3.01 Access Recert_IAM	External Audit
	External Audit
COOIT.LA.PRIV.LA2.01 Privileged Access Recert_SD DB	Management

ARMIT.LA.NEW.LA6.01 New Access Request_IAM	External Audit
COOIT.LA.PRIV.LA2.01 Privileged Access Recert_SD DB	External Audit
SALESIT.LA.RECERT.LA3.05 Access Recert_BQ/BQi/SF	External Audit
COOIT.CM.POL.CM01.02 Program Change Policy/Methodology_Enterprise Technology;;COOIT.CM.REQS.CM02.02 Change Approvals_Enterprise Technology;;COOIT.CM.TEST.CM04.02 Tested Before Prod_Enterprise Technology;;COOIT.LA.PRIV.LA2.01 Privileged Access Recert_SD DB;;COOIT.CM.MIGR.CM05.02 Leader Approval_Enterprise Technology	Internal Audit

COOIT.CM.SoD.CM03.02 Change Monitoring and SoD_ Enterprise Technology	External Audit
COOIT.LA.PRIV.LA2.01 Privileged Access Recert_SD DB	External Audit

COOIT.CM.MIGR.CM05.02 Leader Approval_Enterprise Technology;;COOIT.CM.REQS.CM02.02 Change Approvals_Enterprise Technology;;COOIT.CM.TEST.CM04.02 Tested Before Prod_Enterprise Technology	Internal Audit
ARMIT.LA.RECERT.LA3.01 Access Recert_IAM	External Audit
COOIT.CO.JOB.CO2.02 Job Scheduler Access to EDI Eligibility Feeds;;CORPIT.SOC2.PI.PI1.3_06 Job Scheduler Access to PBM Claim Feeds;;COO.VF.LA.VF.LA.03 Job Scheduler Access to modify Airflow	External Audit
ARMIT.LA.RECERT.LA3.01 Access Recert_IAM	External Audit
COOIT.LA.PRIV.LA2.01 Privileged Access Recert_SD DB	External Audit

ARMIT.LA.NEW.LA6.01 New Access Request_IAM	External Audit
	External Audit
ARMIT.LA.NEW.LA6.01 New Access Request_IAM	External Audit
	Internal Audit
COOIT.LA.PRIV.LA2.01 Privileged Access Recert_SD DB	Internal Audit

	External Audit

ARMIT.LA.RECERT.LA3.01 Access Recert_IAM	External Audit
CORPIT.SOC2.ERM.CC3.2_05 Internal Vulnerability Scanning	External Audit
COOIT.CM.TEST.CM04.04 Patch Testing	Internal Audit
CORPIT.SOC2.CTRL.CC5.3_01 OS Security Configuration	Internal Audit

	Management

COOIT.LA.TRANS.LA4.03 Transferred User Access_Enterprise Technology;;COOIT.LA.TRANS.LA4.03.a Transferred User Access_Enterprise Technology	External Audit
FIN.ASC.ASC.ASC.KC.12 ASCBE Error Control	Internal Audit

	Internal Audit
	External Audit
	Internal Audit
	Internal Audit

	Internal Audit
	External Audit
	Internal Audit
	Internal Audit
COOIT.LA.RECERT.LA3.07 SD Monthly Review	External Audit
CORPIT.SOC2.ACC.CC6.1_06 MFA;;CORPIT.SOC2.ACC.CC6.6_01 Remote/VPN Access	Internal Audit
	Internal Audit

	Internal Audit
	Internal Audit
	External Audit
	External Audit
	External Audit
	Internal Audit

ARMIT.LA.RECERT.LA3.01 Access Recert_IAM	Internal Audit
	External Audit
COOIT.CO.DRP.CO4.01 DRP Testing;;ARMEL.EL.EL.ELC-04 BC DR Program	Internal Audit

COO.PHC.PHC.PHC.KC.01 MyPBM Quality Assurance	Internal Audit
	Internal Audit
	Management

	External Audit
	External Audit
	External Audit

	External Audit
	External Audit
	External Audit
	External Audit

	Internal Audit
	External Audit
	Internal Audit
FINIT.CM.MIGR.CM05.01 Leader Approval_Finance	External Audit

COO.AQC.AQC.AQC.KC.02 AQC Settlement Quality	Management

Notes
EY identified a sample user, Lisa Jenkins, whose access was provisioned without the appropriate approval. A ticket on 1/26/2023 was opened by Paula Bailey who is not Lisa Jenkin's leader. Lisa's profile was updated on 1/26/2023, but was then reverted back after realizing that the leader information was incorrect and subsequently closed the ticket. The appropriate leader, Taryn Photos, was then contacted and requested a new ticket for Lisa Jenkins which was done on 1/30/2023. Access to BCBSMA LAN and application data is approved by the associate’s leader. The Security Administrators work with the business leaders to validate the access request and ensure that the application access is in accordance with job responsibilities, and that the request is authorized by the leader.

For 2022, another exception was identified in Q3 2022 and is noted in Priority 1 Incident was not resolved within SLA timeline. (Issue #392)
5/4: initial discussion with Tracy Lehman, potential for escalation reporting to ensure proper closure and documentation. To regroup in 1 week.
per Lori Sheehan - During our discussions after the upgrade from ADP version Ev5 to Ev6, the simplified view of Operators was no longer available in Ev6 and ADP suggested that the operators can be seen in the UTL007 reports. It was requested that management provide screen shots of the screen where we can select operators and provide those by class. When HRIS scrolling down thru the screens to capture shots of the HRIS group I scrolled past KBLAHA so she did not appear.
Q1 2023 Sample: Ewing, Victoria Application: SalesForce PCMS Effective Date: 02/04/23 Associated Canvas Request: Q1 2023 EY IT Audit Request 5 0- Salesforce PCMS Transfers Sample Selections (IT3.2 / ACC.06) Q1 2023 Sample: Harding, Cody Application: SalesForce PCMS Effective Date: 02/04/23 Associated Canvas Request: Q1 2023 EY IT Audit Request 5 0- Salesforce PCMS Transfers Sample Selections (IT3.2 / ACC.06)

SOC2 only control (EY control BUP.07). EY Inspected the annual review of the Tivoli Workload Scheduler and Avamar to determine whether access is restricted to authorized individuals and is revalidated on an annual basis. User Jeff Fortin signed off on his own access.
CAP1 (0105.02a2Organizational.1)
CAP09 (baseline 0627.10h1System.45) CAP10 (baseline 0663.10h1System.7) CAP21(baseline 0643.10k3Organizational.3) CAP27(baseline 0710.10m2Organizational.1) CAP30(baseline 0715.10m2Organizational.8)

CAP11 (baseline 0664.10h2Organizational.10) CAP12 (baseline 0663.10h2Organizational.9) CAP43 (baseline 1196.01l3Organizational.24)
CAP81(baseline 1823.08j3Organizational.12) CAP82(baseline 1824.08j3Organizational.3)
CAP07(baseline 0620.09b2System.3) HiTrust Baseline: Fallback procedures are defined and implemented, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.
CAP29(baseline 0714.10m2Organizational.7) HiTrust Baseline: The technical vulnerability management program is evaluated on a quarterly basis.

CAP31(baseline 0790.10m3Organizational.22) HiTrust Baseline: The organization reviews historic audit logs to determine if high vulnerability scan findings identified in the information system have been previously exploited.
CAP36(baseline 1004.01d1System.8913) HiTrust Baseline: The organization maintains a list of commonly-used, expected, or compromised passwords, and updates the list (i) at least every 180 days and (ii) when organizational passwords are suspected to have been compromised (either directly or indirectly); allows users to select long passwords and passphrases, including spaces and all printable characters; employs automated tools to assist the user in selecting strong passwords and authenticators; and verifies, when users create or update passwords, that the passwords are not found on the organization-defined list of commonly-used, expected, or compromised passwords.
CAP37(baseline 1110.01b1System.5). HiTrust Baseline: Users are given a written statement of their access rights, which they are required to sign stating they understand the conditions of access. Guest/anonymous, shared/group, emergency and temporary accounts are specifically authorized and use monitored.
CAP48(baseline 1313.02e1Organizational.3). HiTrust Baseline: The organization provides incident response and contingency training to information system users consistent with assigned roles and responsibilities within 90 days of assuming an incident response role or responsibility; when required by information system changes; and within every 365 days thereafter.
CAP49(baseline 1334.02e2Organizational.12) HiTrust Baseline: The organization ensures that the senior executives have been trained in their specific roles and responsibilities.

CAP50(baseline 1315.02e2Organizational.67) CAP51(baseline 1304.02e3Organizational.1) HiTrust Baseline: The organization provides specialized security and privacy education and training appropriate to the employee's roles/responsibilities, including organizational business unit security POCs and system/software developers.
CAP52(baseline 1331.02e3Organizational.4) CAP59(baseline 1514.11a3Organizational.12) CAP72(baseline 1810.08b3Organizational.2) CAP73(baseline 1812.08b3Organizational.46) CAP74(baseline 1813.08b3Organizational.56) CAP75(baseline 18145.08b3Organizational.7) CAP76(baseline 18146.08b3Organizational.8) CAP78(baseline 1816.08d2Organizational.4)
CAP67(baseline 1789.10a2Organizational.3). HiTrust Baseline: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of security requirements and controls in developed and acquired information systems.

CAP68(baseline 1791.10a2Organizational.6)
CAP69(baseline 17101.10a3Organizational.6) HiTrust Baseline: The organization requires the developer of the information system, system component, or information system service to provide specific control design and implementation information.
CAP70(baseline 1803.08b1Organizational.5) HiTrust Baseline: Repairs or modifications to the physical components of a facility which are related to security (e.g., hardware, walls, doors and locks) are documented and retained in accordance with the organization's retention policy.
CAP79(baseline 1862.08d3Organizational.3) HiTrust Baseline: Fire authorities are automatically notified when a fire alarm is activated.

CAP83(baseline 19140.06c1Organizational.1)
CAP84(baseline 1908.06c1Organizational.4) HiTrust Baseline: The organization documents and maintains (i) designated record sets that are subject to access by individuals, and (ii) titles of the persons or office responsible for receiving and processing requests for access by individuals as organizational records for a period of six years.
CAP71(baseline 1809.08b3Organizational.1) CAP72(baseline 1810.08b3Organizational.2) CAP75(baseline 18145.08b3Organizational.7) CAP76(baseline 18146.08b3Organizational.8) CAP77(baseline 1815.08d2Organizational.123)
Reviewer: Andrew Moore Associated Canvas Request:EY IT Audit Walkthrough Request - Solutions Development.3.5.a

Rich T updates –
Access Recert – We sent out the requests to the 28 leaders with users that have access to IICS (as of 9/6). This is modeled after our regular QAR process. We will frequently remind the leaders that haven't responded to give us time to remove any access required by the end of the month if not sooner. This review will also include the removal of any users that are terminated.

Transferred users – The Informatica team is reviewing the 9/5 Transfer list. We will reach out to the leaders for any transferred users on the list that may have IICS access and take any necessary actions.

The AD groups have been identified by the Cloud Operations team. The IAM Operations team is in process of identifying which users are in each group as well as which users have been terminated. Once this information is available the DAL application teams will review the users. All users already terminated as well as those that are requested to be removed will need to be removed from the groups.

Q2 2023 Sample: Mark Perigard
Application: Solutions Development
Access Removal Date: 8/1/2023 (Next month's available listing)
Reviewer: Andrew Moore

Mark Perigard continued to be listed with access to the GG-ClaimOpsAdmin group. SOC, Customer Facing

SOC, Customer Facing

Q1 2023 Sample: Lynn Supple
Application: DAL
Effective Date: 3/18/2023
Approver: Jonathan Barron

Q1 2023 Sample: Kim Fountaine
Application: DAL
Effective Date: 3/18/2023
Approver: Jonathan Barron

UPDATE
Q2 2023 Sample: Franco Bueno Mattera
Application: DAL
Effective Date: 4/25/2023
Approver: Yeswanth Poolinkunta
- email to the manager for review upon transfer did not state that the user had DAL PROD access

Q2 2023 Sample: Michaela Witteman
Review Date: 7/20/2023
Removal Date 8/29/2023
Access reviewed by: Wilhelmina Cunningham

Three users were marked as approved when they had been previously terminated. As such EY request to obtained evidence that the users access was appropriate prior to their termination. The confirmation from the users manager can be see below.
Ddulka01 - re-approved by manager msuple01 - Michelle Suplee on 10/24/2023
mmorri02 - re-approved by manager camblo01 - Christina Ambloe on 10/24/2023
spakhi01 - re-approved by manager wbozag01 - William Bozaglu on 10/24/2023

Manager: Tara Fulton The access review assigned to Tara Fulton was completed by Kimberly Young, who reports to Tara Fulton, instead of the review being delegated to Tara Fulton's manager.
Pending information about these system accounts and the users with access to these accounts.
CAP05 (baseline 0618.09b1System.1)
Reviewer: Andrew Moore EY: Received evidence that Andrew's manager reviewed and approved Andrew's access to the group
Whitehead Chelsea (Associate) Term Date 7/24/2023 - RITM0281657 Dembinski Noah (Contractor) Term Date 2/1/2023 - RITM0299516 Thibodeaux Suzann (Contractor) Term Date 10/18/2022 - RITM0239075 Pena-Ortiz Tatiana (Contractor) Term Date 1/6/2023 - RITM0250832 Louismar Maya (Contractor) Term Date 2/13/2023 - RITM0257180 Thimsen Joel (Contractor)Term Date 7/22/2023 - RITM0280527

User EBARNE01 - The user with Core DW access was not reviewed as part of the Q4 recertification and continues to still have access. System id QEDMRPT0 - this ID with QEDM access wasn't reviewed as part of the initial recertification. A ticket was submitted to remove this id's access. System id QEDMAPP0 - this ID with QEDM access wasn't reviewed as part of the initial recertification. The id's access has since been removed.
Salesforce Sales accounts - refer to Canvas request 'BQ/BQI & Salesforce Sales Recertification Walkthrough Request' for the accounts
Per EY: Walkthrough 4/23/2024 (User validation received 4/30/2024): User Vamsi Sanagapally (vsanag02) was identified by the Edifecs Support team manager, Elena Henkin (Senior Manager, Product Management), indicating that Vamsi did not have appropriate access to both of the ess5_eadm_nprd and ess7_eadm_prd regions and needed to have their access removed from the ess7_eadm_prd role. Follow-ups are out to Elena for evidence of access removal, explanation on when access became inappropriate, and activity performed by user Reviewing logs from Rich Update: The following 9 users have access to the ess7_eadm_prd group and the development area in GIT: Divyalakshmi Chandran, Gangareddy Ade, Harshitha Chandrashekhar, Mahesh Mudragaddam, Parthiban Chandran, Riya Gurbani, Sandhiya Bala, Vamsi Sanagapally, Venkat Vemury

6 service accounts: airflow.prd, service account, CAI Anonymous, DAL Support, vendor vendor, iics_dal_api_user.prd Individual account: vbanga01 (initially identified 1); 15 additional identified Questions going out to Rich on other individual accounts that were marked as 'terminated' and the timing of the service account review Received explanation back from Rich that these additional individual accounts were not reviewed due to status issue (terminated vs. active)
6/10 - pending follow-up responses from Rich (developer vs. deployer evidence) 6/17 - evidence received 6/17. EY reviewing 6/24 - some follow-ups on evidence tie out (Q1 2024 EY IT Audit Request # 126 - DAL Change Management Segregation of Duties Additional Evidence) # 328 7/15 - explanation received back from Rich is that some of these changes deployed outside of the pipeline had JIRA tickets only and did not have ServiceNow tickets 7/22 - question is out to Rich on why these did not have ServiceNow tickets and only had JIRA tickets Related to issues: I#509 I#580 I#505

Note that 1 user was identified for Q2 2024 testing - The 2nd user was identified for Q4 2024 testing. Q2 2024: For user Dayie Thomas who had a transfer date of 4/1/2024, their access was not removed until 7/26/2024. EY also inspected a copy of a Deactivated Users Report that was generated on 8/2/2024 by Ashley Leavitt which showed the user's last log in date into the FEP Direct system was 09/29/2023. As a result of this exception, EY expanded the sample size and tested a 100% of the transfer users. Q4 2024: For user Jahne Osorio-Wright, access was not reviewed upon the user's transfer date 11/7/2024. Per inquiry with Ashley Leavitt (Manager II - FEP), the hyphen in the user's last name caused the user to not be captured in the transfer listing for the PSA. The user's transfer review was not performed until 1/27/2025, after the error was identified (after 30 days). Upon EY's selection of the sample, an email was sent to the leader for user's review. Access was confirmed to be appropriate.

Note that 1 user was identified for Q2 2024 testing - see item #25. The 2nd user was identified for Q4 2024 testing.

User Christopher Grant was created as part of BQi and was provisioned Salesforce Commerce access.

EY requested evidence of the transfer review performed for Salesforce Commerce access (not BQi access); no evidence has been provided over the review of Salesforce Commerce access. Evidence provided for BQI access but not commerce access

User's transfer date was 4/27/2024.

EY has the evidence to show that Christopher Grant's access was eventually reviewed and approved by the appropriate reviewer.

10/21 - Meeting held on 10/18 to discuss. EY has the necessary evidence to document the issue.

For the user Matthew Soleyn (msoley01), no transfer review was performed over the user's access in Salesforce Commerce at the time of the transfer.
The user's transfer took place on 10/26/2024 and upon the inspection of Salesforce email action logs, there was no review for the transfer event. EY inspected that the user's access was reviewed on 10/9/2024 as a part of the quarterly review process by the user's manager Mallina Subrahamanyam.

Vendor 'Receivable Management Services LLC - subsidiary of iQor' had its review on 3/19/2024 and reported one risk, which was a high level risk with a remediation due date of 6/19/2024. Due to a manual error logging the risk, the risk was not within the normal reporting query parameters, so it was not remediated within the required 90 days. The error occurred because the IRM analyst, who was recording the risk in ServiceNow, did not check the box that the risk was for TPRM, so it was not reported on for third-party risks from the GRC-IRM team. Evidence to close this risk was received 10/1/2024. Vendor 'Carelon Behavioral Health Inc.' had its review on 4/26/2024 and reported on high-level risk with a remediation due date of 7/26/2024. Per inquiry with Michael Helm (Sr. Informatino Risk Analyst), the identified risk was not reproted internally for follow-up due to a manual entry error causing the risk to not be within the normal risk reporting query parameters. BCBSMA later contacted the vendor and learned that the vendor had remediated the risk but had not communicated that to BCBSMA. EY inspected that the risk was remediated and closed on 11/1/2024 after BCBSMA received evidence from the vendor.
User Matthew Soleyn was provisioned temporary admin access on 5/9/2024 and was requested to have access until 5/23/2024. Per inspection of the user's AD access, the user still had temporary admin access until 10/17/2024. 10/24: EY requested evidence of Matthew Soleyn's activity log starting from 5/9/2024 to 10/17/2024.
Per Donnie Kyne, user Francyne Lee never started at BCBSMA. However, this user's profile was created on 11/13/2023, which was her planned start date. Even though this user was included in the daily Workday email to remove badge access, their access was only disabled three months later due to inactivity.
BCBSMA did not recover the laptops of 9 users after those users were terminated, and the Intune Remote Wipes for these laptops are all still pending months after the users were terminated. Per Walter Endyke (Associate Director Desktop Engineering & Support), the remote wipe activity is a command issued from Intune over the internet. Because it relies on internet, if the laptops never connect to internet, the wipe will not execute and will remain listed as 'pending'. One (1) of 9 exceptions was listed as 'Intune wipe failed'. Per inquiry with Walter, BCBSMA took every available action to recover the device and attempt a remote wipe, but will ultimately list the item as 'stolen' and close the ticket. The hard drive on the laptop is encrypted and all accounts related to the user and machine have been disabled.

Saval Pathak was provisioned access to the Salesforce Sales Instance 'System Administrator' profile and role after Saval's manager Jesus Garcia approved reactivation of Saval's account on 11/4/2024. Saval was provisioned the same 'System Administrator' access in August 2023, but this access was deactivated in Q1 2024. In his Q4 2024 approval, Jesus Garcia did not specify what role and profile Saval was to be provisioned. EY expanded Q4 2024 testing by 10 samples (tested 20 total instances of new access in 2024) and did not identify any additional exceptions.
For the recertification performed for Solutions Development intended for the month of October, EY identified that the user listing was generated on 10/1/2024 for review but the final review was not performed timely as the October review was signed by Andrew Moore on 11/21/2024, more than halfway through the subsequent month. User UdayTeja was marked to be reviewed on 11/21/2024 and had access revoked on 11/22/2024. As the user's access was removed beyond 30 days since 10/1/2024, we requested evidence of the user's activity log. We received evidence from PAM that the user's account was disabled and that there was no access of history since the account's creation on 9/4/2024.

discussion date of 7/12/22 = date of Risk committee meeting in which VPs and above were informed of actions needed.
the 7/12/22 discussion date was the Risk Committee date in which the findings were discussed with VPs and above. We will reconvene at Risk Committee in October 2022 for status updates.
Related to issues: I#505 I#580 I#509
Specialty Pricing - PwC identified 1,873 discrepant specialty claims that were not cleared in the initial inquiry to ESI. A sample of these claims have been sent to ESI for follow up research. The claims in question were filled at BCBSMA's custom specialty pharmacies and were subject to a custom specialty guarantee. The total shortfall for these claims is $481,481. ESI researched the claims and agreed that that the claims did not adjudicate in accordance with the specialty list provided and should it be determined that the system was not set up correctly, ESI will review whether adjustments are needed.

11 CAPS:
CAP06(baseline 0619.09b2System.12)
CAP08(baseline 0626.10h1System.3)
CAP13(baseline 0606.10h2System.1)
CAP14(baseline 0629.10h2System.45)
CAP15(baseline 0635.10k1Organizational.12)
CAP16(baseline 0671.10k1System.1)
CAP18(baseline 0637.10k2Organizational.2)
CAP19(baseline 0638.10k2Organizational.34569)
CAP20(baseline 0639.10k2Organizational.78)
CAP23(baseline 0672.10k3System.5)
CAP28(baseline 0713.10m2Organizational.5)

CAP04(baseline 0425.01x1System.13)
HiTrust Baseline: A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing entity (client) or cloud service provider-managed client data, and the use of unapproved application stores is prohibited for company-owned and BYOD mobile devices. Non-approved applications or approved applications not obtained through approved application stores are prohibited.

CAP24(baseline 0701.07a1Organizational.12) HiTrust Baseline: An inventory of assets and services is maintained.

CAP26(baseline 0706.10b1System.12)
HiTrust Baseline: Applications developed by the organization are based on secure coding guidelines to prevent common vulnerabilities or undergo appropriate testing.

CAP35(baseline 1031.01d1System.34510) HiTrust Baseline: The organization changes passwords for default system accounts, whenever there is any indication of password compromise, at first logon following the issuance of a temporary password, and requires immediate selection of a new password upon account recovery.
CAP39(baseline 1111.01b2System.1)
CAP41(baseline 1168.01e2System.2) HiTrust Baseline: The organization reviews critical system accounts and privileged access rights every 60 days; all other accounts, including user access and changes to access authorizations, are reviewed every 90 days.
CAP45(baseline 11126.01t1Organizational.12) HiTrust Baseline: A time-out mechanism (e.g., a screen saver) pauses the session screen after 15 minutes of inactivity, closes network sessions after 30 minutes of inactivity, and requires the user to reestablish authenticated access once the session has been paused or closed; or, if the system cannot be modified, a limited form of time-out that clears the screen but does not close down the application or network sessions is used.
CAP46(baseline 1240.09aa2System.56) HiTrust Baseline: The organization provides a rationale for why the auditable events are deemed adequate to support after the fact investigations of security incidents and which events require auditing on a continuous basis in response to specific situations; and the listing of auditable events and supporting rational are reviewed and updated periodically within 365 days.
CAP65(baseline 1794.10a2Organizational.12) HiTrust Baseline: When developing software or systems the organization performs thorough testing and verification during the development process.

Ananth KS and Gazula Srikanth were logged as both change developer and approver.

Users were Senior Developers who initiated the change to assist with a developer's code migration who lacked access to initiate the change at that point in time. CAB performs a review of all changes before being promoted into production.

Related to issues:
I#509
I#580
I#339

For the Q1 - Q3 2023 period, the completeness of the population of changes for the Data Access Layer (DAL) application from the ticketing system could not be validated for the period as evidence to reconcile the manually created tickets to the production source was not available which could result in an incomplete or inaccurate population. For the Q4 2023 period, the completeness of the population of manually deployed changes for the Data Access Layer (DAL), outside of the pipeline, could not be validated for the period as evidence to reconcile the manually created ticket to the production source was not available which could result in an incomplete or inaccurate population.

Update: For the Q4 2023 - Q1 2024 period, the completeness of the population of manually deployed changes for the Data Access Layer (DAL), outside of the pipeline, could not be validated for the period as evidence to reconcile the manually created ticket to the production source was not available which could result in an incomplete or inaccurate population.

74 individuals with the ability to deploy DAL changes manually outside of the pipeline have development responsibilities, creating a segregation of duties concern. - Moved to separate issue I#579

Q1 2023 - Q3 2023: no evidence from source system for the completeness of the population

Q4 2023: follow-ups remain outstanding on users who can deploy changes manually.

As of 4/22 - follow-up sent to Rich on 1 change; pending full list with tieout from Informatica log to change ticket information.

4/29 - received updated file to cover through 12/31/2023

5/6 - will need evidence for 2024

6/3 - received evidence. reviewing

Common themes seen in Corporate financial statement audit and EBP Audits listed below: Refer to file path: P:\Audit\Tri-Audit\! Financial Operational Audit\MAR\2023 MAR DOCS\Pension\1. Carryforward\Historical Issues with participant data

Corporate Audit Findings from 2022, 2020 and 2018:

- 2022 Corporate Audit - RWBP Census file had one participant that were incorrectly included in the census. (2022 Corporate Audit - RWBP census data folder)

- 2020 Corporate Audit - RWBP Census file - there were different assumptions that both EY and Mercer had on what participants should be included in the participation. EY assumed all eligible retirees regardless of whether they've commenced their benefit or not should be included in the population to ensure we weren't grossly understating the post retirement obligation on our financials but Mercer disagreed given that there is a low rate of eligible retirees returning to commence their benefits. As a result, Mercer performed a 5 year experience study between 2016 to 2020 to prove out the low rate of return. Based on that study, they are setting the participation assumption at 80% to account for pre 2022 retirees who are still able to opt in to the plan as well as the potential increase in immediate participation upon retirement for post 2021 retirees who will not have the option to participate later. Note that effective January 1, 2022, new retirees will no longer have the option to opt in to PRB benefits if they do not elect to participate within 30 days of termination.

- 2018 Corporate Audit - RWBP Census file had 22 participants that were incorrectly included in the census.

Employee Benefit Plan Audit Findings:

2022 Audit Year - Retiree Contributions were calculated incorrectly for one participant. To give some background, Benefit Concepts was our vendor in 2019 and it looks like they didn't perform the calculation of the subsidy correctly and it was carried forward each year. WEX Health is now our vendor as of 2020 (used to be called Discovery Benefits).

Since there should have been a recovery, but no business area submitted a request, there appears to be a gap in the process. It is unclear who should be responsible for submitting the request. TBD on total impact For more details, see wps "A.2.0" and "A.2.20b & 22b" here: J:\Audit\Tim Bulman\3. BCBS Association\FEP DO\Control Self Assessments\2023 Assessments (scope 10.1.22 through 9.30.23)\Overpayment\Prevention Protocols\A.2 Pricing File Updates
User: Suman Dutta Access role: Core_DW, QEDM; POWERUSER, QUERYUSR Access aproval date for QEDM: 10/17/2023 The user Suman Dutta has two new access roles within the listings QWDM & DW. However, no access request and approval were provided for the DW role.
Rebecca Blyth - had BQ access per the BQ user listing. Other access was reviewed but for BQ access the recertification results said 'No access' when the user did have BQ access. Michaela Witteman - had BQI access per the BQI user listing. Other access was reviewed but for BQI access the recertification results said 'No access' when the user did have BQI access.
ESI agrees with the finding and will be crediting BCBSMA.

User Elansuriyan Selvaraju (eselva01) was requested to have DAL non-production access. The user was provisioned production access instead of non-production access. Received confirmation from user's manager that access is appropriate
3 service accounts: admin, distributionlist_fkm, engine_user Following up with Ryan to confirm that they were not reviewed. Ryan had indicated that there were no Ataccama service accounts Ryan confirmed that these were not reviewed
BQI - Web Sales BCBSMA account
• s3://bcbsma-dal-prod-repl-97d4/data-views/fm_transfer/tgt_claim/ • s3://bcbsma-odh-prod-inbound-49f0/raw/claims/ Per call on 8/8/2024: S3 reporting complete - report uploaded to Action Plan. Mahes to provide script used to generate report S3 change logging retention pending Rapidcsale ticket Update 10/8: Per discussion, implementation pending cost analysis. This may be able to be done in Splunk.

Twelve (12) users were identified having access to both the deployer role ('APP_ACCESS_DAL_Prod_PADMIN_GROUP' admin role) and the developer role ('APP_ACCESS_DAL_Prod_Developer_GROUP') as of 5/31/2024. Received explanation back from Ryan that there was an issue with the job that generated the report of users both admin and developer roles and has since been updated (list as of 6/20/2024 shows update) - (Canvas request EY IT 2024 WT Request - DAL ODH.1.12.a). Open questions to Ryan on what users with access to both of these groups have the ability to do - to discuss with AD on 7/22   Related to issues: I#509 I#505 I#339
6 Abacus accounts: Farhan Faisal, Franco Mattera, Lynne Supple, Muazzam Ali, Peter Butler, and Shobin Antony Based on discussion with Ryan, they were later able to get an updated listing from the vendor showing the users with access. Ryan and his team were using an internally owned listing to identify users with access. 4 of these users were not on the internal list and 2 were listed as not having access on the internal listing so they were not included. Explanation from Ryan is that they have reached out to Abacus for removal of the users. Received evidence of removal - EY has a question out on the activity for one of the users with activity from February 2024. Received response for appropriateness of access.   Final SOC report issue: For two (2) (QI 2024 and Q2 2024) of three (3) quarterly reviews sampled, 12 of 46 (Q1 2024) and 12 of 47 (Q2 2024) total Abacus accounts were not included in the review.

For one user, 'insights integration', was not included in the Q2 Salesforce Commerce recertification. Per inquiry with Malar, the Insights Integration account is a user record created by Salesforce and no one can edit this user record; the profile and role assigned to this user record is specific to the user record only. EY is reviewing Malar's response to provide clarification as to why the account was not included in the recertification Question sent to Malar on 8/9 regarding the creation of the accounts
1 user account: Bulleddula Rajesh (rbulle01) was marked for access removal but access was not removed per the 6/26/2024 listing. EY received evidence to show that the user did not perform any inappropriate activity and was subsequently removed.
User Brandon Bathalon (bbatha01) was requested to have their access to global group GG-IACoE-Dev-SQL_Admin removed as part of the Q1 2024 review that was conducted on 2/6/2024, but was not removed as of 5/29/2024. Received evidence from Rich showing the BSSID05VW activity log (the GG-IACoE-Dev-SQL_Admin grants access to the BSSID05VW server) for user bbatha01 and showed that there was no activity from 5/30/2023 to 5/29/2024. Received evidence from Rich showing the BSSID05VW activity log (the GG-IACoE-Dev-SQL_Admin grants access to the BSSID05VW server) for user bbatha01 and showed that there was no activity from 5/30/2023 to 5/29/2024.
Users cbucke05, jmason03, and mstaph01 were not included in the review process - they were included on the screenshots of users with access but did not on the team's internal Excel sheet used to identify users to be recertified. Received evidence confirming the user's appropriateness as of July / August. Evidence under EY review

Users Daniel Tran was given Sales Representative access instead of Underwriter access Underwriter access was requested and approved. Question out to Elise on root cause and on evidence of the updated user listing
User Manickam Kasi (mkasi01) was requested to have Data Warehouse non-production access (the PDWAPPRP_TEST and PDWETL_DEV databases). The user was provisioned production access (CORE_DW; POWERUSR, QUERYUSR) instead of non-production access. 9/16 - Requested evidence for the removal of the user's access, as well as evidence for the user's activity log to validate if there was any activity performed while the user had the inappropriate access
In JSON Inline Policy "/*" is full access to resource for the associated group PutObject - allow users to write data to bucket

CRITERIA:

FAM Vol. III, Chapter 4, Document 4133 – Goods and Services Acquired from Plan Organizations, states, "Some Plans may contract with other Plan organizations for supplies or services used to administer the Federal Employee Program…. This section defines the cost allowable for the FEP contract when the services of internal business units, subsidiaries, affiliates, or a sister Plan organization are used."
FAM Vol. III, Chapter 4, Document 4134 – General Policy, states, "Plan organizations may agree to provide goods or services to each other at prices that include a profit element. However, neither party may charge any of the profit to FEP, absent one of the exceptions discussed below.
Plan organizations must maintain adequate accounting records to determine the cost of the supplies or services being purchased by the Plan. The standard for the adequacy of the Plan organization's accounting records is whether they are adequate for OPM and other external auditors to verify the cost of the services."

FAM Vol. III, Chapter 4, Document 4135 – Policy Exceptions, states, "Plans may charge employee health insurance and other types of insurance purchased from Plan affiliates for the amounts of premiums paid if the Plan is rated using the same underwriting and actuarial formulas as other locally underwritten groups.
The amount allowable for FEP for other goods and services may be at a price different than cost when all of the following requirements are satisfied:
- It is the established practice of the transferring organization to price interorganizational transfers at other than cost for commercial work of the contractor or any division, subsidiary, or affiliate or other type of Plan organization; and
- OPM has not determined the price to be unreasonable. This determination is made through an audit or during OPM's advance notice and consent procurement process, if applicable. Advance determination is not required unless OPM's advance notice and consent process applies; and
- The item being transferred qualifies for an exception from the submission of cost and pricing data. The two most common exceptions are:
  - A determination that the price is based on adequate price competition;

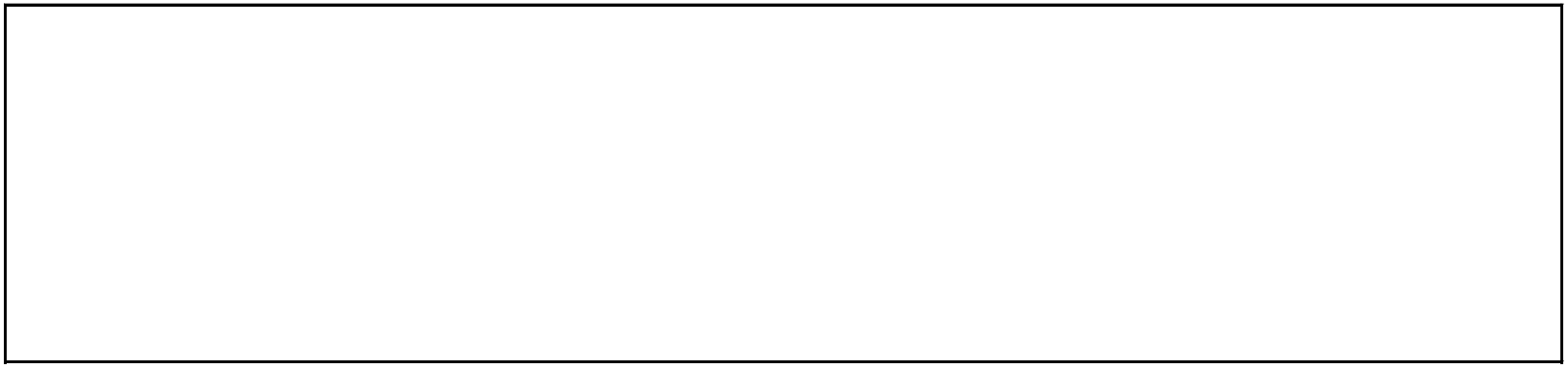
For RTMS samples with IDs QZ0N5X and DZJW53, we see on the recertification results that these were tagged as 'APP_OWNER_REV - NO_NACOS_REC (VALIDATE OR REMOVE)', did not have employee / contractor name details on the results, and appear to be marked as 'VALID' by Cindy McKinnon. However, on the 8/9/2024 RTMS user listings, we see that these IDs correspond to Nancy Stanton and Trachelle Williams, who are showing as terminated individuals with 2023 end dates on the Active Inactive report.

Per Bessie Ezuma-Ngwu, the referenced RTMS sample IDs QZ0N5X and DZJW53 are RTMS accounts not associated with an identity at the time of recertification, where no active EIN/LAN IDs were found. The accounts were reviewed by application owner Cindy McKinnon, but the recertification results did not identify an identity associated with the RTMS IDs.

Given that there are no identities associated with the RTMS IDs, an issue is being noted regarding the precision of the review performed by the app owner.

For the vulnerabilities listed below, the target SLA of 90 days were missed:
- VIT0051197 was resolved in 161 days
- VIT0165560 was resolbed in 135 days.
- VIT0244963 was unresolved as of 11/12/24
- VIT0255911 was resolved in 167 days
- VIT0698840 was unresolved as of 11/12/24

Update 1/21/2025: Rich to review ownership of IPE for 2024 DB patching.



Transferred user Peter Lakin had a transfer date of 11/21/2024, and Peter Lakin's manager, Sheila Gordon, approved the user's access to applications IPRO and SNOWFLAKE_ACCESS through email on 11/27/2024. This email did not include approval for Peter Lakin's access to CORE_DW for the Data Warehouse application. As such, Peter's access was not reviewed within 30 days of his transfer date. Upon inquiry with Sheila Gordon on 2/14/2025, she confirmed that Peter Lakin was approved to have CORE_DW access after his transfer, but the review was performed after 30 days from his transfer date.

EY expanded its Q4 testing population to 100% of transferred users (13 additional users; 16 total in Q4). Eight of the thirteen additional selections' DW and/or DAL access were reviewed by their managers in February 2025, more than 30 days after their Q4 2024 transfer dates:
- Ivan Fernandez transferred 10/12/2024. Access review email was sent 2/19/2025 and Emily Nangle approved CORE_DW access 2/19/2025.
- Rajan Frantz transferred 10/26/2024. Access review email was sent 11/4/2024 but did not include CORE_DW. Follow-up approval email sent on 2/19/2025 and Daniel Tran approved CORE_DW access on 2/19/2025.
- Xiaoxin Chen transferred 10/12/2024. Access review email was sent 10/22/2024 but did not include CORE_DW. Follow-up approval email sent on 2/19/2025 and Michael Mangini approved CORE_DW access on 2/20/2025.
- Bhumika Kamani transferred 10/12/2024. Access review email was sent 2/19/2025 and Michael Mangini approved CORE_DW access from October 2024 - January 2025 on 2/19/2025.
- Abiodun Akogun transferred 10/12/2024. Access review email was sent 10/22/2024 but did not include CORE_DW. Follow-up approval email sent on 2/19/2025 and Michael Mangini approved CORE_DW access on 2/20/2025.
- Jennifer Karampatsos transferred 11/23/2024. Access review email was sent 11/27/2024 but did not include CORE_DW. Follow-up approval email sent on 2/19/2025 and Kelli Callahan approved CORE_DW access on 2/20/2025.
- Kyle Florence transferred 10/12/2024. Access review email was sent 2/19/2025 and Michael Mangini approved CORE_DW access on 2/20/2025.
- Abiodun Akogun transferred 10/12/2024. Access review email was sent 10/22/2024 but did not include CORE_DW. Follow-up approval email sent on 2/19/2025 and Michael Mangini approved DAL_PROD_ACCESS access on 2/20/2025.

This risk is being addressed as IA is regrouping with all ASC Billing control owners to confirm controls and control details.

Rebates: SBG found that CVSH's initial reconciliation of the minimum rebate guarantees incorrectly categorized claims having Days' Supply between 35 and 83 into the Retail-30 channel instead of the Retail-90 channel, which has a higher per-claim rate. CVSH's standard channel designation logic classifies claims having Days' Supply of 84+ as Retail-90; however, BCBSMA's MAPD contract defines claims with Days' Supply of 35+ as Retail-90. SBG submitted 6 samples representing 11,234 claims with this discrepancy, and CVSH confirmed that the incorrect Retail-90 Days' Supply logic had been applied. CVSH's revised reconciliation of $63,279,246 aligns 99.9% with SBG's $63,337,980 minimum guarantee calculation. Although the revised calculation increased CVSH's reported guarantee by over $2.1M, there is no financial impact for this audit period because the overall rebates collected exceed the minimum guarantee. Discounts: SBG found that CVSH incorrectly applied their standard Retail90 logic to the National Network discount and dispensing fee guarantee pricing channel definitions. SBG also found that for both the Liberty and National Network, CVSH incorrectly excluded claims for Paxlovid and Lagevrio under Vaccine Exclusion logic and incorrectly included 340B and reversal claims in the discount and dispensing fee reconciliation. Due to overperformance offsetting, SBG does not estimate that these errors would result in additional dollars being owed to the plan. However, SBG recommends that CVSH implement appropriate corrective measures to ensure that the correct Retail90 logic is applied to BCBSMA's pricing reconciliation and as well as the correct application of claim inclusion and exclusion.

I#625
I#509 | DAL System Changes are not logged and monitored. | Pending Remediation
I#562
I#333
Andrew Moore requested through email that Carolyn Robinson approve Gokul Baskaran's GG-ClaimOpsPAM group access on 2/4/2025 as part of the February review. Per inspection of the evidence, Carolyn did not provide a response for the February review until 4/25/2025. EY inspected that Carolyn Robinson provided a response on 4/25/2025, stating that Gokul should not have GG-ClaimpsOpsPam and only 'GG-ClaimsOpsAdmin' was required. Andrew Moore confirmed that Gokul's access to PAM was removed as of 4/28/2025. Follow-ups out for activity log/evidence of access removal Access removed on 3/3/2025. Some additional follow-ups out on activity logs
#333

I#685
number of affected members is very small, but this is a compliance issue

BNTZP04Z(PROD ETL) "Netezza Transformation". cp4d appliance

Last Date of Mgmt Response
9/5/22

Date Remediation Completed - TBD

Application does not have a Disaster Recovery Plan (migration is in progress to AWS cloud). Procedure for system recovery is updated, tested periodically, and meets the business requirements set forth in the Disaster Recovery Plan.

Per CVS and as a mitigating factor, there is a history/audit trail screen on MyPBM that would note any benefit changes. However, using the history screen requires manual inspection and may be difficult to identify when there are changes after the QC.
As of 6/26, Maryjo needs to be added to AB and tagged to this AB issue/action plan. She is currently the owner of the QC for OLB. As part of EY's substantive procedures relating to BAFA earned premiums, EY needs to trace their premium samples to customer agreements or support showing mutual agreement between account/member and BCBSMA on agreed upon rates. The National and Commercial segments do not have a standardized way of saving account confirmation of rates. This support is currently in the respective AE's mailbox as opposed to it being centralized in one place for all AEs. When IA is able to perform an end to end review of BARS and the overall Sales process, this gap needs to be considered. This new ask (tracing premium selections to customer agreements) was raised by EY as part of the 2024 FS audit and will be part of their requests going forward.

See CVS Impact Analysis here: J:\Audit\Tim Bulman\1. CMS Audits\1. CMS Financial Audits\9. S2893 Financial Audit_2023 (2021 base)\5. Info Requests\NEJE MSP Impact Analysis.zip\NEJE MSP Impact Analysis
Final CMS report to be rec'd in mid Sept. CMS treatment of finding is TBD.

CAP02 (baseline 0116.04b3Organizational.1)
CAP03 (baseline 0209.09m3Organizational.7) CAP44 (baseline 1197.01l3Organizational.3)
CAP25(baseline 0704.07a3Organizational.12) HiTrust Baseline: Organizational inventories of IT assets are updated during installations, removals, and system changes, with full physical inventories performed for capital assets (at least annually) and for non-capital assets.
CAP38(baseline 1139.01b1System.68) HiTrust Baseline: Account types are identified (individual, shared/group, system, application, guest/anonymous, emergency and temporary), conditions for group and role membership are established, and, if used, shared/group account credentials are modified when users are removed from the group.

Management will not change its process, accepting the risk of non-compliance with the FEP contract.
Change (CHG0144663) was retroactively approved through monitoring; meeting minutes show discussion of change but no evidence of an approval before Prod deployment

Due to the HPV error, SSID HMO settlement was reissued. The business noted, there was no financial impact to the settlement due to the error.

Root Cause	* No. of Exceptions in Sample/Control	Identified Date	* Explanation for Deficiency Level	Mitigating Controls
Documentation issue	1	2022-08-01		
Ineffective oversight		2023-02-15		
Process/Control gap	1	2023-03-01		#COOIT.LA.RECERT.LA3.06: Access Recert_Salesforce Provider Ops

Vendor control gap	1	2023-02-06		
Documentation issue;;Process/Control gap		2023-05-04		
Manual process	1	2023-05-08		
Manual process	2	2023-05-15		

Process/Control gap	1	2023-05-15		
Process/Control gap		2023-06-04		
		2023-05-26		

		2023-05-26		
		2023-05-26		
		2023-05-26		
		2023-05-26		

		2023-05-26		
		2023-05-26		
		2023-05-26		
		2023-05-26		
		2023-05-26		

		2023-05-26		
		2023-05-26		
		2023-05-26		

		2023-05-26		
		2023-05-26		
		2023-05-26		
		2023-05-26		

		2023-05-26		
		2023-05-26		
		2023-05-26		
Manual process	1	2023-05-22		

		2023-08-24		
		2023-08-01		
Manual process	1	2023-09-11		

Manual process	3	2023-09-22		
Manual process	1	2023-10-10		
Manual process	3	2023-10-10		

Ineffective oversight;;Process/Control gap	2	2023-10-23		
Process/Control gap	44	2023-11-09		
		2023-05-26		
	1	2024-01-22		
		2023-11-30		
		2024-02-15		

	3	2024-02-20		
	1	2024-03-06		
	21	2024-03-18		#SALESIT.LA.NEW.LA6.04 #SALESIT.LA.TERM.LA5.04
	1	2024-05-29		#ARMIT.LA.RECERT.LA3.01

	6	2024-06-03		#ARMIT.LA.TRANS.LA4.01 #ARMIT.LA.TERM.LA5.03
	74	2024-07-15		#COOIT.CM.REQS.CM02.02

	2	2024-07-29		#ARMIT.LA.RECERT.LA3.01
	3	2024-07-30		

	2	2024-09-30		#SALESIT.LA.RECERT.LA3.05

	1	2024-09-18		#CORPIT.SOC2.COMM.CC2.2_05
	1	2024-10-28		#ARMIT.LA.RECERT.LA3.01
	1	2024-10-28		none
	9	2024-10-28		#ARMIT.LA.TERM.LA5.03

		2024-12-13		
	1	2025-03-20		#SALESIT.LA.RECERT.LA3.05
	1	2025-02-26		
		2025-04-07		

Ineffective oversight;;Manual process;;Process/Control gap		2022-07-12		
Ineffective oversight	2	2022-07-06		
Process/Control gap	3	2022-06-01		
Vendor control gap		2022-11-17		

System limitation;;Ineffective oversight;;Manual process;;Process/Control gap		2022-12-12		
System limitation;;Manual process;;Process/Control gap		2023-01-01		
Documentation issue;;Ineffective oversight;;Process/Control gap		2022-12-12		

		2023-05-26		
		2023-05-26		

		2023-05-26		
		2023-05-26		

		2023-05-26		
		2023-05-26		
		2023-05-26		
		2023-05-26		
		2023-05-26		
		2023-05-26		

Ineffective oversight		2023-10-25		
Control not followed	100	2023-10-25		
Ineffective oversight		2023-10-25		
Ineffective oversight		2023-10-25		

Process/Control gap	2	2023-09-29		#COOIT.CM.REQS.CM02.02

Process/Control gap		2023-11-27		

	1	2024-01-25		
	0	2024-02-15		

	1	2024-02-06		
	1	2024-02-19		
	2	2024-02-19		
		2024-02-12		
		2024-04-15		

	1	2024-05-20		#ARMIT.LA.RECERT.LA3.01
	3	2024-06-03		No mitigating controls
	1	2024-03-18		#SALESIT.LA.TRANS.LA4.04 #SALESIT.LA.TERM.LA5.04
		2024-05-23		

	12	2024-07-15		
	12	2024-07-15		#ARMIT.LA.TERM.LA5.03 #ARMIT.LA.TRANS.LA4.01

	1	2024-08-01		#COOIT.CM.SOD.CM03.02
	1	2024-08-05		#ARMIT.LA.NEW.LA6.01
	1	2024-07-29		#ARMIT.LA.NEW.LA6.01
	1	2024-06-26		none
	3	2024-08-12		#ARMIT.LA.TERM.LA5.03 #ARMIT.LA.TRANS.LA4.01

	1	2024-08-12		#ARMIT.LA.RECERT.LA3.01
		2024-04-23		
	1	2024-09-16		#ARMIT.LA.RECERT.LA3.01
		2024-09-18		
		2024-09-19		

		2024-10-16		

	2	2024-10-28		#ARMIT.LA.NEW.LA6.01
	5	2024-11-18		
		2024-12-31		
		2024-12-16		

	0	2025-02-07		

	9	2025-02-17		#ARMIT.LA.RECERT.LA3.01
	12	2024-11-14		

	1	2025-03-05		
		2025-02-25		
		2023-12-11		
		2023-12-11		

		2025-02-14		
		2024-09-30		
		2024-10-31		
		2024-09-30		
		2022-09-30		
	2	2025-05-05		
		2025-05-20		
		2025-05-23		

		2025-05-23		
		2025-06-05		
		2025-04-07		
		2025-04-07		
		2025-04-07		
		2025-06-26		

		2025-06-26		
System limitation		2020-09-17		Key control is that we do not pay FEP claims until they have been approved by the FEPDO
Ineffective oversight	2	2022-06-01		

System limitation	0	2022-11-07		As a mitigating factor and per CVS, there is a history/audit trail screen on MyPBM that should note any benefit changes but this would require manual inspection.
Documentation issue;;System limitation;;Ineffective oversight;;Manual process;;Process/Control gap	0	2022-12-16		
Manual process;;Process/Control gap		2022-12-19		

Vendor control gap		2023-03-10		
Vendor control gap;;Ineffective oversight		2023-07-21		
Ineffective oversight		2023-05-12		

		2023-06-12		
		2023-05-26		
		2023-05-26		
		2023-05-26		

	0	2025-01-09		
		2018-09-18		
		2025-02-28		Regardless of whether BCBSMA has recuperated the overpayment amount from the provider, FEP receives the full recovery amount automatically each month.
	1	2025-04-14		#FINIT.CM.SOD.CM03.01

	0	2024-12-05		

Business Objective	Risk Level	* Deficiency Type	IA Validation Date	Impact
	Moderate	Issue		Operational
	Moderate	Issue		Compliance;;Member
	Moderate	Control Exception		Information Security

	Moderate	Control Exception		Operational;;Information Security
	Moderate	Issue		Information Security
	Moderate	Control Exception		Information Security
	Moderate	Control Exception		Information Security

	Moderate	Control Exception		Information Security
	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security

	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security;;Operational
	Moderate	HiTrust Cap		Information Security

	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security

	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security

	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security

	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security
	Moderate	Control Exception		Information Security

	High	Issue		Information Security
	High	Issue		Information Security
	Moderate	Control Exception		Information Security

	Moderate	Control Exception		Information Security
	Moderate	Control Exception		Information Security
	Moderate	Control Exception		Information Security

	Moderate	Control Exception		Information Security
	Moderate	Control Exception		Information Security
		HiTrust Cap		Information Security
	Moderate	Control Exception		Information Security
	Moderate	Control Failure		Information Security
	Low	Issue		Reputational;;Financial;; Operational;;Provider

	High	Control Exception		Information Security
	High	Control Exception		Information Security
	High	Control Exception;;Control Failure		Information Security
	Moderate	Control Exception		Compliance;;Information Security

	Moderate	Control Exception;;Control Failure		Information Security
	Moderate	Control Exception		Information Security

	Moderate	Control Exception;;Control Failure		Information Security
	Low			Information Security

	Moderate	Control Exception		Information Security

	Moderate	Control Exception		Information Security
	Moderate	Control Exception		Information Security
	Moderate	Control Exception		Information Security
	Moderate	Control Exception		Information Security

	Low	Issue		Compliance;;Information Security
	High	Control Exception		Compliance;;Information Security
	High	Control Exception		Compliance;;Information Security
	Observation			

	High	Issue		Member;;Reputational;;Compliance
	High	Issue		Account;;Member;;Reputational;;Compliance
	High	Issue		Information Security;;Operational;;Reputational
	Moderate			Account;;Financial

	High	Issue		Account;;Compliance;;Member;;Operational;;Reputational
	High	Issue		Compliance;;Member;;Provider
	High	Issue		Account;;Compliance;;Member;;Operational;;Reputational

	Moderate			Information Security
	Moderate	HiTrust Cap		Information Security

	Moderate	HiTrust Cap		Operational;;Information Security
	Moderate	HiTrust Cap		Information Security

	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security

	High	Issue		Operational
	Moderate	Control Failure		Information Security
	Moderate	Issue		Information Security
	High	Issue		Compliance

	Moderate	Control Failure		Information Security

	Moderate	Issue;;Control Failure		Information Security

	Moderate	Issue		Compliance;;Financial;;Reputational
	Moderate	Issue		Operational;;Financial;;Reputational;;Provider

	Low	Issue		Compliance;;Financial;;Provider
	Moderate	Control Exception		Information Security
	Moderate	Control Exception		Information Security
	Moderate			Compliance;;Financial
	Moderate	Issue		Compliance;;Information Security

	Moderate	Control Exception		Compliance;;Information Security
	Moderate	Control Exception;;Control Failure		Information Security
	Moderate	Control Exception		Information Security
	Low	Issue;;Control Exception		Information Security

	Moderate	Control Failure		Information Security
	Moderate	Control Exception;;Control Failure		Information Security

	Moderate	Control Exception		Information Security
	Moderate	Control Exception		Information Security
	Moderate	Control Exception		Information Security
	Moderate	Control Exception		Information Security
	Moderate	Control Exception;;Control Failure		Information Security

	Moderate	Control Exception		Information Security
				Compliance;;Financial
	Moderate	Control Exception		Information Security
	Moderate			Information Security
	High	Issue		Information Security

	Low	Issue		Compliance

	Moderate	Control Exception		Information Security
	Moderate	Control Exception		Information Security
	Low	Issue;;Control Exception;;Control Failure		Information Security
	Low	Issue		Compliance;;Information Security

	High	Issue;;Control Failure		Compliance;;Information Security
	Moderate	Control Exception		Account;;Financial;;Operational

	Low	Control Failure		Compliance;;Financial
	Low	Issue		
	High			
	Moderate			

	Observation			Operational
	Low			Compliance;;Information Security
	Moderate			Compliance;;Operational
	Moderate			Operational
	Moderate			Operational
	Moderate	Control Failure		Information Security
	Moderate	Issue		Information Security
	Moderate			Compliance;;Financial;;Member;;Operational;;Provider;;Reputational

	High			Compliance;;Information Security
				Compliance
		Issue		
	Low			Compliance;;Member
	Moderate			Information Security

	High	Issue		Information Security
	Moderate			Compliance
	High	Issue;;Control Failure		Account;;Member;;Operational;;Reputational

	Moderate	Issue		Compliance;;Information Security;;Member;;Account;;Financial
	Moderate	Issue		Account;;Financial;;Member;;Reputational;;Compliance
	Moderate	Issue		Account;;Financial;;Member;;Compliance;;Provider

	Low	Issue		Member;;Compliance;;Financial
	Moderate	Issue;;Medicare Issue [DEPRECATED]		Compliance;;Reputational;;Financial
	Low	Issue		Compliance;;Financial

	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security
	Moderate	HiTrust Cap		Information Security

	Low			Compliance
	Moderate	Control Exception		Information Security

	Observation			

Reference Issue	EVP Reporting?	Error Category Type	YesNo
	Yes		
	Yes		

	Yes		

	Yes		
	Yes		

	Yes		
	Yes		
	Yes		

	Yes		
	Yes		

	Yes		
	Yes		
	Yes		
	Yes		
	Yes		

	Yes		

	Yes		
	Yes		
	Yes		

	Yes		

Confirmed On	Confirmed By
2023-07-11 12:21:52 AM	Lisa George
2023-03-28 10:02:55 AM	Kim Sok
2023-07-05 08:58:37 PM	Lisa George

2023-07-07 12:17:01 AM	Lisa George
2023-05-04 10:57:21 AM	Lisa George
2023-07-05 10:33:35 PM	Lisa George
2023-07-07 12:23:17 AM	Lisa George

2023-07-05 10:54:38 PM	Lisa George
2023-06-16 03:13:49 PM	Alex Rodriguez
2023-06-12 11:29:48 PM	Lisa George

2023-06-12 11:37:24 PM	Lisa George
2023-06-14 10:38:26 AM	Alex Rodriguez
2023-06-14 12:12:50 PM	Alex Rodriguez
2023-07-27 09:30:39 PM	Lisa George

2023-06-16 01:54:22 PM	Alex Rodriguez
2023-06-16 01:54:46 PM	Alex Rodriguez
2023-06-16 01:54:53 PM	Alex Rodriguez
2023-06-16 01:56:22 PM	Alex Rodriguez
2023-06-16 01:56:43 PM	Alex Rodriguez

2023-06-16 02:00:58 PM	Alex Rodriguez
2023-07-27 08:57:57 PM	Lisa George
2023-07-27 09:33:35 PM	Lisa George

2023-06-16 02:01:30 PM	Alex Rodriguez
2023-06-16 02:01:37 PM	Alex Rodriguez
2023-06-16 02:01:44 PM	Alex Rodriguez
2023-06-16 02:01:52 PM	Alex Rodriguez

2023-06-16 02:02:00 PM	Alex Rodriguez
2023-06-16 02:02:08 PM	Alex Rodriguez
2023-07-27 09:25:38 PM	Lisa George
2023-07-27 07:56:15 PM	Lisa George

2023-09-06 08:31:18 PM	Alexander DeSimone
2023-12-01 07:47:10 PM	Alexander DeSimone
2023-11-29 02:22:42 AM	Alexander DeSimone

2023-11-29 02:53:44 AM	Alexander DeSimone
2023-11-29 02:36:27 AM	Alexander DeSimone
2023-11-29 02:42:40 AM	Alexander DeSimone

2023-11-29 03:01:07 AM	Alexander DeSimone
2023-12-01 07:40:59 PM	Alexander DeSimone
2024-01-22 06:04:02 PM	James Farrell
2024-02-02 06:36:31 PM	Alexander DeSimone
2024-02-09 04:14:51 PM	Alexander DeSimone
2024-02-22 02:09:09 PM	Kim Sok

2024-03-05 07:15:22 PM	Alexander DeSimone
2025-04-08 02:07:22 PM	Bernard Mumuluh
2025-05-30 11:40:03 PM	Alexander DeSimone
2024-08-14 12:06:05 AM	Alexander DeSimone

2024-08-13 10:39:29 PM	Alexander DeSimone
2024-08-13 11:56:48 PM	Alexander DeSimone

2025-02-20 01:24:10 AM	Alexander DeSimone
2024-08-23 11:47:55 AM	Bernard Mumuluh

2025-02-27 08:56:20 PM	Alexander DeSimone

2024-10-08 01:05:11 AM	Alexander DeSimone
2024-11-25 08:03:17 PM	Alexander DeSimone
2024-11-14 12:22:51 PM	Alexander DeSimone
2024-11-25 08:08:54 PM	Alexander DeSimone

2025-02-17 11:01:12 PM	Alexander DeSimone
2025-03-03 05:29:49 PM	Alexander DeSimone
2025-03-03 05:38:35 PM	Alexander DeSimone
2025-06-13 01:16:53 PM	Melissa Trenholm

2024-01-09 08:32:50 PM	Lisa George
2022-09-07 08:13:43 PM	Lisa George
2022-10-27 02:30:58 PM	Alex Rodriguez
2023-01-31 09:37:48 AM	Melissa Trenholm

2023-03-15 04:47:17 PM	Nikita Sujan
2023-03-12 09:35:00 PM	Lisa George
2023-03-15 05:40:50 PM	Nikita Sujan

2023-06-12 11:19:34 PM	Lisa George
2023-06-14 12:09:29 PM	Alex Rodriguez

2023-06-16 12:05:53 PM	Alex Rodriguez
2023-07-27 09:28:13 PM	Lisa George

2023-06-16 01:54:38 PM	Alex Rodriguez
2023-06-16 01:55:35 PM	Alex Rodriguez
2023-06-16 01:55:54 PM	Alex Rodriguez
2023-06-16 01:56:10 PM	Alex Rodriguez
2023-06-16 01:55:12 PM	Alex Rodriguez
2023-06-16 02:01:15 PM	Alex Rodriguez

2023-11-28 05:56:49 PM	Margaret Fu
2023-11-28 06:09:48 PM	Margaret Fu
2023-11-28 06:13:38 PM	Margaret Fu
2023-11-28 06:17:33 PM	Margaret Fu

2023-12-01 07:25:52 PM	Alexander DeSimone

2024-07-24 10:29:36 PM	Alexander DeSimone

2024-04-10 07:53:38 AM	Nikita Sujan
2024-02-22 02:09:38 PM	Kim Sok

2024-02-20 01:40:19 PM	Melissa Trenholm
2025-05-30 12:07:59 PM	Alexander DeSimone
2024-03-05 07:37:32 PM	Alexander DeSimone
2024-03-26 04:55:13 PM	Melissa Trenholm
2025-05-06 03:54:44 PM	Alexander DeSimone

2024-08-13 11:09:51 PM	Alexander DeSimone
2024-08-13 10:32:49 PM	Alexander DeSimone
2024-08-08 09:50:33 PM	Alexander DeSimone
2024-08-08 01:13:13 PM	Alexander DeSimone

2024-08-14 12:03:38 AM	Alexander DeSimone
2024-08-13 11:19:16 PM	Alexander DeSimone

2024-10-09 05:21:23 PM	Alexander DeSimone
2024-08-13 11:46:33 PM	Alexander DeSimone
2024-08-13 11:39:03 PM	Alexander DeSimone
2024-08-13 11:07:41 PM	Alexander DeSimone
2024-08-13 11:49:21 PM	Alexander DeSimone

2024-08-13 11:51:33 PM	Alexander DeSimone
2024-08-28 04:24:40 PM	Melissa Trenholm
2024-11-25 08:01:20 PM	Alexander DeSimone
2024-10-24 03:13:21 PM	Alexander DeSimone
2024-09-26 09:53:26 PM	Alexander DeSimone

2024-10-31 09:32:07 AM	Theresa Lynch

2025-04-07 12:18:41 AM	Lisa George
2024-12-10 05:43:06 PM	Alexander DeSimone
2025-01-21 08:15:10 PM	Alexander DeSimone
2025-06-11 07:08:02 PM	Lisa George

2025-02-17 05:19:34 PM	Zachary Mucha

2025-02-27 08:43:43 PM	Alexander DeSimone
2025-02-18 04:11:13 PM	Nikita Sujan

2025-03-20 08:43:53 AM	Zachary Mucha
2025-03-31 01:36:16 PM	Melissa Trenholm
2025-04-29 12:07:51 AM	Lisa George
2025-04-06 11:49:18 PM	Lisa George

2025-04-07 12:10:58 AM	Lisa George
2025-04-07 12:35:04 AM	Lisa George
2025-04-07 12:56:09 AM	Lisa George
2025-04-07 01:05:57 AM	Lisa George
2025-04-07 01:18:20 AM	Lisa George
2025-05-14 06:38:42 PM	Lisa George
2025-06-05 07:04:39 PM	Lisa George
2025-05-30 07:49:02 PM	Lisa George

2025-05-30 07:57:08 PM	Lisa George
2025-06-05 07:13:07 PM	Lisa George
2025-06-13 01:12:20 PM	Melissa Trenholm
2025-06-13 01:28:28 PM	Melissa Trenholm
2025-06-13 01:40:37 PM	Melissa Trenholm
2025-06-26 09:21:36 PM	Alexander DeSimone

2025-06-27 04:02:49 PM	Alexander DeSimone
2022-09-07 08:39:07 PM	Lisa George
2022-09-14 10:31:18 AM	Gregory Wehn (no-access)

2023-06-26 04:13:34 PM	Kim Sok
2023-02-08 07:35:26 PM	Kim Sok
2023-02-08 07:35:39 PM	Kim Sok

2024-01-03 09:51:42 AM	Theresa Lynch
2023-09-05 11:53:46 AM	Lisa George
2023-09-07 07:07:22 PM	Lisa George

2023-06-12 10:33:28 PM	Lisa George
2023-06-12 10:44:57 PM	Lisa George
2023-06-16 01:49:41 PM	Alex Rodriguez
2023-06-16 01:55:00 PM	Alex Rodriguez

2025-01-09 12:04:41 PM	Nikita Sujan
2025-02-21 10:27:17 AM	Timothy Bulman
2025-02-28 10:49:12 AM	Melissa Trenholm
2025-06-17 10:17:28 AM	Bernard Mumuluh

2025-05-15 10:39:17 AM	Ollie Bodden

Pending Remediation Date	Pending Remediation By User
2023-07-11 12:21:55 AM	Lisa George
2023-07-27 08:14:35 PM	Lisa George
2023-07-05 08:58:45 PM	Lisa George

2023-07-07 12:17:04 AM	Lisa George
2023-05-04 10:57:26 AM	Lisa George
2025-06-17 09:47:29 AM	Bernard Mumuluh
2023-07-07 12:23:22 AM	Lisa George

2023-07-05 10:54:44 PM	Lisa George
2025-03-14 04:30:14 PM	Korelle Foy
2023-07-26 10:20:56 PM	Lisa George

2023-07-26 10:22:37 PM	Lisa George
2023-07-27 09:37:38 PM	Lisa George
2025-03-14 04:34:07 PM	Korelle Foy
2023-07-27 09:30:42 PM	Lisa George

2023-07-27 09:31:16 PM	Lisa George
2025-03-14 04:42:25 PM	Korelle Foy
2023-07-27 09:38:02 PM	Lisa George
2023-07-27 09:40:21 PM	Lisa George
2023-07-27 09:40:45 PM	Lisa George

2023-07-27 09:41:08 PM	Lisa George
2023-07-27 08:58:00 PM	Lisa George
2023-07-27 09:33:38 PM	Lisa George

2023-07-27 09:41:51 PM	Lisa George
2025-03-14 04:17:17 PM	Korelle Foy
2025-03-14 04:13:00 PM	Korelle Foy
2025-03-14 04:11:42 PM	Korelle Foy

2025-03-14 04:09:09 PM	Korelle Foy
2025-03-14 04:07:29 PM	Korelle Foy
2023-07-27 09:25:41 PM	Lisa George
2023-07-27 07:56:17 PM	Lisa George

2023-09-15 02:56:37 PM	Alex Rodriguez
2023-12-01 07:47:12 PM	Alexander DeSimone
2024-01-05 01:00:30 AM	Alexander DeSimone

2023-11-29 02:53:47 AM	Alexander DeSimone
2023-11-29 02:36:31 AM	Alexander DeSimone
2023-11-29 02:42:43 AM	Alexander DeSimone

2023-11-29 03:01:09 AM	Alexander DeSimone
2024-03-13 03:20:05 PM	Alexander DeSimone
2024-04-25 01:44:43 PM	Bernard Mumuluh
2024-02-02 06:36:35 PM	Alexander DeSimone
2024-02-09 04:14:55 PM	Alexander DeSimone
2024-02-22 02:10:41 PM	Zachary Mucha

2024-03-05 07:15:26 PM	Alexander DeSimone
2025-06-17 03:04:28 PM	Bernard Mumuluh
2025-05-30 11:40:05 PM	Alexander DeSimone
2024-08-14 12:06:07 AM	Alexander DeSimone

2024-08-13 10:39:31 PM	Alexander DeSimone
2024-08-13 11:56:50 PM	Alexander DeSimone

2025-02-20 01:24:13 AM	Alexander DeSimone
2024-09-27 10:39:47 AM	Alexander DeSimone

2025-02-27 08:56:34 PM	Alexander DeSimone

2024-10-08 01:05:13 AM	Alexander DeSimone
2024-11-25 08:03:18 PM	Alexander DeSimone
2024-11-14 12:22:57 PM	Alexander DeSimone
2024-11-25 08:08:56 PM	Alexander DeSimone

2025-03-05 05:19:11 PM	Alexander DeSimone
2025-03-05 10:59:10 AM	Alexander DeSimone
2025-03-03 05:38:37 PM	Alexander DeSimone
2025-06-13 01:16:55 PM	Melissa Trenholm

2024-01-09 08:32:53 PM	Lisa George
2023-10-31 11:04:39 AM	Alex Rodriguez
2023-07-11 12:37:42 AM	Lisa George
2024-01-04 02:43:10 PM	Melissa Trenholm

2023-03-15 04:47:31 PM	Nikita Sujan
2023-03-12 09:35:04 PM	Lisa George
2023-07-27 08:11:14 PM	Lisa George

2023-07-27 09:35:40 PM	Lisa George
2023-07-27 09:29:14 PM	Lisa George

2023-07-27 09:32:35 PM	Lisa George
2023-07-27 09:28:16 PM	Lisa George

2023-07-27 09:29:48 PM	Lisa George
2023-07-27 09:38:25 PM	Lisa George
2023-07-27 09:39:55 PM	Lisa George
2023-07-27 09:39:23 PM	Lisa George
2023-07-27 09:32:03 PM	Lisa George
2023-07-27 09:41:28 PM	Lisa George

2024-06-05 03:26:17 PM	Margaret Fu
2023-11-28 06:09:50 PM	Margaret Fu
2023-11-28 06:13:41 PM	Margaret Fu
2023-11-28 06:17:38 PM	Margaret Fu

2024-12-03 03:47:07 PM	Alexander DeSimone

2024-07-24 10:29:39 PM	Alexander DeSimone

2024-04-10 07:53:41 AM	Nikita Sujan
2025-03-13 04:44:45 PM	Zachary Mucha

2024-03-26 04:53:52 PM	Melissa Trenholm
2025-05-30 12:08:01 PM	Alexander DeSimone
2024-03-08 04:36:39 PM	Alexander DeSimone
2024-03-26 04:55:32 PM	Melissa Trenholm
2025-05-06 03:54:46 PM	Alexander DeSimone

2024-08-13 11:09:53 PM	Alexander DeSimone
2024-08-13 10:32:51 PM	Alexander DeSimone
2024-08-08 09:50:48 PM	Alexander DeSimone
2024-08-08 01:13:15 PM	Alexander DeSimone

2024-08-14 12:03:41 AM	Alexander DeSimone
2024-08-13 11:19:18 PM	Alexander DeSimone

2024-10-09 05:21:25 PM	Alexander DeSimone
2024-08-13 11:46:36 PM	Alexander DeSimone
2024-08-13 11:39:06 PM	Alexander DeSimone
2024-08-13 11:07:43 PM	Alexander DeSimone
2024-08-13 11:49:22 PM	Alexander DeSimone

2024-08-13 11:51:36 PM	Alexander DeSimone
2024-08-28 04:24:44 PM	Melissa Trenholm
2024-11-25 08:01:22 PM	Alexander DeSimone
2024-10-24 03:13:25 PM	Alexander DeSimone
2025-05-08 03:00:04 PM	Alexander DeSimone

2024-10-31 09:32:09 AM	Theresa Lynch

2025-04-07 12:18:43 AM	Lisa George
2024-12-10 05:43:08 PM	Alexander DeSimone
2025-01-21 08:15:11 PM	Alexander DeSimone
2025-06-11 07:08:04 PM	Lisa George

2025-02-17 05:19:41 PM	Zachary Mucha

2025-02-27 08:43:45 PM	Alexander DeSimone
2025-02-18 04:11:15 PM	Nikita Sujan

2025-03-20 08:43:59 AM	Zachary Mucha
2025-04-23 12:37:25 PM	Melissa Trenholm
2025-04-29 12:07:52 AM	Lisa George
2025-04-06 11:49:20 PM	Lisa George

2025-04-07 12:11:00 AM	Lisa George
2025-04-07 12:35:07 AM	Lisa George
2025-04-07 12:56:11 AM	Lisa George
2025-04-07 01:06:27 AM	Lisa George
2025-04-07 01:18:23 AM	Lisa George
2025-05-14 06:38:45 PM	Lisa George
2025-06-05 07:04:42 PM	Lisa George
2025-05-30 07:49:04 PM	Lisa George

2025-05-30 07:57:24 PM	Lisa George
2025-06-05 07:13:09 PM	Lisa George
2025-06-13 01:12:25 PM	Melissa Trenholm
2025-06-13 01:28:32 PM	Melissa Trenholm
2025-06-13 01:40:39 PM	Melissa Trenholm
2025-06-26 09:21:38 PM	Alexander DeSimone

2025-06-27 04:02:50 PM	Alexander DeSimone
2023-05-09 11:10:13 AM	Timothy Bulman
2025-03-20 04:49:45 PM	Alexander DeSimone

2024-05-17 12:13:13 PM	Kim Sok

2023-09-05 11:53:49 AM	Lisa George
2023-09-07 07:07:25 PM	Lisa George

2025-02-21 10:27:24 AM	Timothy Bulman

Remediated On	Remediated By
2024-04-24 02:50:31 PM	Rich Trisoline
2024-01-04 09:56:18 AM	Theresa Lynch
2024-03-05 04:58:02 PM	Bernard Mumuluh

2024-03-08 01:12:03 PM	Stephanie Laing
2024-04-02 01:30:36 PM	Stephanie Laing
2025-06-17 09:47:39 AM	Bernard Mumuluh
2024-06-27 10:30:45 AM	Rashi Khanna

2023-09-26 01:57:30 PM	Rich Trisoline
2025-03-14 04:30:15 PM	Korelle Foy
2025-03-03 08:53:20 AM	Rich Trisoline

2024-04-24 03:03:10 PM	Rich Trisoline
2025-03-14 04:03:24 PM	Korelle Foy
2025-03-14 04:34:08 PM	Korelle Foy
2025-03-14 04:36:14 PM	Korelle Foy

2025-03-14 04:38:34 PM	Korelle Foy
2025-03-14 04:42:26 PM	Korelle Foy
2024-05-13 02:05:33 PM	Ryan Canney
2025-03-14 04:28:14 PM	Korelle Foy
2025-03-14 04:26:45 PM	Korelle Foy

2025-03-14 04:23:53 PM	Korelle Foy
2025-03-14 04:56:17 PM	Korelle Foy
2025-03-14 04:18:45 PM	Korelle Foy

2024-04-03 08:38:16 AM	Bill Gates (Deleted)
2025-03-14 04:17:18 PM	Korelle Foy
2025-03-14 04:13:07 PM	Korelle Foy
2025-03-14 04:11:46 PM	Korelle Foy

2025-03-14 04:09:11 PM	Korelle Foy
2025-03-14 04:07:39 PM	Korelle Foy
2025-03-14 03:58:59 PM	Korelle Foy
2024-06-02 03:07:09 AM	Arunkumar Ramakrishnan

2023-09-15 04:15:58 PM	Rich Trisoline
2024-01-16 03:50:49 PM	Adeola Adebiyi
2024-06-02 03:19:22 AM	Arunkumar Ramakrishnan

2024-02-29 10:01:06 AM	Ryan Canney
2024-06-27 10:30:28 AM	Rashi Khanna
2024-03-05 04:26:12 PM	Jozef Nagy

2024-03-05 10:52:42 AM	Adeola Adebiyi
2024-03-13 03:22:02 PM	Ryan Canney
2024-04-30 11:43:57 AM	Rich Trisoline
2024-06-02 03:07:33 AM	Arunkumar Ramakrishnan
2024-05-09 01:04:29 PM	Walter Endyke
2024-03-18 03:03:36 PM	Kathleen Moitoso

2024-03-13 03:33:35 PM	Ryan Canney
2025-06-17 03:04:29 PM	Bernard Mumuluh
2025-05-30 11:40:07 PM	Alexander DeSimone
2024-08-14 09:26:12 AM	Elena Henkin

2024-12-18 11:01:02 AM	Rich Trisoline
2025-04-03 01:43:18 PM	Rich Trisoline

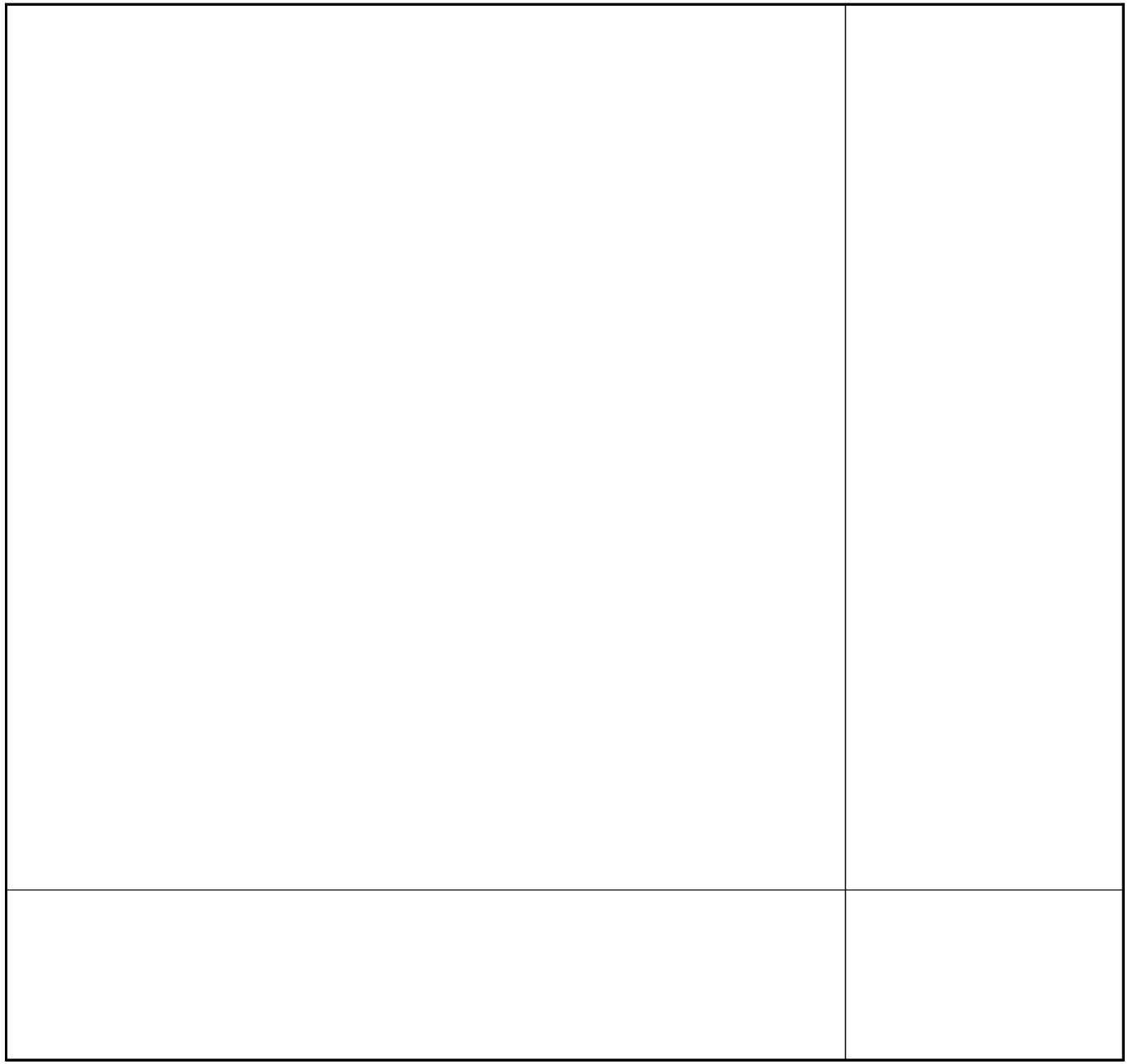
2025-04-09 01:36:02 PM	Ashley Leavitt
2024-09-27 01:44:48 PM	Andrew Spisak

2025-03-05 10:58:24 AM	Alexander DeSimone

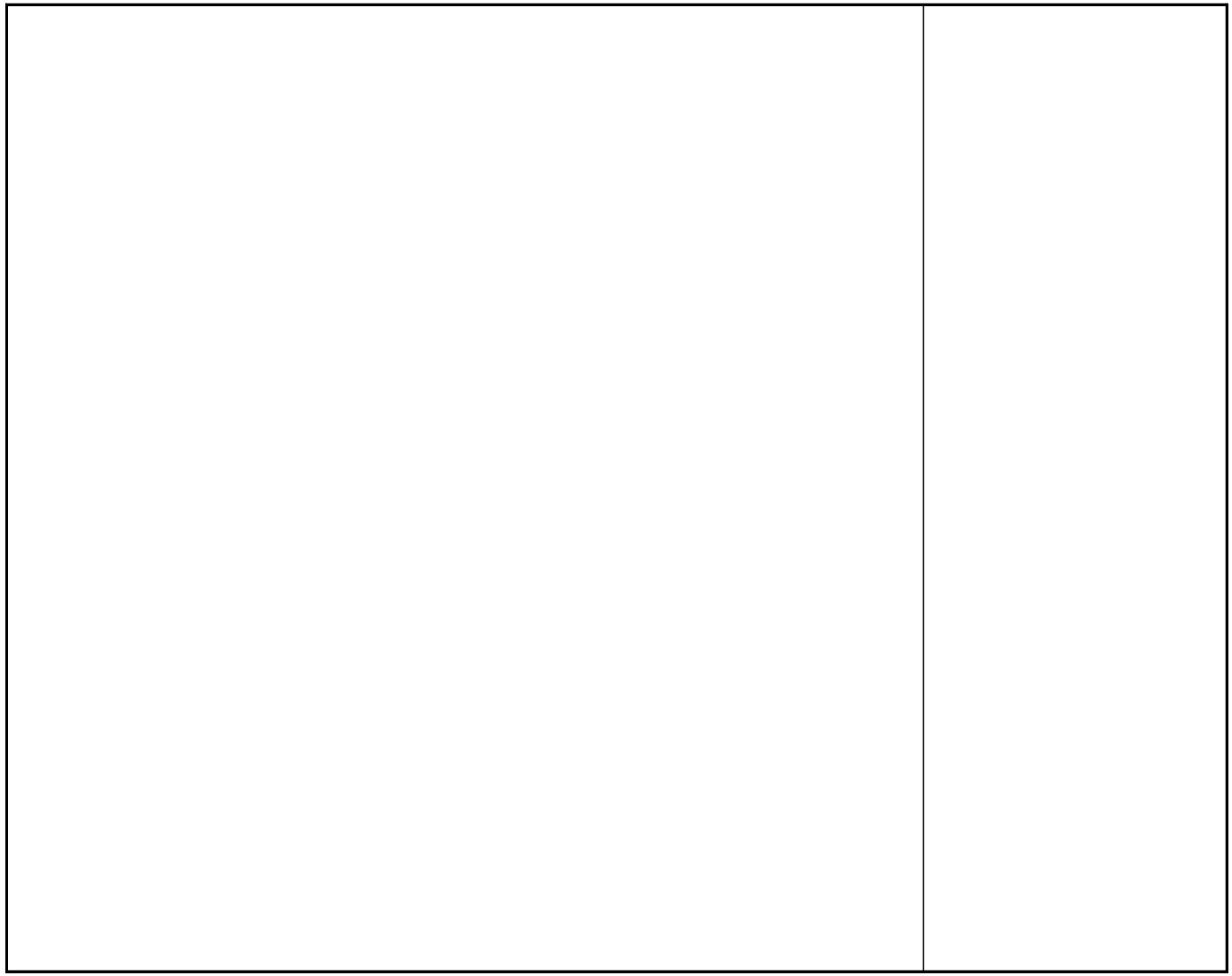
2025-02-21 12:43:17 AM	Alexander DeSimone
2025-01-06 10:38:37 AM	Diana Salvucci
2025-01-06 03:02:44 PM	Donnie Kyne
2024-12-05 09:21:05 AM	Walter Endyke

2025-04-02 04:42:19 PM	MaheswaraReddy Talla
2025-03-18 05:37:49 AM	Malar Vizhi Somasundaram
2025-03-24 09:53:59 AM	Andrew Moore
2025-06-13 01:17:11 PM	Melissa Trenholm

2022-11-07 06:51:48 PM	Lisa George



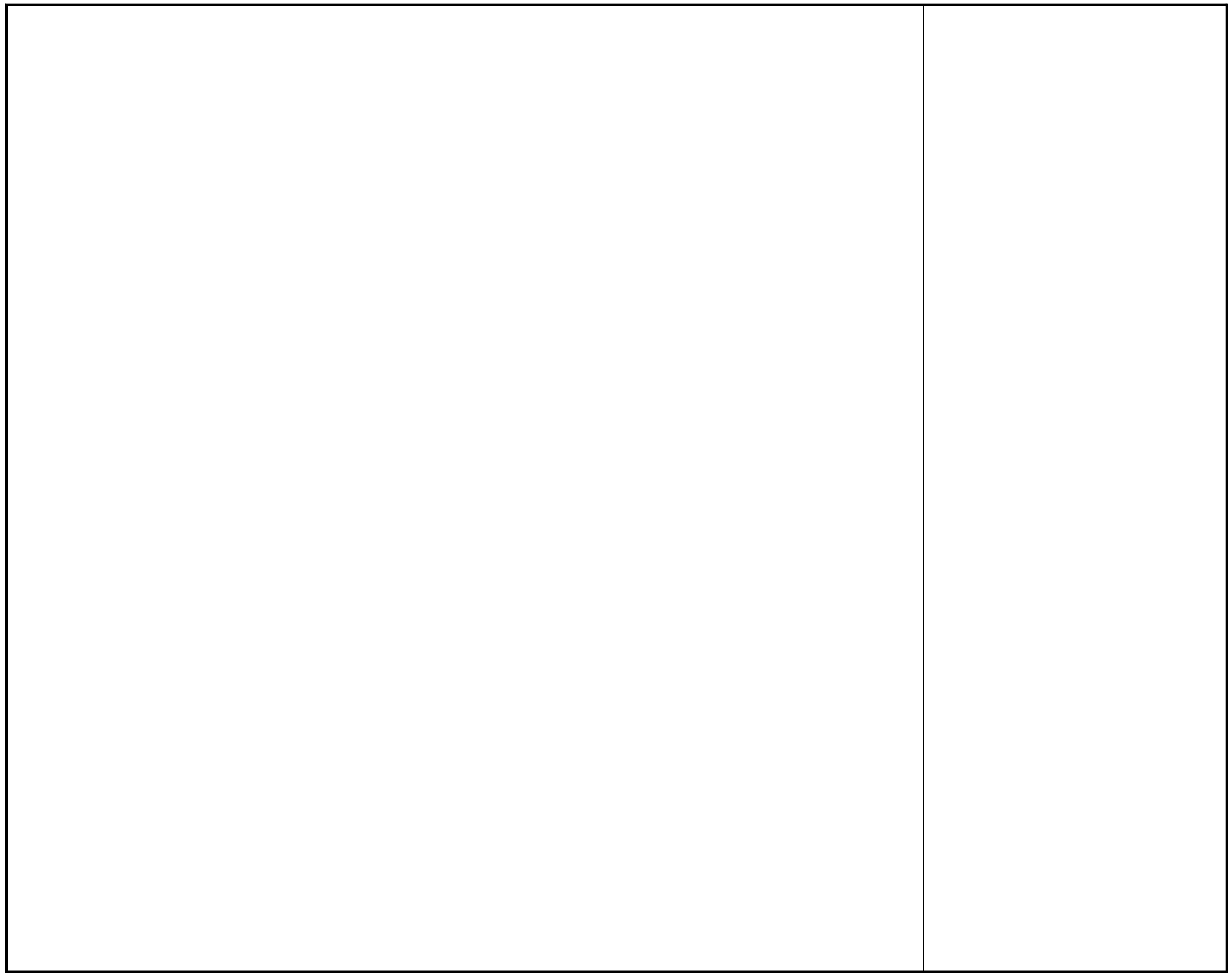
2024-04-02 02:35:29 PM	Alexander DeSimone

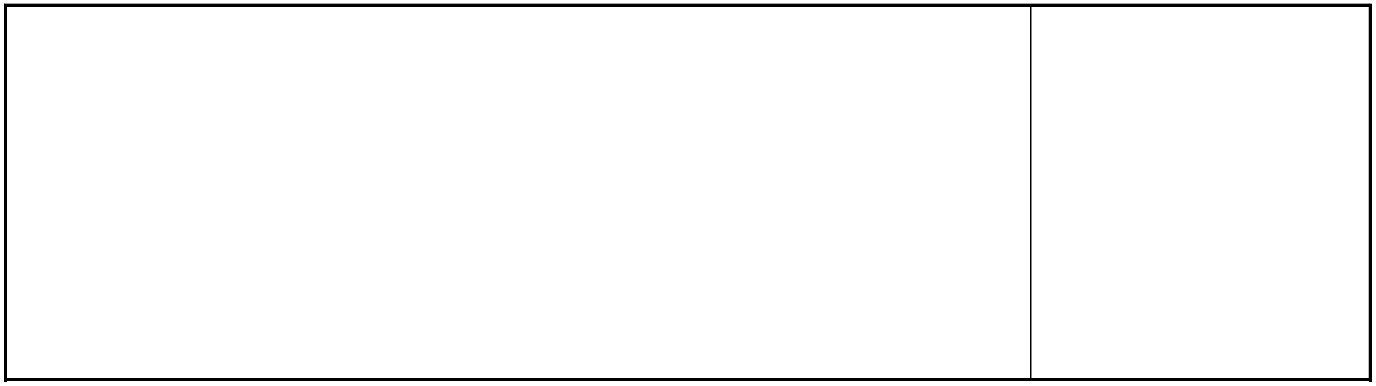


2025-03-03 01:08:23 PM	Zachary Mucha

2024-05-15 12:46:32 PM	Ryan Canney

2025-04-06 11:59:48 PM	Lisa George





2025-04-23 12:12:26 PM	Timothy Bulman

2023-05-09 11:09:43 AM	Timothy Bulman
2025-04-07 01:26:51 PM	Rich Trisoline

2024-10-01 08:05:59 AM	Michele Bernache

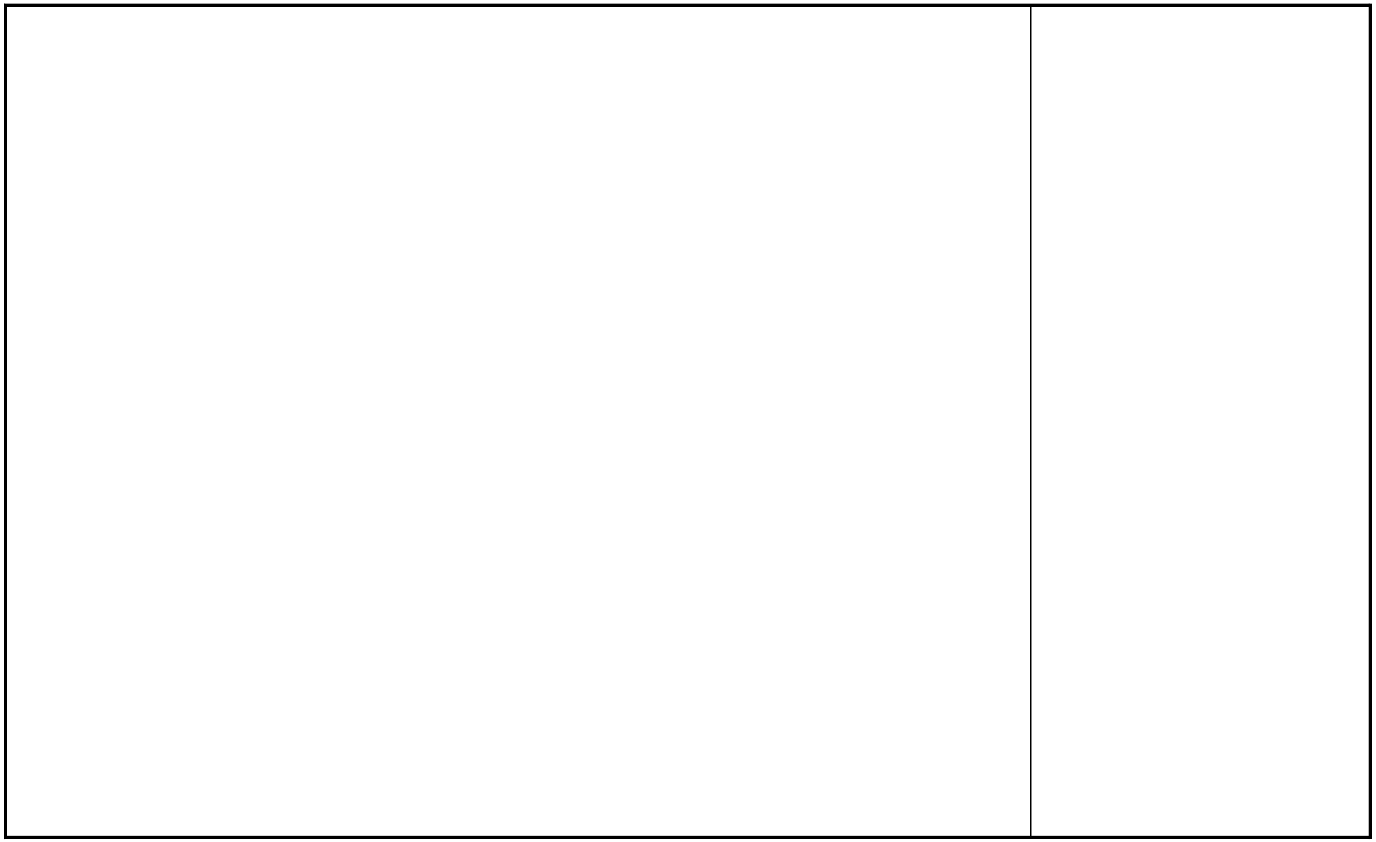
2023-08-14 02:21:04 PM	Theresa Lynch

Closed On	Closed By
2025-01-21 08:13:32 PM	Alexander DeSimone
2024-01-04 11:46:48 AM	Kim Sok

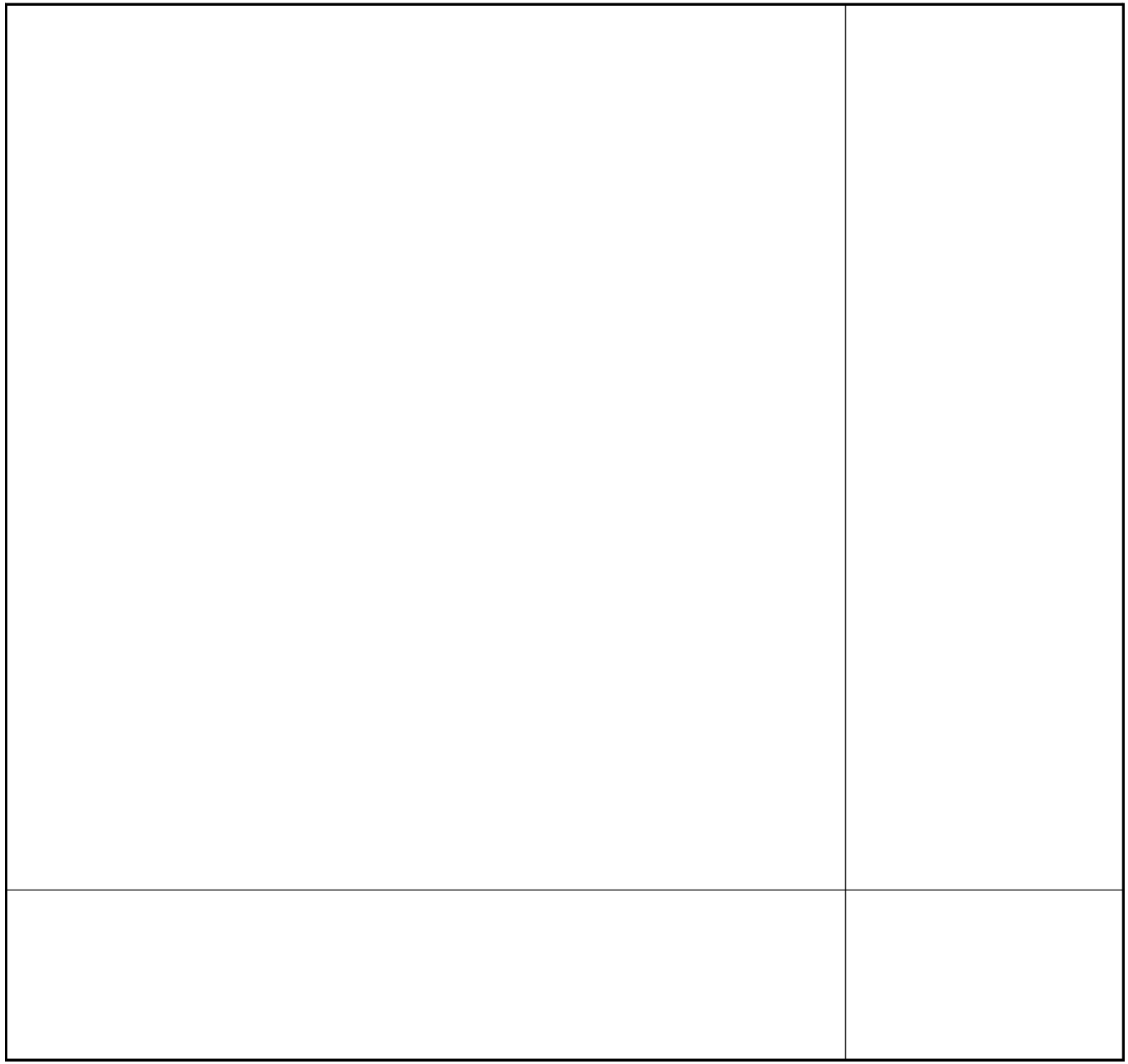
2024-01-05 12:57:11 AM	Alexander DeSimone

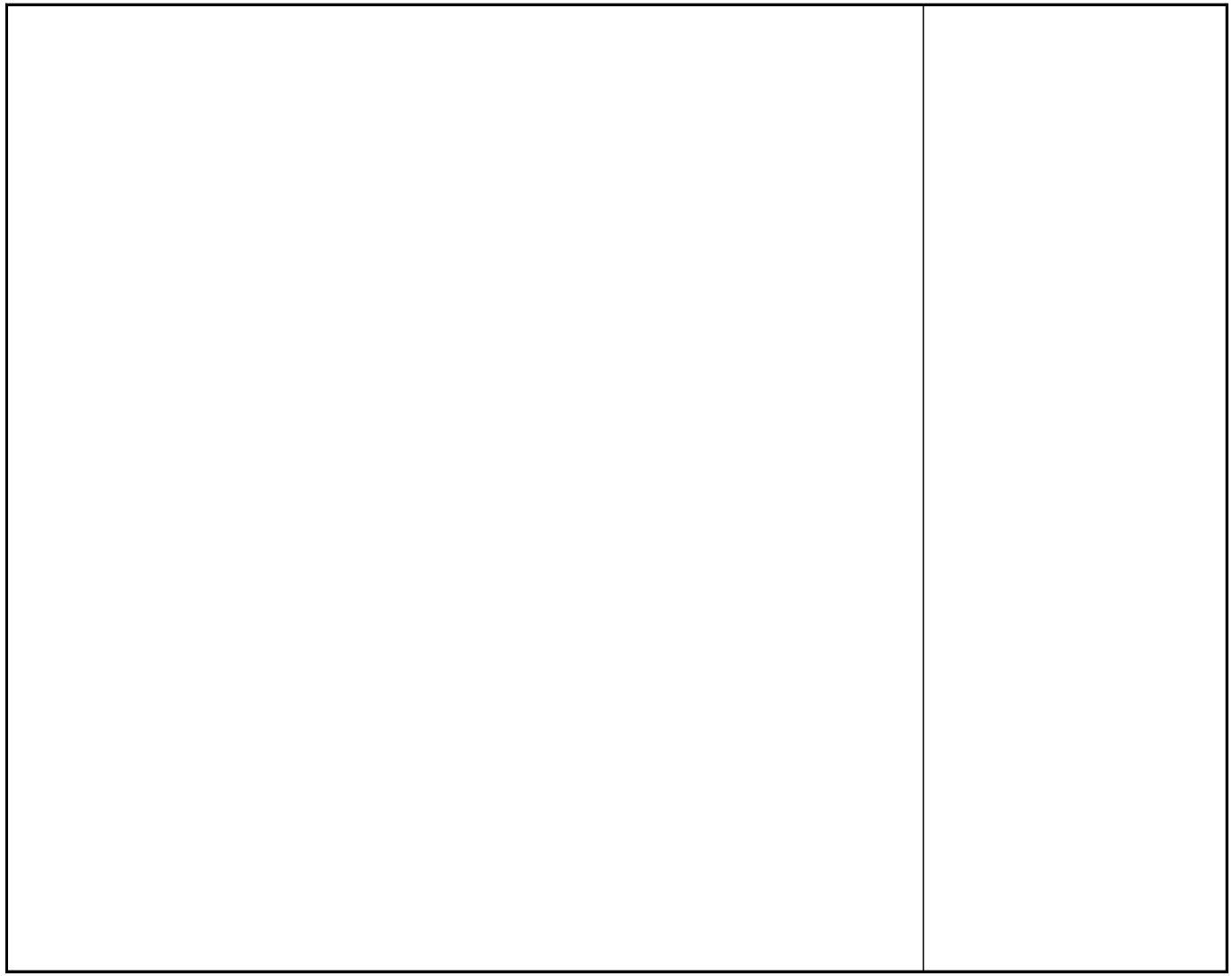
2025-01-16 01:04:45 PM	Bernard Mumuluh

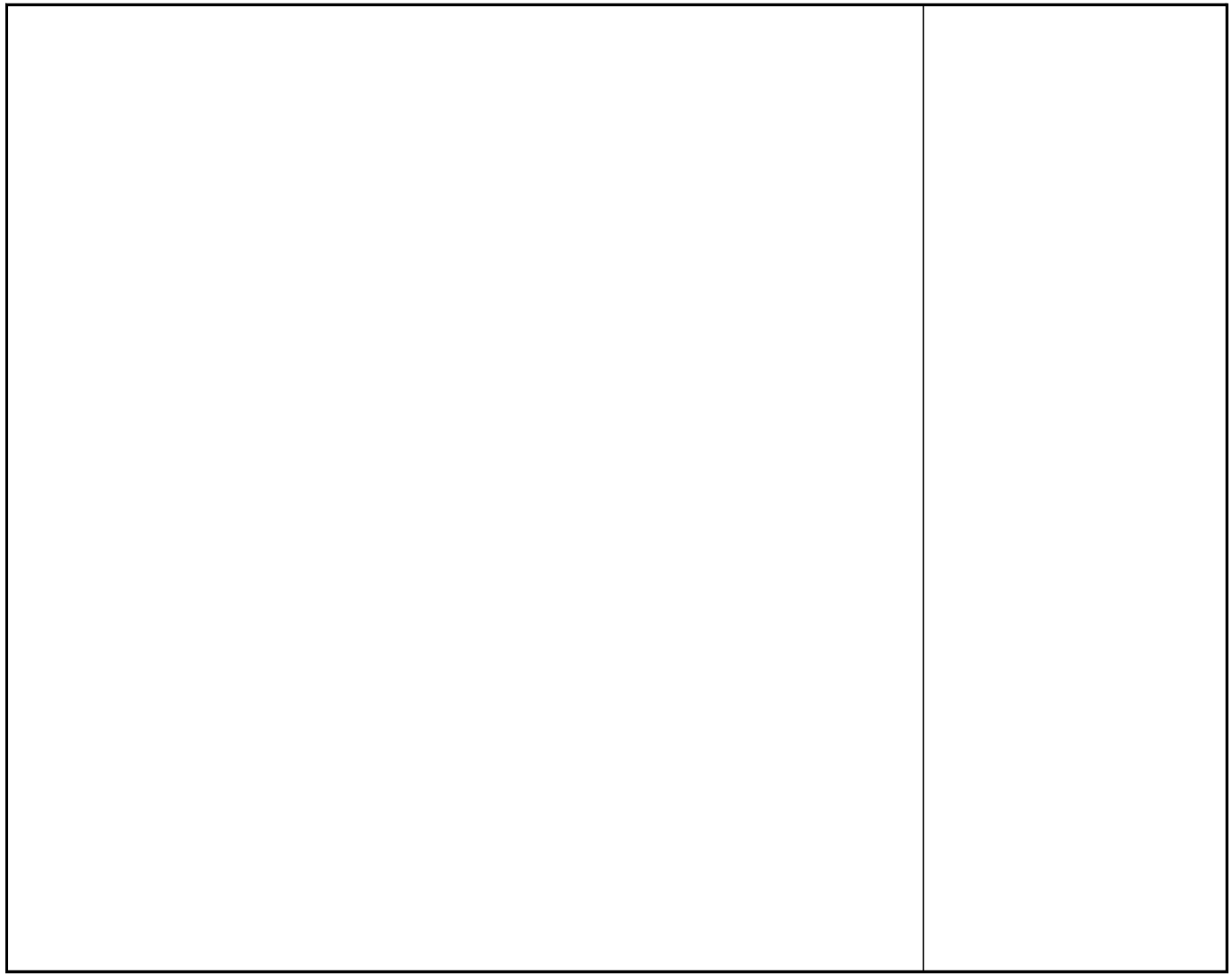
2025-05-08 10:27:36 AM	Ollie Bodden

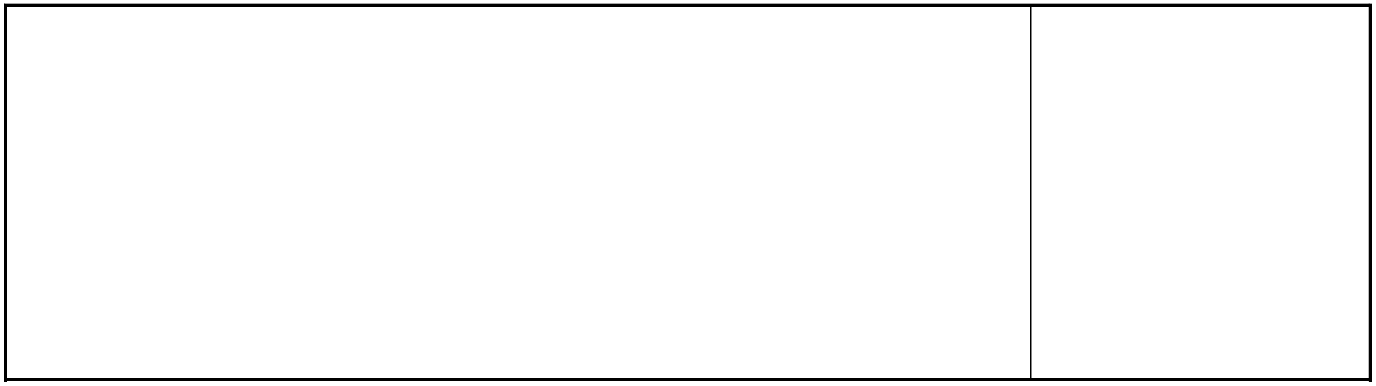


2022-11-07 06:51:58 PM	Lisa George









Date Created	Is Remediation Owner
2022-09-14 03:21:57 PM	No
2023-03-28 09:49:40 AM	No
2023-03-30 11:18:51 AM	No

2023-03-30 03:42:40 PM	No
2023-05-04 10:45:51 AM	No
2023-05-22 03:29:41 PM	No
2023-05-22 04:11:02 PM	No

2023-05-22 04:27:32 PM	No
2023-06-04 11:21:43 PM	No
2023-06-12 11:22:43 PM	No

2023-06-12 11:33:11 PM	No
2023-06-14 10:24:24 AM	No
2023-06-14 11:51:08 AM	No
2023-06-14 02:07:29 PM	No

2023-06-14 02:17:35 PM	No
2023-06-14 03:38:01 PM	No
2023-06-14 03:51:22 PM	No
2023-06-14 04:45:27 PM	No
2023-06-14 04:53:04 PM	No

2023-06-14 04:56:49 PM	No
2023-06-14 05:00:17 PM	No
2023-06-15 09:52:28 AM	No

2023-06-15 10:22:45 AM	No
2023-06-15 01:09:18 PM	No
2023-06-15 01:18:50 PM	No
2023-06-15 01:43:28 PM	No

2023-06-15 01:56:38 PM	No
2023-06-15 02:04:56 PM	No
2023-06-16 02:31:49 PM	No
2023-06-22 04:53:58 PM	No

2023-09-06 08:05:51 PM	No
2023-09-06 08:12:49 PM	No
2023-11-29 01:27:27 AM	No

2023-11-29 01:45:06 AM	No
2023-11-29 02:32:34 AM	No
2023-11-29 02:38:54 AM	No

2023-11-29 02:57:17 AM	No
2023-12-01 07:35:00 PM	No
2024-01-17 04:14:44 PM	No
2024-02-02 06:30:56 PM	No
2024-02-09 03:54:57 PM	No
2024-02-15 05:07:24 PM	No

2024-02-27 02:39:45 PM	No
2024-03-06 07:20:43 PM	No
2024-03-25 03:02:50 PM	No
2024-05-06 07:25:41 PM	No

2024-06-03 11:15:05 PM	No
2024-07-23 02:19:08 PM	No

2024-08-05 06:08:01 PM	No
2024-08-12 01:16:49 PM	No

2024-10-07 03:39:54 PM	No

2024-10-07 03:57:20 PM	No
2024-11-01 06:30:13 PM	No
2024-11-01 06:39:58 PM	No
2024-11-01 06:58:14 PM	No

2025-01-31 11:24:16 PM	No
2025-03-03 05:24:25 PM	No
2025-03-03 05:33:33 PM	No
2025-06-13 01:14:11 PM	No

2022-07-21 03:43:54 PM	No
2022-07-22 10:47:58 AM	No
2022-09-20 12:30:24 PM	No
2023-01-20 12:08:46 PM	No

2023-01-31 03:29:43 PM	No
2023-03-12 09:23:54 PM	No
2023-03-15 05:36:03 PM	No

2023-06-12 10:49:42 PM	No
2023-06-14 11:25:00 AM	No

2023-06-14 12:11:12 PM	No
2023-06-14 01:37:11 PM	No

2023-06-14 02:42:41 PM	No
2023-06-14 04:09:52 PM	No
2023-06-14 04:17:30 PM	No
2023-06-14 04:25:59 PM	No
2023-06-14 04:31:40 PM	No
2023-06-15 09:29:43 AM	No

2023-10-25 03:38:30 PM	No
2023-10-25 03:40:58 PM	No
2023-10-25 03:41:58 PM	No
2023-10-25 04:00:45 PM	No

2023-12-01 07:14:51 PM	No

2023-12-04 07:25:57 PM	No

2024-02-01 09:28:06 AM	No
2024-02-15 04:26:35 PM	No

2024-02-20 01:29:43 PM	No
2024-02-23 03:17:34 AM	No
2024-02-27 02:33:23 PM	No
2024-03-26 04:24:53 PM	No
2024-05-10 07:23:29 PM	No

2024-06-03 09:51:35 PM	No
2024-06-03 11:08:17 PM	No
2024-06-11 10:35:57 AM	No
2024-06-13 02:53:22 PM	No

2024-07-23 05:52:20 PM	No
2024-07-23 05:58:30 PM	No

2024-08-05 05:16:35 PM	No
2024-08-05 06:00:41 PM	No
2024-08-05 06:19:22 PM	No
2024-08-07 06:44:11 PM	No
2024-08-12 09:42:00 PM	No

2024-08-12 09:49:41 PM	No
2024-08-28 04:20:22 PM	No
2024-09-19 05:24:47 PM	No
2024-09-26 09:20:15 PM	No
2024-09-26 09:47:56 PM	No

2024-10-31 09:11:30 AM	No

2024-11-01 05:41:43 PM	No
2024-11-18 02:51:09 PM	No
2025-01-21 08:05:51 PM	No
2025-01-29 02:34:51 AM	No

2025-02-07 11:15:37 AM	No

2025-02-17 08:58:17 PM	No
2025-02-18 02:35:13 PM	No

2025-03-05 04:26:16 PM	No
2025-03-31 01:06:22 PM	No
2025-04-06 11:30:11 PM	No
2025-04-06 11:45:34 PM	No

2025-04-07 12:04:54 AM	No
2025-04-07 12:24:17 AM	No
2025-04-07 12:46:12 AM	No
2025-04-07 01:02:17 AM	No
2025-04-07 01:13:49 AM	No
2025-05-14 06:31:13 PM	No
2025-05-20 07:57:46 PM	No
2025-05-30 07:43:32 PM	No

2025-05-30 07:51:56 PM	No
2025-06-05 07:09:12 PM	No
2025-06-13 12:56:25 PM	No
2025-06-13 01:22:36 PM	No
2025-06-13 01:35:30 PM	No
2025-06-26 09:18:23 PM	No

2025-06-27 03:53:06 PM	No
2021-05-12 02:44:33 PM	No
2022-09-14 10:13:12 AM	No

2023-02-01 12:42:09 PM	No
2023-02-02 05:22:41 PM	No
2023-02-02 05:30:23 PM	No

2023-04-03 10:53:22 AM	No
2023-05-24 10:25:09 AM	No
2023-05-24 10:29:36 AM	No

2023-06-12 09:44:58 PM	No
2023-06-12 10:35:29 PM	No
2023-06-14 01:26:15 PM	No
2023-06-14 04:04:18 PM	No

2025-01-09 09:16:24 AM	No
2025-02-04 03:05:51 PM	No
2025-02-28 10:43:11 AM	No
2025-04-21 02:47:30 PM	No

2025-05-08 09:20:09 AM	No