CYBERSECURITY PROCESS AUDIT REPORT

Risk-Based Cybersecurity Process Assurance for Core Information Technology and Digital Operations

Report Date: 30 December 2025

Audit Type: Limited-Scope Cybersecurity Process Audit covering Control Design Effectiveness and Control Operating Effectiveness

Audit Criteria and References: National Institute of Standards and Technology Cybersecurity Framework 2.0; risk-based assurance using Likelihood multiplied by Impact; Common Vulnerability Scoring System version 3.x used as an input to likelihood for vulnerability-related risks

Portfolio Project Note: This is a portfolio sample audit for a fictional organization. The report does not include operational metrics, such as sample sizes, counts, volumes, or percentages.

DOCUMENT CONTROL

Field	Value
Report Title	Cybersecurity Process Audit Report – Risk-Based Cybersecurity Process Assurance
Report Date	30 December 2025
Version	1.5
Prepared By	Cyber Safety Assurance (Portfolio Project)
Reviewed By	Cybersecurity Audit Quality Review (Portfolio)
Approved By	Not applicable (Portfolio Sample)
Report By	Ruchi Giradkar
Classification	Internal (Portfolio Sample)

1. EXECUTIVE SUMMARY

1.1 Audit Objective

The objective of this audit is to provide independent assurance over the **design effectiveness** and **operating effectiveness** of three cybersecurity processes that materially influence security outcomes across core information technology and digital operations:

1. **User and Access Management**
2. **Vulnerability and Patch Management**
3. **Incident Handling and Response**

The objective is to determine whether these processes are designed appropriately, executed consistently, and evidenced sufficiently to reduce cybersecurity risk exposure across information technology environments, cloud services environments, and business-critical application environments.

1.2 Audit Period and Scope Boundary

Audit period: The period represented by the artefacts made available in the portfolio project pack.
Scope boundary: The audit is limited to process assurance for the three processes listed above and the in-scope assets defined in this report. The audit is evidence-led and does not assume direct administrative access to production systems.

1.3 In-Scope Systems Summary

The audit focuses on critical systems supporting identity services, cloud operations, customer-facing services, monitoring, and resilience. These include:

- Identity provider service
- Cloud production account and associated administrative controls
- Customer portal application and customer database
- Security information and event management platform
- Endpoint detection and response platform
- Core enterprise resource planning system
- Backup vault and recovery store
- Corporate endpoint fleet

1.4 Overall Assurance Rating

Overall Assurance Rating: Partially Effective (Medium Assurance)

Meaning: Control design intent is visible across the audited processes; however, operating effectiveness is not consistently demonstrated due to governance cadence gaps, incomplete verification discipline, and limitations in evidence available within the portfolio project pack. In real operating environments, these issues commonly arise due to competing operational priorities and incomplete embedding of “control as part of workflow” expectations.

1.5 Formal Audit Opinion

Based on the procedures performed and the evidence reviewed in the portfolio project pack, the cybersecurity controls supporting **User and Access Management**, **Vulnerability and Patch Management**, and **Incident Handling and Response** are **partially effective**. Foundational design is present; however, gaps in execution, oversight, and evidence retention reduce confidence in sustained risk reduction.

1.6 Executive Risk Snapshot (Added for Leadership Readability)

The following statements summarize what leadership should care about most:

- **Exploitation risk remains elevated** if patch verification and failed patch rework are not embedded as mandatory workflow steps.
- **Unauthorized access risk remains elevated** if periodic access reviews are not performed and if offboarding service level adherence is not consistently evidenced.
- **Detection and investigation capability is weakened** if cloud administrative activity logging is not complete and centrally available for monitoring and forensics.
- **Control maturity will stagnate** if post-incident reviews are not performed and corrective actions are not tracked to closure.

1.7 Decisions and Actions Requested from Management

Management is requested to take the following actions:

1. Approve the Corrective Action Plan described in this report and assign accountable owners and responsible implementers.
2. Require governance reporting that demonstrates closure evidence for the highest risks, with recurring oversight.
3. Direct process owners to embed verification, review, and evidence retention into workflows so that operating effectiveness can be demonstrated reliably.

1.8 Highest Priority Risks

Priority	Risk Identifier	Risk Summary	Risk Score	Risk Severity
1	Risk 03	Critical vulnerabilities not patched and verified within defined service levels	25	High / Critical
2	Risk 05	Excessive privileges due to missing periodic access reviews	20	High
3	Risk 04	Legacy or unpatchable assets managed without complete governance and compensating controls	20	High
4	Risk 02	User access not revoked timely for leavers and movers	16	High
5	Risk 01, Risk 06, Risk 07	Privileged access hygiene, incident escalation delays, and incomplete cloud administrative logging	15	High

2. AUDIT APPROACH AND METHODOLOGY

2.1 Audit Method

This audit assessed controls using two dimensions:

- **Control design effectiveness:** Whether the control is designed appropriately to mitigate the intended risk if executed as intended.
- **Control operating effectiveness:** Whether the control is executed consistently and is supported by sufficient evidence to demonstrate sustained performance.

2.2 Audit Criteria and Benchmarks

Controls were assessed against the National Institute of Standards and Technology Cybersecurity Framework 2.0 categories as criteria anchors:

- Access control requirements (identity governance, least privilege, access reviews)
- Protective process requirements (patch management discipline, secure operations procedures)
- Security monitoring requirements (logging coverage, monitoring, event detection)
- Incident response requirements (response playbooks, escalation, post-incident improvement)
- Recovery requirements (backup, restoration testing, resilience verification)

Where the portfolio project pack indicates internal requirements (for example, patch service levels or access review cadence), these requirements are treated as explicit audit criteria.

2.3 Evidence Collection Approach

Evidence was collected by:

- Reviewing walkthrough artefacts (as represented in the portfolio project pack)
- Reviewing available policy and procedure documentation
- Reviewing workflow artefacts such as access request indicators, offboarding indicators, vulnerability intake indicators, patch governance indicators, and incident response artefacts
- Reviewing configuration exports and screenshots provided in the portfolio project pack
- Reviewing monitoring integration indicators between logging sources and the security information and event management platform

Where evidence was unavailable in the portfolio project pack, the report states: **“Not available in the portfolio project pack.”**

2.4 Risk Scoring Model

- Likelihood is scored from 1 to 5
- Impact is scored from 1 to 5
- Risk score equals Likelihood multiplied by Impact, with a maximum of 25

For vulnerability-related risks, the Common Vulnerability Scoring System version 3.x informs likelihood:

- Score from 0.1 to 3.9 results in a likelihood score of 1

- Score from 4.0 to 6.9 results in a likelihood score of 3
- Score from 7.0 to 10.0 results in a likelihood score of 5

Risk severity bands:

- Low risk: 1 to 7
- Medium risk: 8 to 14
- High risk: 15 to 25

Risk scoring note: Risk scores in this report are qualitative and based on professional judgment using the defined model and the evidence available in the portfolio project pack.

2.5 Control Rating Scale

- Control design rating: Adequate, Partially Adequate, Inadequate
- Control operating rating: Effective, Partially Effective, Ineffective
- Implementation status: Implemented, Partially Implemented, Not Implemented

Audit rule applied: When operating evidence is missing or incomplete in the portfolio project pack, the control is concluded as ineffective for operating effectiveness.

3. LIMITATIONS AND RELIANCE

Area	Detailed Statement
Reliance on provided information	This audit relies on documents, configuration exports, screenshots, and workflow artefacts included in the portfolio project pack.
No independent production system access	The audit did not assume direct administrative access to production environments. Therefore, configuration verification is based on provided exports and screenshots.
No quantitative sampling	This portfolio audit does not present sample sizes, operational volumes, or percentages. Conclusions are evidence-based and qualitative.
Out-of-scope activities	Penetration testing, exploit validation, red team exercises, and source code review were not performed.

4. AUDIT SCOPE DETAILS

4.1 In-Scope Processes

The audit assessed the following cybersecurity processes end-to-end, including governance, procedure design, execution discipline, evidence quality, and management oversight:

1. **User and Access Management**
   This includes identity lifecycle governance and access control across business systems, cloud services, and core information technology. Areas included are access

request approval, user provisioning, joiner-mover-leaver handling, privileged access controls, multi-factor authentication enforcement for privileged users, privileged account separation expectations, and periodic access review governance for sensitive systems.

2. **Vulnerability and Patch Management**
   This includes vulnerability intake, triage, remediation planning, patch acquisition, patch testing, deployment governance, exception handling, and verification that remediation actions have been completed. It also includes oversight mechanisms such as service level monitoring, escalation for overdue remediation, and evidence retention supporting vulnerability and patch closure.

3. **Incident Handling and Response**
   This includes detection and monitoring inputs, escalation procedures, severity classification, incident response playbooks, coordination with operations and business owners, evidence retention, forensic readiness indicators, and post-incident review processes to ensure lessons learned and corrective actions are tracked to closure.

4.2 In-Scope Environments

The audit covered cybersecurity processes across the following environments:

1. **Core Information Technology Environment**
   This includes corporate endpoints, identity services, core internal systems, and enterprise tooling used to manage user accounts, devices, and operational changes. This environment typically includes on-premises infrastructure, enterprise management tooling, and hybrid connectivity to cloud services.

2. **Cloud Services Environment**
   This includes cloud infrastructure services, cloud platform services, and software-as-a-service solutions supporting identity, production workloads, logging, monitoring, and security operations. The audit focus includes cloud administrative access controls, administrative activity logging, and integration of cloud logs into centralized monitoring.

3. **Business-Critical Application Environment**
   This includes applications and data stores that support critical business functions and contain sensitive information, including customer platforms, enterprise resource planning systems, customer databases, and backup or recovery systems. The audit focus includes access governance for sensitive data, vulnerability remediation discipline for internet-facing services, and recovery readiness practices.

4.3 Out of Scope

The following activities were explicitly excluded from this audit:

1. **Penetration Testing and Exploit Validation**
   The audit did not include active exploitation, vulnerability exploitation validation, or offensive security testing against systems.

2. **Source Code Review and Secure Code Analysis**
   The audit did not include application source code review, static code analysis, software composition analysis, or secure development lifecycle assessment beyond what is reflected indirectly through vulnerability and patch management processes.

3. **Red Team Exercises and Adversary Simulation**
   The audit did not include adversary simulation, social engineering campaigns, attack chain simulation, or extended compromise testing.

5. PROCESS OWNERSHIP AND GOVERNANCE

This section clarifies ownership and governance expectations for the audited processes. Ownership is expressed as roles for portfolio purposes.

Process	Accountable Owner Role	Responsible Delivery Role	Governance Expectations
User and Access Management	Information Technology Security Lead	Information Technology Operations Manager	Access lifecycle governance, periodic access reviews, and evidence retention must be formally reviewed on a recurring basis and escalated when overdue.
Vulnerability and Patch Management	Information Technology Security Lead	Information Technology Operations Manager	Patch governance and verification discipline must be reviewed on a recurring basis, including exception handling, rework-to-closure discipline, and evidence retention.
Incident Handling and Response	Security Operations Center Lead	Security Operations Center Analysts and Incident Coordinators	Escalation readiness, logging coverage validation, and post-incident review tracking must be reviewed on a recurring basis with documented outcomes.

Governance note: The audit does not impose a numeric cadence in this portfolio project. “Recurring basis” indicates that governance must be scheduled, evidenced, and enforced.

6. EFFECTIVE PRACTICES OBSERVED

Based on evidence available in the portfolio project pack, the following effective practices were observed:

- Multi-factor authentication enforcement for privileged roles is implemented and supported by configuration evidence.
- Incident response playbooks exist and are structured to address common scenarios.
- Restoration testing evidence exists and indicates attention to recovery readiness.

These strengths should be maintained while addressing the gaps identified in findings and corrective actions.

7. ROOT CAUSE THEMES

The findings and risks in this report are driven by a small number of recurring root cause themes:

1. **Governance cadence is not consistently evidenced**
   Controls that require recurring activity (access reviews, logging coverage checks, post-incident reviews) are not consistently demonstrated through artefacts.
2. **Verification and closure discipline is incomplete**
   Patch verification and rework tracking are not implemented as mandatory workflow steps, which reduces confidence that remediation outcomes are sustained.
3. **Evidence retention is not standardized**
   Even where processes likely exist, inconsistent evidence retention prevents confirmation of operating effectiveness.
4. **Ownership for recurring controls is not sufficiently formalized**
   Controls requiring business owner attestations or ongoing validation lack consistently enforced accountability and escalation.

Corrective actions in this report are designed to address these systemic themes, not only individual symptoms.

8. ARTEFACT A - IN-SCOPE ASSET INVENTORY (A4-FRIENDLY)

Part 1 (Asset 001 to Asset 006)

Asset Identifier	Asset Name	Asset Owner Role	Data Sensitivity and Criticality	Environment
Asset 001	Identity Provider Service	Information Technology Security Lead	High sensitivity, critical business impact	Cloud software service
Asset 002	Human Resources System	Human Resources Operations Manager	High sensitivity, high business impact	Cloud software service
Asset 003	Corporate Endpoint Fleet	Information Technology Operations Manager	Medium sensitivity, high business impact	Core information technology
Asset 004	Core Enterprise Resource Planning System	Business Systems Owner	High sensitivity, critical business impact	Hybrid environment
Asset 005	Customer Portal Application	Product Owner	High sensitivity, critical business impact	Cloud platform service

Asset Identifier	Asset Name	Asset Owner Role	Data Sensitivity and Criticality	Environment
Asset 006	Customer Database	Data Platform Lead	High sensitivity, critical business impact	Cloud infrastructure service

Asset Identifier	Dependencies and Audit Notes
Asset 001	Depends on multi-factor authentication service, human resources identity feed, and centralized monitoring logs. Core identity governance and privileged access assurance.
Asset 002	Depends on identity provisioning integration. Primary trigger for joiner-mover-leaver lifecycle.
Asset 003	Depends on endpoint detection and response and patch management tooling. Used for endpoint coverage assurance indicators.
Asset 004	Depends on single sign-on integration and recovery tooling. High impact if access governance fails.
Asset 005	Internet-facing service. Patch discipline and logging completeness are critical due to exposure.
Asset 006	Sensitive data store. Least privilege, strong monitoring, and backup governance are critical.

Part 2 (Asset 007 to Asset 012)

Asset Identifier	Asset Name	Asset Owner Role	Data Sensitivity and Criticality	Environment
Asset 007	Security Information and Event Management Platform	Security Operations Center Lead	Medium sensitivity, high business impact	Cloud environment
Asset 008	Endpoint Detection and Response Platform	Security Operations Center Lead	Low sensitivity, high business impact	Cloud environment
Asset 009	Patch Management Platform	Information Technology Operations Manager	Low sensitivity, high business impact	Hybrid environment
Asset 010	Cloud Production Account	Cloud Platform Owner	High sensitivity, critical business impact	Cloud infrastructure and platform services

Asset Identifier	Asset Name	Asset Owner Role	Data Sensitivity and Criticality	Environment
Asset 011	Source Code Repository Platform	Engineering Manager	Medium sensitivity, high business impact	Cloud software service
Asset 012	Backup Vault and Recovery Store	Disaster Recovery Coordinator	High sensitivity, critical business impact	Hybrid environment

Asset Identifier	Dependencies and Audit Notes
Asset 007	Central evidence source for detection and response. Depends on identity, cloud, and endpoint logging sources.
Asset 008	Depends on endpoint agent deployment and connectivity. Used as endpoint detection coverage indicator.
Asset 009	Depends on endpoint and server inventory accuracy. Used for patch lifecycle governance indicators.
Asset 010	High-risk administrative environment. Requires complete administrative activity logging and privileged access governance.
Asset 011	Supports investigation traceability and containment. Depends on identity integration and audit logging.
Asset 012	Supports recovery readiness. Requires restoration testing and access governance due to sensitivity.

---

9. ARTEFACT B - CONTROL ASSESSMENT (UPDATED WITH OPERATING BASIS)

Part 1 (User and Access Management and Vulnerability and Patch Management)

Control Identifier	Control Description	Design Rating	Operating Rating	Implementation Status	Basis for Operating Effectiveness Conclusion
User Access 01	Access requests require documented approval and business justification	Adequate	Partially Effective	Partially Implemented	Workflow records in the portfolio project pack indicate approvals exist; justification is not consistently evidenced.

Control Identifier	Control Description	Design Rating	Operating Rating	Implementation Status	Basis for Operating Effectiveness Conclusion
User Access 02	Multi-factor authentication is enforced for privileged roles	Adequate	Effective	Implemented	Configuration evidence in the portfolio project pack supports enforcement for privileged roles.
User Access 03	Joiner-mover-leaver handling is integrated with the human resources identity feed and defined access removal service levels	Adequate	Partially Effective	Partially Implemented	Integration is indicated; consistent service level adherence evidence is not available in the portfolio project pack.
User Access 04	Periodic access reviews are performed for sensitive systems and privileged roles	Adequate	Ineffective	Not Implemented	Completed periodic access review packs are not available in the portfolio project pack.
User Access 05	Privileged accounts are separated from standard user accounts	Partially Adequate	Partially Effective	Partially Implemented	Account model indicators exist, but full separation and governance evidence is incomplete in the portfolio project pack.
Patch 01	Vulnerability intake and remediation ticket creation occur within defined expectations	Adequate	Effective	Implemented	Intake workflow indicators are available in the portfolio project pack and show structured triage initiation.

Part 2 (Vulnerability and Patch Management and Incident Handling and Response)

Control Identifier	Control Description	Design Rating	Operating Rating	Implementation Status	Basis for Operating Effectiveness Conclusion
Patch 02	Patch lifecycle governance includes testing, approvals, and deployment control	Adequate	Partially Effective	Partially Implemented	Governance indicators exist; end-to-end evidence is incomplete in the portfolio project pack.
Patch 03	Patch service level monitoring exists for internet-facing and internal services	Adequate	Partially Effective	Partially Implemented	Monitoring indicators exist; consistent evidence of exception escalation is incomplete in the portfolio project pack.
Patch 04	Patch verification is performed and failed patch rework is tracked to closure	Adequate	Ineffective	Not Implemented	Verification artefacts and rework-to-closure evidence are not available in the portfolio project pack.
Patch 05	Exception handling includes compensating controls and risk acceptance	Adequate	Partially Effective	Partially Implemented	Exception concept exists; evidence of formal risk acceptance and expiry governance is incomplete in the portfolio project pack.
Incident 01	Severity classification matrix and escalation path are maintained	Adequate	Partially Effective	Partially Implemented	Documentation exists; evidence of recurring roster validation is incomplete in the portfolio project pack.
Incident 02	Centralized logging covers identity, cloud administrative activity, and endpoints	Adequate	Partially Effective	Partially Implemented	Logging exists; evidence for complete production administrative logging coverage is incomplete in the portfolio project pack.
Incident 03	Incident response playbooks exist	Adequate	Effective	Implemented	Playbook evidence exists in the portfolio project pack and

Control Identifier	Control Description	Design Rating	Operating Rating	Implementation Status	Basis for Operating Effectiveness Conclusion
	and are tested through exercises				supports structured response preparation.
Incident 04	Forensic readiness includes retention and chain-of-custody practices	Partially Adequate	Partially Effective	Partially Implemented	Retention indicators exist; consistent chain-of-custody usage evidence is incomplete in the portfolio project pack.
Incident 05	Post-incident reviews are performed and corrective actions are tracked to closure	Adequate	Ineffective	Not Implemented	Post-incident review records and closure tracking artefacts are not available in the portfolio project pack.

---

10. ARTEFACT C - RISK REGISTER (A4-FRIENDLY)

Part 1 (Risk Summary)

Risk Identifier	Risk Statement	Risk Score	Risk Severity
Risk 01	Compromise of privileged accounts may enable administrative access to critical systems	15	High
Risk 02	Access for leavers and movers may not be revoked timely, enabling unauthorized persistence	16	High
Risk 03	Critical vulnerabilities may remain exploitable due to patch and verification gaps	25	High / Critical
Risk 04	Legacy or unpatchable assets may accumulate unmanaged risk without complete governance	20	High
Risk 05	Privilege creep may occur due to missing periodic access reviews	20	High
Risk 06	Incident escalation delays may increase outage duration and regulatory exposure	15	High
Risk 07	Incomplete cloud administrative logging may reduce detection and forensic capability	15	High

Part 2 (Risk Detail)

Risk Identifier	Key Assets	Threat Scenario	Likelihood	Impact	Common Vulnerability Scoring System Input
Risk 01	Asset 001, Asset 010, Asset 007	Credential theft and privileged misuse	3	5	Not applicable
Risk 02	Asset 001, Asset 002, Asset 004, Asset 006	Ex-employee retains sensitive access	4	4	Not applicable
Risk 03	Asset 005, Asset 010	Exploit of known vulnerability in exposed service	5	5	9.8
Risk 04	Asset 004, Asset 012	Legacy dependency prevents patching and is exploited	5	4	7.5
Risk 05	Asset 004, Asset 006	Privilege creep after role change	4	5	Not applicable
Risk 06	Asset 007, Asset 008, Asset 005	Account takeover and delayed escalation	3	5	Not applicable
Risk 07	Asset 010, Asset 007	Administrative actions not centrally logged	3	5	Not applicable

---

11. ARTEFACT D - AUDIT CHECKLIST (NO FABRICATED SAMPLE SIZES)

Test Identifier	Area	Test Procedure	Evidence Type Expected	Pass Criteria	Result
Test 01	User and Access Management	Verify access requests include approval and business justification	Access request workflow records	Approval and justification are present	Partially Met
Test 02	User and Access Management	Verify access removal for leavers follows the defined	Offboarding evidence and identity	Service level tracking exists and is consistently met	Partially Met

Test Identifier	Area	Test Procedure	Evidence Type Expected	Pass Criteria	Result
		service level process	deprovisioning indicators		
Test 03	Vulnerability and Patch Management	Verify patch service level monitoring exists for internet-facing services	Patch compliance reporting indicators	Monitoring exists and exceptions are acted upon	Partially Met
Test 04	Vulnerability and Patch Management	Verify patch verification and failed patch rework tracking exist	Verification artefacts and rework trail	Failed patches are tracked to closure	Not Met
Test 05	Incident Handling and Response	Verify cloud administrative activity logs are centralized	Central monitoring source list and cloud logging indicators	Coverage exists for production administrative activity	Partially Met
Test 06	Incident Handling and Response and Recovery	Verify restoration testing evidence exists and is current	Restoration testing artefacts	Restoration testing evidence is current and complete	Met

---

12. CORRECTIVE ACTION PLAN (UPDATED WITH DEPENDENCIES AND CLOSURE VALIDATION)

Note on target dates: The target dates below are proposed for portfolio illustration and are not based on measured delivery performance.

12.1 Closure Validation Approach

Closure of corrective actions will be validated through a combination of:

- Review of updated procedures and standards that define mandatory control steps
- Review of configuration exports and screenshots demonstrating control enforcement
- Review of governance artefacts demonstrating recurring execution and oversight
- Review of workflow records demonstrating evidence retention and tracking to closure

12.2 Implementation Dependencies and Sequencing Considerations (Added)

Corrective actions in this plan may depend on factors that commonly influence delivery in operational environments, such as:

- Availability of identity, patching, and logging tooling features required to enforce workflow steps

- Change management windows and operational stability requirements for production environments
- Coordination across multiple owners for shared services (for example, cloud platform, security operations, and information technology operations)
- Standardization of evidence retention expectations across teams and systems

These dependencies should be managed through governance oversight to prevent delays and to ensure that closure evidence reflects real operating effectiveness.

12.3 Corrective Action Plan Actions (A4-Friendly Part 1)

Corrective Action Identifier	Linked Risks	Corrective Action Description	Owner Role	Proposed Target Date	Priority
Corrective Action 01	Risk 03	Implement patch verification and ensure failed patch rework is tracked to closure	Information Technology Operations Manager	31 January 2026	Critical
Corrective Action 02	Risk 03	Implement an emergency patch playbook for critical internet-facing risks	Information Technology Security Lead	31 January 2026	Critical
Corrective Action 03	Risk 02, Risk 05	Implement periodic access review attestation with accountable business owner sign-off	Business Systems Owner	29 February 2026	High
Corrective Action 04	Risk 02	Implement monitoring for offboarding service level adherence and exception governance reporting	Information Technology Operations Manager	29 February 2026	High
Corrective Action 05	Risk 01	Remove dual-use administrative accounts and enforce separate privileged identities	Cloud Platform Owner	29 February 2026	High
Corrective Action 06	Risk 01	Implement time-bound privileged access elevation	Cloud Platform Owner	31 March 2026	High

12.4 Corrective Action Plan Actions (A4-Friendly Part 2)

Corrective Action Identifier	Linked Risks	Corrective Action Description	Owner Role	Proposed Target Date	Priority
Corrective Action 07	Risk 06	Update incident escalation roster and assign recurring review ownership	Security Operations Center Lead	31 January 2026	High
Corrective Action 08	Risk 06	Implement post-incident review process and track actions to closure	Security Operations Center Lead	29 February 2026	High
Corrective Action 09	Risk 07	Ensure cloud administrative logs are forwarded to centralized monitoring for full production scope	Cloud Platform Owner	31 January 2026	High
Corrective Action 10	Risk 04	Implement formal time-bound risk acceptance for unpatchable assets with expiry	Business Systems Owner	31 March 2026	High
Corrective Action 11	Risk 04	Implement compensating controls such as segmentation and enhanced monitoring for legacy systems	Information Technology Security Lead and Operations	31 March 2026	High

12.5 Closure Evidence Types

Corrective Action Identifier	Closure Evidence Type
Corrective Action 01	Updated procedure and workflow records showing verification used and rework items tracked to closure
Corrective Action 02	Approved playbook, exercise artefact, and emergency change evidence
Corrective Action 03	Signed attestation pack, evidence of access removals, and attestation tracker export
Corrective Action 04	Service level monitoring evidence, exception report, and governance review artefact
Corrective Action 05	Before and after identity export and updated privileged access standard
Corrective Action 06	Privileged elevation policy artefact, elevation log evidence, and governance report artefact

Corrective Action Identifier	Closure Evidence Type
Corrective Action 07	Updated roster evidence and escalation readiness drill artefact
Corrective Action 08	Post-incident review template, post-incident review records, and action tracker artefact
Corrective Action 09	Logging enabled evidence and centralized ingestion indicators
Corrective Action 10	Signed acceptance with expiry and reassessment checklist artefact
Corrective Action 11	Segmentation evidence and monitoring rule artefacts

13. RESIDUAL RISK OUTLOOK (ADDED)

Even if all corrective actions are implemented, some residual risk is expected to remain, consistent with real operating environments:

- **Legacy and unpatchable technology risk is rarely eliminated fully.** Compensating controls and time-bound risk acceptance reduce risk, but they do not remove inherent exposure.
- **Human process dependency remains a factor.** Access reviews, post-incident reviews, and logging coverage validation require recurring execution discipline and management oversight to remain effective.
- **Detection and response capability improves incrementally.** Centralized logging and improved post-incident learning reduce time-to-detection and time-to-recovery, but response outcomes remain dependent on preparedness, staffing, and escalation discipline.

Sustained reduction of residual risk will depend on governance, evidence retention, and recurring validation becoming embedded operational practice.

14. RISK HEAT MAP (QUALITATIVE)

14.1 Risk Coordinates

- Risk 01: Likelihood 3, Impact 5
- Risk 02: Likelihood 4, Impact 4
- Risk 03: Likelihood 5, Impact 5
- Risk 04: Likelihood 5, Impact 4
- Risk 05: Likelihood 4, Impact 5
- Risk 06: Likelihood 3, Impact 5
- Risk 07: Likelihood 3, Impact 5

14.2 Heat Map Matrix (Counts Per Cell)

Likelihood \ Impact	1	2	3	4	5
5	0	0	0	1	1
4	0	0	0	1	1
3	0	0	0	0	3
2	0	0	0	0	0
1	0	0	0	0	0

Heat map note: This matrix is a qualitative representation derived from the defined likelihood and impact model and the evidence available in the portfolio project pack.

14.3 Interpretation

The risk landscape is concentrated in high-impact areas. Priority improvements remain patch verification discipline, access review governance, logging completeness, and post-incident corrective action tracking.

15. MANAGEMENT RESPONSE (UPDATED TO BE MORE REALISTIC)

Item	Statement
Management response status	Accepted, with phased implementation based on operational priorities and change windows.
Implementation approach	Process owners will integrate workflow controls into operational tooling and define evidence retention expectations. Where tooling limitations exist, interim manual controls will be applied and documented until automated enforcement is feasible.
Target completion	Proposed target dates in the corrective action plan will be reviewed against delivery dependencies and operational constraints, and then confirmed through governance oversight.
Residual risk acceptance	Residual risk for legacy or unpatchable assets will require explicit business owner sign-off with time-bound expiry and documented compensating controls.

Item	Statement
Follow-up and validation	Closure will be validated using procedure updates, configuration evidence, governance records, and workflow artefacts demonstrating sustained execution.

16. FINAL OUTCOME

This audit produced a complete process assurance package across **User and Access Management**, **Vulnerability and Patch Management**, and **Incident Handling and Response**. The report provides a clear audit opinion, prioritized risks, corrective actions, operating effectiveness basis statements, and audit-grade findings without introducing fabricated operational metrics. Enhancements in this version improve realism, leadership readability, and closure governance expectations.

APPENDIX A - FINDINGS REGISTER (CRITERIA, CONDITION, CAUSE, IMPACT, RECOMMENDATION)

Finding 01 - Patch Verification and Failed Patch Rework Are Not Operating Effectively (High)

Criteria: National Institute of Standards and Technology Cybersecurity Framework 2.0 Protective Processes requires disciplined vulnerability and patch remediation governance including verification.
Condition: Evidence of patch verification and evidence of failed patch rework tracked to closure were not available in the portfolio project pack.
Cause: Verification responsibility and rework tracking are not embedded as mandatory steps in the patch workflow.
Impact: Increased likelihood of exploitation of known vulnerabilities, affecting confidentiality and integrity of customer-facing and cloud production systems, and increasing the chance of service disruption. Key assets impacted include the customer portal application and the cloud production account.
Recommendation: Implement a verification and rework-to-closure workflow and ensure evidence is retained and reported through governance mechanisms.

Finding 02 - Periodic Access Reviews for Sensitive Systems Are Not Implemented (High)

Criteria: National Institute of Standards and Technology Cybersecurity Framework 2.0 Access Control requires periodic review of access for sensitive systems and privileged roles to enforce least privilege.
Condition: Completed periodic access review packs were not available in the portfolio project pack for sensitive systems, including enterprise resource planning and customer database access.
Cause: Access review governance cadence is not enforced and accountable business ownership for access attestation is not established.

Impact: Privilege creep increases the likelihood of unauthorized access to sensitive business and customer data, impacting confidentiality and integrity. Key assets impacted include the enterprise resource planning system, the customer database, and privileged access in the cloud production account.
Recommendation: Implement periodic access attestation with accountable business owner sign-off and evidence retention.

Finding 03 - Timely Access Removal for Leavers and Movers Is Not Consistently Evidenced (High)

Criteria: National Institute of Standards and Technology Cybersecurity Framework 2.0 Access Control requires timely revocation of access aligned with joiner-mover-leaver lifecycle events.
Condition: Human resources integration exists; however, consistent evidence that access removal service levels are met and exceptions are governed was not available in the portfolio project pack.
Cause: Service level monitoring, alerting, and exception governance reporting are not institutionalized for offboarding processes.
Impact: Unauthorized access persistence risk increases, potentially enabling misuse or fraud and compromising confidentiality and integrity of sensitive systems. Key assets impacted include the identity provider service, the enterprise resource planning system, and the customer database.
Recommendation: Implement service level monitoring and recurring exception reporting to accountable owners, supported by evidence retention.

Finding 04 - Centralized Logging of Cloud Administrative Activity Is Incomplete (High)

Criteria: National Institute of Standards and Technology Cybersecurity Framework 2.0 Security Monitoring requires logging sufficient to detect anomalous activity and support investigation and forensic analysis.
Condition: Centralized monitoring exists, but evidence indicates a gap in coverage for cloud administrative activity logging across production scope in the portfolio project pack.
Cause: There is no recurring control to validate logging coverage and ensure all production administrative logs are forwarded to centralized monitoring.
Impact: Detection capability and investigation completeness are reduced, increasing the likelihood of prolonged compromise and extended service disruption. Key assets impacted include the cloud production account and the security information and event management platform.
Recommendation: Ensure cloud administrative logs are forwarded to centralized monitoring for full production scope and implement recurring coverage validation.

Finding 05 - Post-Incident Review and Corrective Action Tracking Are Not Operating (High)

Criteria: National Institute of Standards and Technology Cybersecurity Framework 2.0 Incident Response requires post-incident review practices and continuous improvement mechanisms.
Condition: Incident response playbooks exist; however, evidence of post-incident review records and corrective actions tracked to closure were not available in the portfolio project pack.

Cause: Post-incident review ownership and enforcement are not defined or not consistently applied.
Impact: Root causes remain unaddressed, increasing the probability of repeat incidents and longer recovery times, impacting availability and business continuity. Key assets impacted include the centralized monitoring platform, the endpoint detection and response platform, and customer-facing services.
Recommendation: Implement a post-incident review process, require documented reviews, and track corrective actions to closure with governance oversight.

APPENDIX B - CROSS-REFERENCE (FINDING TO CONTROLS, RISKS, AND CORRECTIVE ACTIONS)

Finding Identifier	Related Control Areas	Related Risk Identifiers	Related Corrective Actions
Finding 01	Patch service level governance; patch verification governance	Risk 03	Corrective Action 01; Corrective Action 02
Finding 02	Periodic access review governance	Risk 02; Risk 05	Corrective Action 03
Finding 03	Offboarding and access removal governance	Risk 02	Corrective Action 04
Finding 04	Centralized monitoring and logging coverage	Risk 07	Corrective Action 09
Finding 05	Post-incident review governance; escalation governance	Risk 06	Corrective Action 08; Corrective Action 07