ISO/IEC 27001:2022

INFORMATION SECURITY MANAGEMENT SYSTEM AUDIT & READINESS ASSESSMENT

2026 Illustrative Sample Deliverable

NorthBridge Digital Services, Inc.

Fictional U.S.-Based Technology & SaaS Organization

CONFIDENTIAL — SAMPLE / DEMONSTRATION

FICTIONAL SAMPLE REPORT — NOT AN ACTUAL ISO/IEC 27001 CERTIFICATION AUDIT

This document is a simulated ISO/IEC 27001:2022 ISMS Audit & Readiness Assessment created by TMG Security to demonstrate assessment methodology, control evaluation, and professional reporting standards. NorthBridge Digital Services, Inc. is fictional. No actual ISO/IEC 27001 certification audit was performed, and no ISO/IEC 27001 certificate was issued. TMG Security is not an accredited certification body and does not represent itself as one through this sample.

Assessment Period	01 Jan 2026 – 31 Aug 2026	**Report Date**	15 September 2026
Standard Basis	ISO/IEC 27001:2022 + Amd 1:2024	**Classification**	**Confidential**
Prepared By	TMG Security	**Assessment Type**	ISMS Audit & Readiness Assessment

Do not use as, or represent as, evidence of ISO/IEC 27001 certification. ***See Section 02 — Important Disclaimer.***

01 DOCUMENT CONTROL

Document Title	ISO/IEC 27001:2022 Information Security Management System Audit & Readiness Assessment — 2026 Illustrative Sample Deliverable
Document ID	TMG-ISO27001-NBDS-2026-001
Version	1.0
Issue Date	15 September 2026
Assessment Period	01 January 2026 – 31 August 2026
Assessment Type	ISO/IEC 27001:2022 ISMS Audit & Readiness Assessment (Illustrative Sample — Not a Certification Audit)
Classification	CONFIDENTIAL — SAMPLE / DEMONSTRATION
Organization Assessed	NorthBridge Digital Services, Inc. (Fictional)
Prepared By	TMG Security Assessment Team
Assessment Lead	TMG Security — Lead ISMS Assessor (Fictional Engagement Role)
Reviewed By	TMG Security Quality Assurance Lead
Approved By	TMG Security — Governance, Risk & Compliance Practice Lead
Document Owner	TMG Security — Governance, Risk & Compliance Practice

This document control record is itself illustrative and forms part of the fictional sample. Version history beyond v1.0 does not exist for this demonstration deliverable.

02 IMPORTANT DISCLAIMER

FICTIONAL SAMPLE REPORT — NOT AN ACTUAL ISO/IEC 27001 CERTIFICATION AUDIT

This report has been produced solely for demonstration and portfolio purposes on behalf of TMG Security. It is intended to illustrate the structure, depth, and professional standard of an ISO/IEC 27001:2022 ISMS Audit & Readiness Assessment deliverable. To ensure there is no ambiguity regarding the nature of this document, TMG Security sets out the following clarifications:

- NorthBridge Digital Services, Inc. is a fictional entity. It does not correspond to any real company, and any resemblance to an actual organization is purely coincidental.
- No actual ISO/IEC 27001 audit, certification audit, certification decision, or certificate issuance was performed or issued.
- No production environment, system, or network of any kind was accessed, scanned, or tested in the creation of this report.
- No real evidence was collected, and no actual personnel interviews occurred; the interview and evidence registers in this document are entirely fictional.
- All findings, risk ratings, dates, metrics, control statuses, and management responses contained in this report are illustrative and fictional. They were constructed to demonstrate realistic assessment and reporting conventions and do not describe any actual security or compliance condition.
- TMG Security is not an accredited ISO/IEC 27001 certification body and does not represent itself as one through this document. A formal certification decision must be made by an appropriately accredited independent certification body.
- This document is not evidence of ISO/IEC 27001 certification for any organization, real or fictional.
- The fictional tabletop exercise scenario referenced in Section 29 (Incident Management) is provided solely to demonstrate TMG Security's incident-readiness assessment methodology. No actual incident, breach, or security event occurred.
- This document does not reproduce the copyrighted text of ISO/IEC 27001:2022 or its amendments. Control references are cited by number; themes and audit interpretation are TMG Security's own concise, original summaries.

Intended Use

This sample report may be shared with prospective clients, partners, and other interested parties to illustrate TMG Security's ISMS assessment methodology, documentation standards, and reporting quality. It should not be relied upon for any compliance, legal, contractual, procurement, or certification decision. An actual ISO/IEC 27001 certification audit must be performed and a certification decision issued by an appropriately accredited independent certification body, and organizations should consult qualified legal and compliance counsel regarding their own ISMS readiness.

Current Standard Basis

This sample assessment is built around the current ISO/IEC 27001:2022 requirements and Annex A control set, together with ISO/IEC 27001:2022/Amendment 1:2024 (the climate-action amendment to Clauses 4.2 and 6.1.3, addressed in Section 57). ISO/IEC 27001:2013 is referenced in this report only where relevant for historical context and is never presented as the current assessment basis.

TABLE OF CONTENTS

03 EXECUTIVE SUMMARY

TMG Security has prepared this fictional, illustrative ISO/IEC 27001:2022 ISMS Audit & Readiness Assessment sample to represent NorthBridge Digital Services, Inc., a hypothetical U.S.-based enterprise SaaS and cloud technology company. This section presents a fictional executive-level summary of the simulated ISMS assessment, prepared in the style and format TMG Security would use for an actual readiness engagement ahead of a future independent certification audit.

ALL METRICS, FINDINGS, AND SCORES ON THIS PAGE ARE FICTIONAL SAMPLE DATA

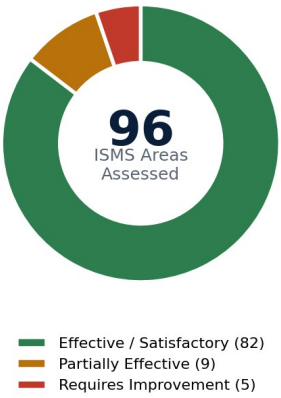
Overall Illustrative ISMS Readiness

PARTIALLY READY

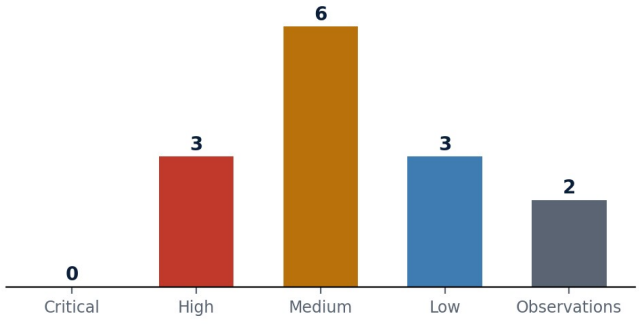
NorthBridge's simulated ISMS demonstrates a mature foundational governance, risk-management and control program, with a defined set of fictional gaps requiring remediation before proceeding to an actual independent certification audit. This illustrative status reflects a sample readiness assessment and does not represent an ISO certification decision.

Fictional Sample Dashboard

Illustrative ISMS Control & Area Effectiveness



Illustrative Findings by Severity (14 Total)



Executive Risk Narrative

The fictional ISO/IEC 27001:2022 ISMS readiness assessment reviewed 96 illustrative ISMS areas — 90 applicable Annex A:2022 controls plus 6 management-system process areas spanning Clauses 4 through 10 — sampling evidence across the 01 January 2026 – 31 August 2026 assessment period rather than evaluating design alone. No sampled area was rated Critical. Three High-severity findings concern enterprise risk treatment tracking discipline, privileged access recertification evidence across cloud and database administrative tiers, and delayed supplier security reassessments. Six Medium-severity findings span internal audit follow-up verification, vulnerability remediation exception governance, backup restoration evidence, security awareness completion tracking, asset inventory reconciliation, and change management security-review evidence. Three Low-severity findings reflect narrower documentation-consistency gaps, and two forward-looking observations note opportunities to further automate ISMS metrics and standardize management review reporting.

Across these fictional results, NorthBridge's simulated program shows particular strength in governance and leadership commitment, its policy framework, incident management, business continuity, and its core technical control baseline (identity, monitoring, and cloud security). Developing areas include risk-treatment evidence discipline, privileged-access governance, and supplier-reassessment cadence enforcement — the pattern TMG Security would expect to identify and help remediate during a readiness engagement conducted ahead of an organization's first, or a subsequent, independent ISO/IEC 27001 certification audit. TMG Security's simulated recommendation is that NorthBridge prioritize closure of the three High-severity findings within the first 30 days of the fictional remediation roadmap (see Sections 45–47), with

remaining items addressed across a 90-day window, ahead of engaging an accredited certification body for an actual certification audit.

04 ASSESSMENT OVERVIEW

This fictional engagement simulates a TMG Security ISMS Audit & Readiness Assessment: a structured evaluation of an organization's information security management system against the ISO/IEC 27001:2022 requirements and Annex A control set, performed in advance of — and to prepare for — an actual independent certification audit. The assessment combines document review, simulated interviews, illustrative technical evidence sampling, and Annex A control testing to form an evidence-based, illustrative view of ISMS design and operating effectiveness.

Assessment Objectives

- Evaluate ISMS governance, leadership commitment, and organizational context definition.
- Evaluate the ISMS scope statement and boundary rationale.
- Evaluate the risk assessment methodology and its consistent application.
- Evaluate the risk treatment plan and treatment-tracking discipline.
- Evaluate control implementation across the Annex A:2022 control set (A.5–A.8).
- Assess the Statement of Applicability for completeness and justification quality.
- Evaluate internal audit programme design and execution.
- Evaluate management review inputs, outputs, and follow-through.
- Evaluate documented information control (approval, versioning, retention).
- Identify gaps and provide a prioritized, illustrative remediation roadmap.
- Assess overall readiness for a future formal ISO/IEC 27001:2022 certification audit.

This sample does not constitute an actual ISO/IEC 27001 certification audit and does not result in a certification decision.

05 ORGANIZATION PROFILE

NorthBridge Digital Services, Inc. is a fictional U.S.-based technology organization headquartered in Denver, Colorado, providing enterprise SaaS applications, cloud-hosted platforms, API services, analytics capabilities, and identity integrations to approximately 2,700 fictional enterprise and mid-market customers. The organization employs approximately 900 fictional personnel across engineering, security, GRC, sales, customer support, and corporate functions.

Industry	Cloud Software / SaaS / Enterprise Technology
Headquarters	Denver, Colorado, USA
Employees	Approximately 900
Customers	Approximately 2,700 enterprise and mid-market customers
Assessment Period	01 January 2026 – 31 August 2026
Services	Enterprise SaaS platform, cloud-hosted business applications, API services, analytics and reporting, identity/IAM integrations, enterprise customer support
Information Processed	Business information, customer information, employee information, authentication data, operational/application data, logs, confidential business information

Fictional Technology Environment

NorthBridge's fictional technology environment spans AWS cloud infrastructure, Kubernetes/containerized workloads, PostgreSQL databases, cloud object storage, API gateways, CI/CD pipelines, Git-based source control, an enterprise identity provider with MFA enforcement, EDR and SIEM platforms, a vulnerability management programme, endpoint management, an ITSM platform, backup and disaster recovery tooling, and a defined set of critical third-party SaaS providers. All technology environment details are fictional and constructed for demonstration purposes.

06 ISMS CONTEXT

Clause 4.1 requires an organization to determine internal and external issues relevant to its purpose and that affect its ability to achieve the intended outcomes of its ISMS. The fictional context analysis below was constructed for NorthBridge Digital Services, Inc. and reviewed as part of this illustrative sample.

Issue	Type	Description	ISMS Relevance
Enterprise SaaS market competition	External	Increasing customer expectations for demonstrable, independently assessed security assurance.	Elevates the priority of ISMS maturity and future certification readiness.
Evolving cloud threat landscape	External	Continued growth in credential-based attacks, ransomware, and cloud misconfiguration exploitation.	Informs risk assessment inputs and technical control prioritization.
Customer contractual security requirements	External	Enterprise customers increasingly require security addenda, questionnaires, and evidence of control operation.	Drives SoA scope and evidence-retention discipline.
Regulatory and privacy expectations	External	Sector-applicable data protection expectations relevant to customer and employee personal information.	Informs the interface between the ISMS and privacy obligations (A.5.34).
Climate-related operational disruption	External	Increasing frequency of extreme-weather events affecting cloud region availability and workforce continuity.	Considered within business continuity planning and the 2024 Amendment 1 climate-action lens (see Section 58).
Rapid engineering headcount growth	Internal	NorthBridge's engineering organization has grown materially over the past 18 (fictional) months.	Increases onboarding, access provisioning, and secure-development training volume.
Multi-team ownership of cloud infrastructure	Internal	Infrastructure responsibility is distributed across several engineering sub-teams.	Introduces asset inventory and configuration-consistency challenges (ISMS-M-008).
GRC platform adoption still maturing	Internal	The organization's centralized GRC platform was adopted after several ISMS processes were already established.	Explains several evidence-retention and tracking findings identified in this sample (ISMS-H-001, ISMS-M-004).
Distributed / remote workforce model	Internal	A meaningful proportion of NorthBridge personnel work remotely on a regular basis.	Elevates the importance of endpoint, remote-access, and awareness controls.
Multiple critical third-party dependencies	Internal	Core service delivery depends on a small number of critical infrastructure and identity suppliers.	Elevates supplier risk management as a priority ISMS focus area.

A dedicated treatment of the climate-related external issue and its consideration under ISO/IEC 27001:2022/Amendment 1:2024 is provided in Section 57 (Regulatory / Standards Watch — 2026).

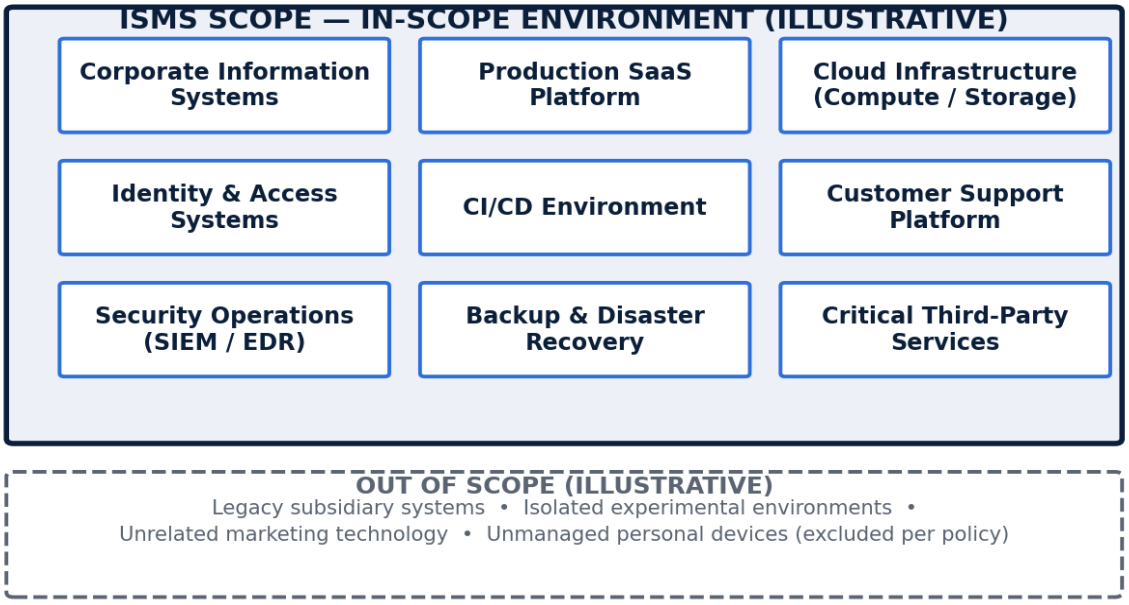
07 INTERESTED PARTIES

Clause 4.2 requires an organization to determine interested parties relevant to the ISMS and their relevant requirements. The fictional interested-party analysis below reflects NorthBridge's illustrative stakeholder landscape.

Interested Party	Expectation / Requirement	Security Relevance	ISMS Response	Owner
Customers (Enterprise & Mid-Market)	Confidentiality and availability of business data hosted on the platform	Direct — core to service commitments and contractual obligations	SoA-mapped technical/organizational controls; customer-facing security documentation	CISO
Employees & Contractors	Clear security expectations, training, and fair disciplinary process	Direct — human-layer control effectiveness	Security Awareness Policy, onboarding programme, Acceptable Use Policy	HR Manager
Executive Leadership & Board	Visibility into ISMS risk posture and resourcing needs	Direct — governance and resource allocation	Quarterly management review, risk register reporting	CISO
Regulators (Sector-Applicable)	Demonstrable, risk-based information security practices	Indirect — contextual compliance posture	Legal/regulatory requirement register maintained under A.5.31	GRC Manager
Contractual Partners / Channel Resellers	Assurance that shared data and integrations are appropriately protected	Direct — contractual security clauses	Standard security addenda in partner agreements	Procurement Lead
Suppliers & Subprocessors	Clear security requirements and reasonable audit/reporting expectations	Direct — supply-chain risk management	Supplier Security Policy, risk-tiered onboarding and reassessment	Procurement Lead
Cloud Infrastructure Providers	Shared-responsibility clarity and configuration diligence	Direct — shared control boundary	Shared responsibility matrix maintained as part of the ISMS scope statement	Cloud Infrastructure Lead
Independent Auditors (Internal & Future External)	Accurate, evidenced representation of ISMS design and operation	Direct — audit readiness	Internal audit programme, evidence register, control testing register	Internal Audit Lead
Cyber Insurers	Demonstrable baseline security controls supporting underwriting	Indirect — informs coverage terms	Security control summary and incident history shared during renewal	CISO
Shareholders / Investors	Reasonable assurance that security risk is identified and managed	Indirect — enterprise risk oversight	Risk register and ISMS performance summarized to leadership	CEO

08 ISMS SCOPE & BOUNDARIES

Clause 4.3 requires the organization to determine the boundaries and applicability of the ISMS to establish its scope. NorthBridge's fictional ISMS scope statement covers the systems, teams, and processes involved in delivering its production SaaS platform to enterprise and mid-market customers.



Illustrative ISMS Scope Boundary — Fictional Environment

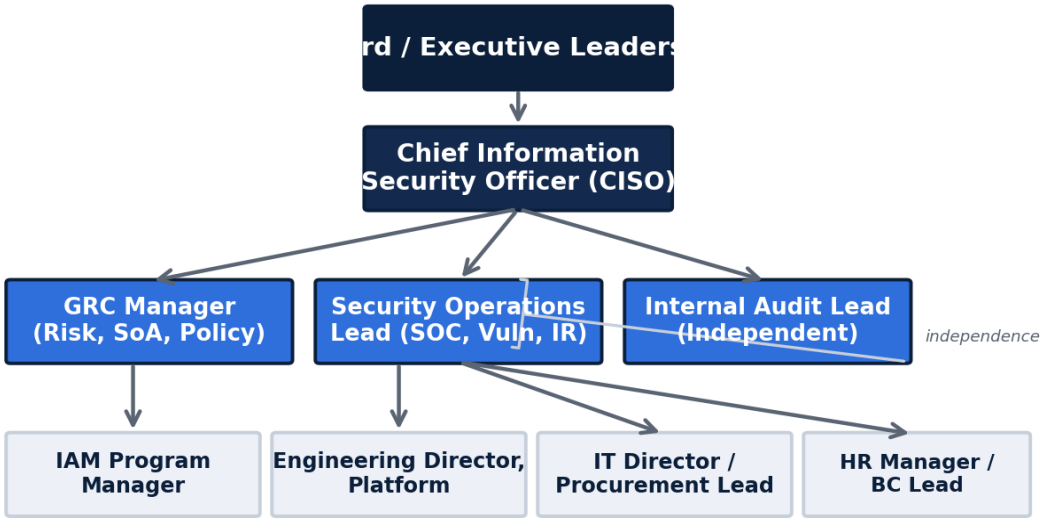
Boundary Rationale

In-scope components were selected because they directly process, store, or transmit customer or business information in support of NorthBridge's production service commitments. Out-of-scope components were excluded because they are legacy, isolated, or do not process in-scope information — a rationale documented in the fictional ISMS Scope Statement (EV-002) and reviewed annually alongside the organizational context analysis.

Cloud infrastructure is included within scope under a shared-responsibility model: NorthBridge is responsible for configuration, access control, and application-layer security, while the underlying cloud infrastructure provider is responsible for physical and environmental controls at the facility level (see Section 23 — Physical Security, and the Section 09 subservice-organization treatment within Section 28).

09 LEADERSHIP & GOVERNANCE

Clause 5 requires top management to demonstrate leadership and commitment to the ISMS. This fictional assessment reviewed NorthBridge's governance structure, policy approval process, resource allocation, and management communication practices.



Illustrative ISMS Governance & Reporting Structure — Fictional Organization

Illustrative Assessment Observations

- Executive leadership formally approves the Information Security Policy annually and reviews ISMS performance quarterly through a defined governance forum.
- The CISO holds documented authority over ISMS resourcing decisions and reports governance status directly to executive leadership.
- Security objectives are communicated to the workforce through onboarding, the intranet policy portal, and periodic all-hands updates.
- Internal Audit maintains independence from the security operations function it reviews, reporting findings directly to the CISO and, where material, to executive leadership.

Governance and leadership commitment were assessed as Effective for this fictional sample; no findings were raised against this section.

10 INFORMATION SECURITY POLICY FRAMEWORK

Clause 5.2 and Annex A.5.1 address the establishment of an information security policy set approved by management. NorthBridge's fictional policy hierarchy comprises a top-level Information Security Policy supported by a set of topic-specific policies, all clearly identified below as illustrative sample documents.

Policy (Illustrative Sample Document)	Purpose	Review Cycle
Information Security Policy	Top-level policy establishing ISMS commitment and structure	Annual
Access Control Policy	Governs identity, authentication, and access provisioning	Annual
Asset Management Policy	Governs asset inventory, ownership, and classification	Annual
Cryptography Policy	Governs encryption and key management practices	Annual
Incident Response Policy	Governs incident classification, escalation, and response	Annual
Business Continuity Policy	Governs continuity planning and disaster recovery	Annual
Supplier Security Policy	Governs supplier risk classification and reassessment	Annual
Vulnerability Management Policy	Governs scanning, prioritization, and remediation SLAs	Annual
Secure Development Policy	Governs the secure SDLC and change management	Annual
Acceptable Use Policy	Governs acceptable use of information and assets	Annual
Data Classification Policy	Governs classification and labelling of information	Annual
Backup Policy	Governs backup frequency, retention, and testing	Annual

Policy (Illustrative Sample Document)	Purpose	Review Cycle
Logging & Monitoring Policy	Governs log generation, retention, and review	Annual
Risk Management Policy	Governs risk methodology and treatment tracking	Annual

All policies listed above are illustrative sample documents referenced for this fictional assessment (see EV-001). No actual policy text is reproduced in this report.

11 ROLES, RESPONSIBILITIES & AUTHORITIES

Clause 5.3 requires top management to assign and communicate responsibilities and authorities for roles relevant to information security. The fictional RACI matrix below (R = Responsible, A = Accountable, C = Consulted, I = Informed) illustrates how key ISMS activities are distributed across NorthBridge's fictional roles.

Activity	CEO	CISO	CIO	IT Director	SecOps Lead	GRC Manager	Eng Director	HR Manager	Procurement Lead	Privacy Officer	BC Lead	IA Lead
ISMS Policy Approval	A	R	C	I	I	C	I	I	I	I	I	I
Risk Assessment & Treatment	I	A	C	C	C	R	C	I	C	C	C	I
Statement of Applicability Maintenance	I	A	C	I	C	R	C	I	I	I	I	C
Incident Response	I	A	C	C	R	C	C	I	I	I	C	I
Internal Audit Programme	I	A	I	C	C	C	C	I	I	I	I	R
Management Review	A	R	C	C	C	C	C	C	C	C	C	C
Supplier Risk Management	I	A	I	I	C	C	I	I	R	I	I	I
Access Control Administration	I	A	C	C	R	C	C	I	I	I	I	I
Business Continuity Planning	A	C	C	C	C	C	R	I	I	I	R	I
Security Awareness Training	I	A	I	I	C	C	I	R	I	I	I	I
Corrective Action Management	I	A	I	C	C	R	C	I	I	I	I	C

12 RISK MANAGEMENT METHODOLOGY

Clause 6.1.2 requires the organization to define and apply an information security risk assessment process. NorthBridge's fictional methodology identifies risks, analyzes likelihood and impact, determines inherent and residual risk, and assigns treatment decisions and ownership.

Risk Identification	Threats and vulnerabilities relevant to information assets are identified through asset review, threat intelligence, incident history, and stakeholder input.
Risk Analysis	Likelihood and impact are rated using the 5x5 scale below to determine inherent risk.
Risk Evaluation	Inherent risk is compared against NorthBridge's fictional risk acceptance criteria to determine treatment priority.
Risk Treatment	A treatment decision (reduce, avoid, transfer, or accept) is documented, mapped to relevant Annex A controls, and assigned an owner and target date.
Residual Risk	Risk remaining after treatment is documented and monitored; residual risk above the acceptance threshold requires management sign-off.
Risk Acceptance	Residual risks within tolerance are formally accepted by the designated risk owner and recorded in the risk register.

Likelihood & Impact Scales

Likelihood	Impact
Rare	Insignificant
Unlikely	Minor
Possible	Moderate
Likely	Major
Almost Certain	Severe

13 INFORMATION SECURITY RISK ASSESSMENT

The fictional enterprise risk register below reflects 12 illustrative information security risks identified for NorthBridge Digital Services, Inc. as part of this sample assessment. Each risk is analyzed for likelihood, impact, and inherent/residual risk, with treatment ownership assigned.

ISMS-RSK-001 — Unauthorized Access to Customer Systems	
Threat	External attacker or malicious insider
Vulnerability	Excessive or stale privileged access rights
Likelihood / Impact	Possible / Major
Inherent Risk	High
Existing Controls	MFA enforcement, RBAC, quarterly access reviews, centralized SSO
Residual Risk	Medium
Treatment	Reduce — strengthen privileged access recertification evidence
Owner / Target Date	IAM Program Manager | 31 Oct 2026
Related Control(s) / Finding	A.8.2, A.5.18 | ISMS-H-002

ISMS-RSK-002 — Compromised Privileged Account	
Threat	Credential theft via phishing or credential stuffing
Vulnerability	Incomplete privileged-account recertification evidence
Likelihood / Impact	Possible / Major
Inherent Risk	High
Existing Controls	MFA, privileged session monitoring, EDR, SIEM alerting
Residual Risk	Medium
Treatment	Reduce — complete IAM governance platform migration for privileged tiers
Owner / Target Date	Security Operations Lead | 31 Oct 2026
Related Control(s) / Finding	A.8.2, A.8.5 | ISMS-H-002

ISMS-RSK-003 — Ransomware Affecting Production Environment	
Threat	Ransomware operator
Vulnerability	Backup restoration evidence gaps for a secondary database
Likelihood / Impact	Unlikely / Severe
Inherent Risk	High
Existing Controls	EDR, immutable backup architecture, network segmentation, SIEM monitoring
Residual Risk	Medium
Treatment	Reduce — consolidate backup restoration testing and evidence retention
Owner / Target Date	Engineering Director, Platform | 15 Dec 2026
Related Control(s) / Finding	A.8.13, A.8.7 | ISMS-M-006

ISMS-RSK-004 — Third-Party Security Failure	
Threat	Supplier compromise or control regression
Vulnerability	Delayed supplier security reassessment
Likelihood / Impact	Possible / Major
Inherent Risk	High
Existing Controls	Supplier risk classification, onboarding due diligence, contractual security clauses
Residual Risk	Medium
Treatment	Reduce — automate reassessment-due alerting and complete overdue reassessments
Owner / Target Date	Procurement Lead | 15 Dec 2026
Related Control(s) / Finding	A.5.19, A.5.22 | ISMS-H-003

ISMS-RSK-005 — Cloud Misconfiguration	
Threat	Human error during infrastructure change
Vulnerability	Configuration baseline documentation gaps
Likelihood / Impact	Possible / Moderate

Inherent Risk	Medium
Existing Controls	Infrastructure-as-code peer review, CSPM scanning, change management workflow
Residual Risk	Low
Treatment	Reduce — enforce baseline documentation updates within change workflow
Owner / Target Date	Cloud Infrastructure Lead | 31 Dec 2026
Related Control(s) / Finding	A.8.9, A.8.32 | No named finding in this sample

ISMS-RSK-006 — Insufficient Vulnerability Remediation	
Threat	Exploitation of a known, unremediated vulnerability
Vulnerability	SLA-exceeding findings without documented exception approval
Likelihood / Impact	Possible / Major
Inherent Risk	High
Existing Controls	Continuous vulnerability scanning, patch management programme, EDR
Residual Risk	Medium
Treatment	Reduce — automate exception-record generation and leadership sign-off
Owner / Target Date	Security Operations Lead | 30 Nov 2026
Related Control(s) / Finding	A.8.8 | ISMS-M-005

ISMS-RSK-007 — Inadequate Backup Recovery	
Threat	Data loss following system failure or attack
Vulnerability	Restoration evidence not consistently retained
Likelihood / Impact	Unlikely / Major
Inherent Risk	Medium
Existing Controls	Encrypted, geographically replicated backups; defined RTO/RPO objectives
Residual Risk	Low
Treatment	Reduce — centralize restoration testing calendar and evidence repository
Owner / Target Date	Engineering Director, Platform | 15 Dec 2026
Related Control(s) / Finding	A.8.13, A.8.14 | ISMS-M-006

ISMS-RSK-008 — Security Incident Detection Delay	
Threat	Slow detection allowing an intrusion to dwell undetected
Vulnerability	Alert triage coverage variability during reduced-staffing periods
Likelihood / Impact	Unlikely / Major
Inherent Risk	Medium
Existing Controls	Centralized SIEM, 24x7 alerting, defined escalation procedures
Residual Risk	Low
Treatment	Accept with monitoring — maintain current SOC staffing model and escalation testing
Owner / Target Date	Security Operations Lead | N/A — accepted, monitored quarterly
Related Control(s) / Finding	A.8.16, A.5.25 | No named finding in this sample

ISMS-RSK-009 — Insufficient Employee Security Awareness	
Threat	Social engineering, phishing
Vulnerability	Overdue training completion not centrally visible
Likelihood / Impact	Possible / Moderate
Inherent Risk	Medium
Existing Controls	Annual role-based training, quarterly phishing simulations, onboarding training
Residual Risk	Low
Treatment	Reduce — integrate LMS overdue data into centralized GRC reporting
Owner / Target Date	HR Manager | 31 Jan 2027
Related Control(s) / Finding	A.6.3 | ISMS-M-007

ISMS-RSK-010 — Improper Information Classification	
Threat	Inadvertent disclosure of confidential information
Vulnerability	Inconsistent application of the classification scheme in newer analytics workflows

Likelihood / Impact	Unlikely / Moderate
Inherent Risk	Low
Existing Controls	Data Classification Policy, DLP tooling, access restrictions by classification tier
Residual Risk	Low
Treatment	Accept with monitoring — reinforce classification training during onboarding and refreshers
Owner / Target Date	GRC Manager | N/A — accepted, monitored annually
Related Control(s) / Finding	A.5.12, A.5.13 | No named finding in this sample

ISMS-RSK-011 — Supplier Access Not Adequately Reviewed	
Threat	Excessive or unreviewed supplier access to NorthBridge systems
Vulnerability	Supplier evidence formatting inconsistency complicating review
Likelihood / Impact	Unlikely / Moderate
Inherent Risk	Medium
Existing Controls	Supplier access provisioning workflow, periodic access review, offboarding checklist
Residual Risk	Low
Treatment	Reduce — standardize supplier evidence template and retrofit existing files
Owner / Target Date	Procurement Lead | 30 Jun 2027
Related Control(s) / Finding	A.5.20, A.8.3 | ISMS-L-012

ISMS-RSK-012 — Unauthorized Software Deployment	
Threat	Deployment bypassing security review
Vulnerability	Change workflow does not enforce a security-review gate
Likelihood / Impact	Unlikely / Moderate
Inherent Risk	Medium
Existing Controls	Peer code review, CI/CD pipeline controls, environment separation
Residual Risk	Low
Treatment	Reduce — implement system-enforced security-review gate in change workflow
Owner / Target Date	Engineering Director, Platform | 15 Dec 2026
Related Control(s) / Finding	A.8.32, A.8.31 | ISMS-M-009

14 RISK TREATMENT PLAN

Clause 6.1.3 requires the organization to define and apply a risk treatment process, including formulation of a risk treatment plan. The fictional treatment plan below summarizes treatment actions for the highest-priority risks identified in Section 13.

Risk	Treatment Option	Action	Control Mapping	Owner	Target Date
ISMS-RSK-001	Reduce	strengthen privileged access recertification evidence	A.8.2, A.5.18	IAM Program Manager	31 Oct 2026
ISMS-RSK-002	Reduce	complete IAM governance platform migration for privileged tiers	A.8.2, A.8.5	Security Operations Lead	31 Oct 2026
ISMS-RSK-003	Reduce	consolidate backup restoration testing and evidence retention	A.8.13, A.8.7	Engineering Director, Platform	15 Dec 2026
ISMS-RSK-004	Reduce	automate reassessment-due alerting and complete overdue reassessments	A.5.19, A.5.22	Procurement Lead	15 Dec 2026
ISMS-RSK-005	Reduce	enforce baseline documentation updates within change workflow	A.8.9, A.8.32	Cloud Infrastructure Lead	31 Dec 2026
ISMS-RSK-006	Reduce	automate exception-record generation and leadership sign-off	A.8.8	Security Operations Lead	30 Nov 2026
ISMS-RSK-007	Reduce	centralize restoration testing calendar and evidence repository	A.8.13, A.8.14	Engineering Director, Platform	15 Dec 2026
ISMS-RSK-008	Accept with monitoring	maintain current SOC staffing model and escalation testing	A.8.16, A.5.25	Security Operations Lead	N/A — accepted, monitored quarterly
ISMS-RSK-009	Reduce	integrate LMS overdue data into centralized GRC reporting	A.6.3	HR Manager	31 Jan 2027
ISMS-RSK-010	Accept with monitoring	reinforce classification training during onboarding and refreshers	A.5.12, A.5.13	GRC Manager	N/A — accepted, monitored annually
ISMS-RSK-011	Reduce	standardize supplier evidence template and retrofit existing files	A.5.20, A.8.3	Procurement Lead	30 Jun 2027
ISMS-RSK-012	Reduce	implement system-enforced security-review	A.8.32, A.8.31	Engineering Director,	15 Dec 2026

Risk	Treatment Option	Action	Control Mapping	Owner	Target Date
		gate in change workflow		Platform	

Each risk treatment action is approved by the designated risk owner and reviewed quarterly at the ISMS governance forum. Treatment actions remain open until residual risk is confirmed within NorthBridge's fictional risk acceptance criteria.

15 STATEMENT OF APPLICABILITY

Clause 6.1.3(d) requires the organization to produce a Statement of Applicability (SoA) documenting the necessary Annex A controls, their justification for inclusion, whether they are implemented, and justification for exclusions. The fictional SoA below covers all 93 Annex A:2022 controls for NorthBridge's illustrative environment. Control themes are TMG Security's own concise, paraphrased summaries and do not reproduce the copyrighted standard text.

Ref.	Control Theme (TMG Summary)	Applic.	Justification	Status	Finding
A.5.1	Establishing and maintaining a top-level information security policy set, approved by management	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.2	Defining and allocating information security roles and responsibilities across the organization	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.3	Segregating conflicting duties and areas of responsibility to reduce misuse opportunity	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.4	Management reinforcing security expectations through visible ongoing direction and support	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.5	Maintaining appropriate contact with relevant authorities (law enforcement, regulators)	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.6	Maintaining contact with security interest groups, forums and professional associations	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.7	Collecting and analyzing threat intelligence relevant to the organization's environment	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.8	Embedding information security considerations into project management practices	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.9	Maintaining an inventory of information and other associated assets, with owners	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Partially Effective	ISMS-M-008
A.5.10	Defining acceptable use rules for information and associated assets	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.11	Ensuring personnel and third parties return organizational assets upon change or termination	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.12	Classifying information according to confidentiality, integrity and availability needs	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.13	Labelling information consistently with its classification scheme	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.14	Protecting information during transfer, internally and with external parties	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.15	Establishing rules to control logical and physical access based on business need	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.16	Managing the full lifecycle of identities used to access organizational systems	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.17	Controlling allocation and management of authentication information	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.18	Provisioning, reviewing, modifying and revoking access rights per business need	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.19	Managing information security risk associated with the use of supplier products and services	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.20	Agreeing relevant security requirements with each supplier based on risk	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Partially Effective	ISMS-L-012
A.5.21	Managing information security risk within the ICT supply chain	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.22	Monitoring, reviewing and managing change in supplier service delivery	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Requires Improvement	ISMS-H-003
A.5.23	Managing information security for the acquisition and use of cloud services	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.24	Planning and preparing for the management of information security incidents	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.25	Assessing and deciding the classification of information security events	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.26	Responding to information security incidents per documented procedures	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.27	Using knowledge gained from incidents to strengthen controls	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.28	Establishing procedures for the identification, collection and preservation of evidence	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.29	Maintaining an appropriate level of information security during disruption	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.30	Planning ICT readiness to support business continuity objectives	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.31	Identifying and meeting legal, statutory, regulatory and contractual security requirements	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.32	Protecting intellectual property rights relevant to the organization	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.33	Protecting records from loss, destruction, falsification and unauthorized access	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.34	Identifying and meeting privacy and personal-information-protection requirements	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Requires Improvement	—
A.5.35	Conducting independent review of the information security approach	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.36	Verifying compliance with information security policies, rules and standards	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.5.37	Documenting and maintaining operating procedures for information-	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment	Effective	—

Ref.	Control Theme (TMG Summary)	Applic.	Justification	Status	Finding
	processing facilities		and organizational operations.		
A.6.1	Performing background verification checks on candidates prior to employment	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.6.2	Stating personnel and contractor security responsibilities in terms of employment	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.6.3	Providing personnel with appropriate security awareness, education and training	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Partially Effective	ISMS-M-007
A.6.4	Maintaining a formal, communicated process for addressing policy violations	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.6.5	Defining security responsibilities and duties that remain valid after termination or change	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.6.6	Identifying and applying confidentiality or non-disclosure agreements	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.6.7	Applying security measures when personnel work remotely	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.6.8	Providing a mechanism for personnel to report observed or suspected security events	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.7.1	Defining and using security perimeters to protect areas containing information assets	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.7.2	Controlling physical entry to secure areas through appropriate entry controls	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Partially Effective	ISMS-L-011
A.7.3	Designing and applying physical security for offices, rooms and facilities	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.7.4	Monitoring premises continuously for unauthorized physical access	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.7.5	Designing and implementing protection against physical and environmental threats	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.7.6	Designing and applying security measures for working in secure areas	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.7.7	Defining clear desk and clear screen rules for information and associated assets	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.7.8	Siting and protecting equipment appropriately	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.7.9	Protecting off-site assets, taking into account differing off-premises risks	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.7.10	Managing storage media through its lifecycle in line with the classification scheme	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.7.11	Protecting information-processing facilities from utility service failures	No	Facility power, cooling and utility services for in-scope production infrastructure are provided and managed by the underlying cloud infrastructure provider under a shared-responsibility model; NorthBridge does not operate its own data center facilities.	Not Applicable	—
A.7.12	Protecting cabling carrying power or data from interception, interference or damage	No	Structured and power cabling for in-scope production infrastructure is owned and protected by the underlying cloud infrastructure provider; NorthBridge corporate office cabling is assessed separately as a lower-risk, non-production asset.	Not Applicable	—
A.7.13	Maintaining equipment correctly to ensure availability, integrity and confidentiality	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.7.14	Verifying that storage media are securely disposed of or re-used	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.1	Protecting information stored on, processed by or accessible via user endpoint devices	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.2	Restricting and managing the allocation and use of privileged access rights	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Requires Improvement	ISMS-H-002
A.8.3	Restricting access to information and associated assets per the access control policy	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.4	Appropriately managing read and write access to source code, tools and libraries	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.5	Implementing secure authentication technologies and procedures	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.6	Monitoring and adjusting resource use in line with current and expected capacity needs	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.7	Implementing protection against malware, supported by user awareness	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.8	Obtaining information about technical vulnerabilities and evaluating exposure	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Partially Effective	ISMS-M-005
A.8.9	Managing configurations, including security configurations, for hardware and software	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Requires Improvement	—
A.8.10	Deleting information held in systems, devices or storage media when no longer required	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.11	Using data masking in line with the access control policy and business requirements	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.12	Applying measures to detect and prevent unauthorized disclosure of information	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.13	Maintaining and regularly testing backup copies of information, software and systems	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Partially Effective	ISMS-M-006
A.8.14	Implementing redundancy sufficient to meet availability requirements	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.15	Producing, storing, protecting and analyzing logs of relevant activity	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.16	Monitoring networks, systems and applications for anomalous behaviour	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.17	Synchronizing clocks of information-processing systems to approved time sources	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—

Ref.	Control Theme (TMG Summary)	Applic.	Justification	Status	Finding
A.8.18	Restricting and tightly controlling the use of privileged utility programs	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.19	Controlling the installation of software on operational systems	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.20	Managing and controlling networks and network devices to protect information	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.21	Identifying, implementing and monitoring security mechanisms for network services	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.22	Segregating groups of information services, users and systems on networks	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.23	Managing access to external websites to reduce exposure to malicious content	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.24	Defining and implementing rules for the effective use of cryptography	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.25	Applying rules for the secure development of software and systems	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.26	Identifying and specifying information security requirements for applications	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.27	Establishing and applying secure system engineering principles	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.28	Applying secure coding principles to software development	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.29	Defining and implementing security testing processes in the development lifecycle	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.30	Directing, monitoring and reviewing outsourced system development activity	No	NorthBridge's fictional software development is performed entirely by internal engineering teams during the assessment period; no development activity was outsourced to a third party.	Not Applicable	—
A.8.31	Separating development, test and production environments	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.32	Subjecting changes to information-processing facilities to formal change control	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Partially Effective	ISMS-M-009
A.8.33	Selecting, protecting and managing test information appropriately	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—
A.8.34	Planning and agreeing audit and assurance testing to minimize disruption to production	Yes	Applicable to NorthBridge's in-scope cloud SaaS environment and organizational operations.	Effective	—

Summary: of 93 Annex A controls considered, 90 were determined applicable to NorthBridge's illustrative environment and 3 were determined not applicable, each with a documented fictional justification. A consolidated numerical summary is presented in Section 55 (Statement of Applicability Summary).

16 ISMS OBJECTIVES & PERFORMANCE METRICS

Clause 6.2 requires the organization to establish measurable information security objectives. NorthBridge's fictional 2026 ISMS objectives focus on improving vulnerability remediation discipline, MFA coverage, security awareness completion, supplier reassessment coverage, incident response exercise coverage, backup recovery validation, and corrective action closure — each tracked through the illustrative KPI dashboard below.

KPI / KRI (Illustrative)	Target	Actual	Status
MFA Coverage (Workforce Identities)	100%	**100%**	On Target
Vulnerability SLA Compliance (Critical/High)	≥ 95%	**88%**	Below Target
Security Training Completion (Annual)	≥ 98%	**94%**	Below Target
Supplier Reassessment Coverage (High/Medium Tier)	100%	**58%**	Below Target
Incident Exercise Completion (Planned Exercises)	100%	**100%**	On Target
Backup Restoration Test Success Rate	100%	**97%**	Near Target
Corrective Action Closure Rate (On-Time)	≥ 90%	**76%**	Below Target
Internal Audit Programme Completion	100%	**100%**	On Target

KPI targets shown above are NorthBridge's own fictional organizational targets and are not mandated by ISO/IEC 27001. All figures are illustrative sample data.

17 COMPETENCE, AWARENESS & COMMUNICATION

Clause 7.2–7.4 and Annex A.6.3 address ensuring personnel are competent, aware of the ISMS, and that relevant internal/external communications occur. This fictional assessment reviewed NorthBridge's onboarding, role-based training, annual awareness, and phishing simulation programme.

- New-hire onboarding includes mandatory security awareness training completed within the first 5 business days of employment.
- Annual role-based training is assigned by job function, with additional privileged-user training for administrative and engineering roles.
- Quarterly phishing simulations are conducted across the workforce, with individual results routed to line managers.
- Policy acknowledgement is captured electronically and retained in the LMS for audit purposes.
- Internal communication of ISMS objectives and updates occurs via the intranet policy portal, onboarding, and periodic all-hands briefings.

Illustrative Evidence: EV-020 (Security Awareness Records) — see also ISMS-M-007 (Section 41) regarding overdue-completion tracking visibility.

18 DOCUMENTED INFORMATION

Clause 7.5 requires the organization to maintain documented information required by the ISMS and by the standard, with appropriate identification, format, review, and control. This fictional assessment reviewed document approval, version control, access, retention, and change control practices for a sample of controlled ISMS documents.

- Controlled documents are maintained in a centralized document management platform with defined owner, approver, and review-cycle metadata.
- Prior versions are retained for audit-trail purposes; obsolete documents are marked and access-restricted rather than deleted.
- Document access is role-restricted consistent with the information classification scheme.
- A sample of 18 controlled documents was reviewed for version metadata consistency — see ISMS-L-010 (Section 41) for the identified exception.

19 OPERATIONAL PLANNING & CONTROL

Clause 8.1 requires the organization to plan, implement, and control the processes needed to meet ISMS requirements and to implement the risk treatment plan. This fictional assessment reviewed how NorthBridge plans and resources the execution of risk treatment actions and operational security processes.

- Risk treatment actions are resourced through the quarterly engineering and security planning cycle, with owners assigned per the risk treatment plan (Section 14).
- Outsourced processes relevant to the ISMS (see Section 28 — Supplier & Third-Party Security) are controlled through contractual security requirements and periodic reassessment.
- Planned changes to the ISMS scope, technology environment, or risk landscape are reviewed for security impact prior to implementation.

Operational planning and control were assessed as Effective for this fictional sample; execution-level gaps identified elsewhere in this report (for example, ISMS-H-001) relate to tracking discipline rather than the planning process itself.

20 ASSET MANAGEMENT

Annex A.5.9–A.5.11 address maintaining an inventory of information and associated assets, acceptable use, and return of assets. This fictional assessment reviewed NorthBridge's asset inventory covering cloud assets, endpoints, applications, databases, and network components.

Asset Category	Ownership	Classification Approach	Lifecycle Control
Cloud Compute & Storage	Cloud Infrastructure Lead	By data sensitivity tier	Provisioning/decommission tracked in IaC
Endpoints (Laptops)	IT Director	Standard corporate asset	MDM-enrolled lifecycle tracking
Applications	Engineering Director, Platform	By customer-data exposure	SDLC-tracked from design to retirement
Databases	Cloud Infrastructure Lead	Confidential / Restricted	Access-restricted, encrypted, backed up

Asset Category	Ownership	Classification Approach	Lifecycle Control
Network Components	Security Operations Lead	Infrastructure-critical	Configuration-managed and monitored

A sample reconciliation between the central asset inventory and a live cloud resource export identified a gap for auto-scaled analytics resources — see ISMS-M-008 (Section 41).

21 ACCESS CONTROL & IDENTITY MANAGEMENT

Annex A.5.15–A.5.18 and A.8.2–A.8.5 address access control rules, identity lifecycle management, authentication information, access rights, and privileged access. This fictional assessment reviewed joiner/mover/leaver workflows, SSO/MFA enforcement, role-based access control, privileged accounts, and periodic access recertification.

- Joiner/mover/leaver workflows are integrated with HR system-of-record triggers for standard workforce access.
- SSO and MFA are enforced organization-wide for access to in-scope systems (see TST-13, Section 53 — no exceptions identified in this sample).
- Role-based access control (RBAC) is applied consistent with least-privilege principles across the production environment.
- Standard user access is recertified quarterly with consistently retained evidence; privileged access recertification evidence retention requires improvement — see ISMS-H-002 (Section 41).
- Service accounts and break-glass emergency access are inventoried separately with additional monitoring controls applied.

Illustrative Evidence: EV-008 (Access Review Records), EV-009 (MFA Configuration), EV-010 (Privileged Access Review)

22 CRYPTOGRAPHY

Annex A.8.24 addresses the effective use of cryptography, including key management. This fictional assessment reviewed NorthBridge's illustrative approach to encryption at rest, encryption in transit, key management, certificate management, and secrets management. Specific cryptographic algorithms referenced below reflect NorthBridge's organizational policy rather than a mandatory ISO/IEC 27001 requirement.

Encryption at Rest	Production databases and object storage encrypted using organization-standard algorithms per internal Cryptography Policy.
Encryption in Transit	TLS enforced for all external and internal service-to-service communication carrying in-scope data.
Key Management	Centralized key management service with defined rotation schedule and access-restricted key administration.
Certificate Management	Automated certificate issuance and renewal for production endpoints, with expiry monitoring and alerting.
Secrets Management	Application secrets and credentials stored in a centralized secrets manager rather than in source code or configuration files.

Cryptography and key management were assessed as Effective for this fictional sample; no findings were raised against this section (see EV-029).

23 PHYSICAL SECURITY

Annex A.7 addresses physical and environmental security, including facility access, monitoring, and equipment protection. NorthBridge's fictional corporate offices maintain physical controls, while facility-level utility and cabling controls for production infrastructure are the responsibility of the underlying cloud infrastructure provider under a shared-responsibility model (A.7.11 and A.7.12 are accordingly assessed as Not Applicable for NorthBridge directly — see Section 15).

- Badge-controlled entry with visitor sign-in and escort requirements at all NorthBridge corporate office locations.
- CCTV monitoring of primary entry points at the corporate headquarters.

- Clear desk and clear screen expectations documented in the Acceptable Use Policy and reinforced through awareness training.
- Secure disposal procedures for storage media and end-of-life equipment, including certificate-of-destruction retention.
- Monthly visitor log review by the facilities coordinator — retention gap identified for 2 of 6 sampled months; see ISMS-L-011 (Section 41).

Illustrative Evidence: EV-028 (Physical Security Procedures)

24 SECURITY OPERATIONS

Annex A.8.7, A.8.16, and related technological controls address malware protection, monitoring, and operational security. This fictional assessment reviewed NorthBridge's SIEM, EDR, endpoint security, threat detection, and alert escalation practices.

- Centralized SIEM aggregates logs across infrastructure, application, and endpoint layers with defined correlation rules.
- EDR is deployed across all managed endpoints with automated containment capability for confirmed malware detections.
- A defined escalation matrix routes High/Critical alerts to on-call Security Operations personnel with documented response-time targets.
- Security metrics (alert volume, mean time to triage, false-positive rate) are reviewed monthly by the Security Operations Lead.

Alert triage timeliness was tested for a sample of 25 High/Critical SIEM alerts in a representative month with no exceptions identified (see TST-14, Section 53).

25 LOGGING & MONITORING

Annex A.8.15–A.8.17 address producing, protecting, and analyzing logs, monitoring activities, and clock synchronization. This fictional assessment reviewed NorthBridge's log generation, retention, protection, and review practices.

Log Generation	Application, infrastructure, and identity systems generate structured logs forwarded to the centralized SIEM.
Log Retention	Logs retained for a defined organizational period consistent with investigative and contractual needs.
Log Protection	Log storage is access-restricted and write-once for the active retention window to reduce tampering risk.
Clock Synchronization	Production systems synchronize to a common trusted time source to support reliable log correlation.
Monitoring Review	Security metrics and monitoring coverage are reviewed monthly; anomalies are escalated per the incident response procedure.

Illustrative Evidence: EV-013 (SIEM Configuration), EV-014 (EDR Configuration). Logging and monitoring were assessed as Effective for this fictional sample.

26 VULNERABILITY MANAGEMENT

Annex A.8.8 addresses obtaining information about technical vulnerabilities and evaluating exposure. This fictional assessment reviewed NorthBridge's vulnerability discovery, scanning, prioritization, remediation, and exception governance practices. Remediation SLAs referenced below are NorthBridge's own organizational policy and are not mandated by ISO/IEC 27001.

- Continuous automated vulnerability scanning covers cloud infrastructure, containers, and web application layers.

- Findings are risk-rated and prioritized using a fictional internal SLA: Critical within 15 days, High within 30 days (organizational policy, not an ISO-mandated deadline).
- Third-party/supplier-reported vulnerabilities are triaged through the same governance process as internally discovered findings.
- SLA-exceeding findings require a documented, approved exception; testing identified 9 individual findings without a retained exception record — see ISMS-M-005 (Section 41).

Illustrative Evidence: EV-011 (Vulnerability Scan Reports), EV-012 (Penetration Test Reports)

27 SECURE DEVELOPMENT & CHANGE MANAGEMENT

Annex A.8.25–A.8.32 address the secure development lifecycle, application security requirements, secure coding, environment separation, and change management. This fictional assessment reviewed NorthBridge's SDLC controls and change management workflow.

- Security requirements are incorporated into the design phase for customer-facing features handling in-scope data.
- Peer code review is mandatory prior to merge; automated dependency and static-analysis scanning run within the CI/CD pipeline.
- Development, test, and production environments are logically and access-separated.
- Changes classified Medium risk or higher require a documented security-review sign-off prior to production deployment; testing identified 3 of 15 sampled tickets without a retained sign-off — see ISMS-M-009 (Section 41).
- Rollback procedures are documented and tested as part of the standard deployment runbook.

Illustrative Evidence: EV-026 (Change Management Records), EV-027 (Secure Development Records)

28 SUPPLIER & THIRD-PARTY SECURITY

Annex A.5.19–A.5.22 address managing information security risk in supplier relationships, contractual security requirements, ICT supply chain risk, and ongoing monitoring/reassessment of supplier services. This fictional assessment reviewed NorthBridge's supplier onboarding, risk classification, and reassessment practices.

Supplier Category	Service	Risk Tier	Reassessment Status
Cloud Infrastructure Provider	Primary cloud compute, storage and networking	High	Current
Identity Provider	Enterprise SSO and identity federation	High	Current
SIEM / Security Monitoring Provider	Centralized log aggregation and alerting platform	High	Current
Backup & Recovery Provider	Off-site encrypted backup replication	High	Current
Customer Support Platform	Enterprise customer ticketing and support portal	Medium	Current
CRM Platform	Sales and customer relationship management	Medium	Overdue — see ISMS-H-003
Code Repository & CI/CD Platform	Source control and build/deployment pipeline	High	Current
HR / Payroll Platform	Human resources and payroll processing	Medium	Overdue — see ISMS-H-003
Email & Collaboration Provider	Corporate email and collaboration suite	Medium	Current
Vulnerability Scanning Provider	Continuous external and internal vulnerability scanning	Medium	Current

Do not fabricate certifications for real vendors: supplier entries above represent generic fictional service categories, not named real companies. Reassessment coverage gaps are addressed under ISMS-H-003 and ISMS-L-012 (Section 41).

29 INCIDENT MANAGEMENT

Annex A.5.24–A.5.28 address planning and preparing for incident management, event assessment, incident response, learning from incidents, and evidence collection. This fictional assessment reviewed NorthBridge's incident classification, detection, escalation, containment, investigation, and lessons-learned practices.

- Incidents are classified by severity (Low/Medium/High/Critical) with defined response-time expectations per tier.

- Detection sources include SIEM alerting, EDR containment events, and workforce-reported events via the security event reporting channel (A.6.8).
- A documented post-incident review process captures lessons learned and feeds corrective actions into the ISMS improvement cycle.

Fictional Tabletop Exercise Scenario

FICTIONAL SCENARIO — NO ACTUAL INCIDENT OCCURRED

Scenario: A simulated phishing campaign results in a fictional compromised workforce credential. The tabletop exercise walks the fictional incident response team through detection (SIEM alert on anomalous login geography), triage, containment (forced credential reset and session revocation), investigation (scope-of-access review), and stakeholder communication — concluding with a fictional lessons-learned session.

This fictional tabletop exercise is provided solely to demonstrate TMG Security's incident-readiness assessment methodology. Illustrative Evidence: EV-015 (Incident Response Plan), EV-016 (Incident Exercise Records).

30 BUSINESS CONTINUITY & DISASTER RECOVERY

Annex A.5.29–A.5.30 address maintaining information security during disruption and ICT readiness for business continuity. This fictional assessment reviewed NorthBridge's business impact analysis, recovery objectives, backup architecture, and disaster recovery testing programme.

Business Impact Analysis	Critical services identified and prioritized annually, informing recovery objective assignment.
Recovery Objectives (Illustrative, Organizational)	Target RTO of 4 hours and RPO of 1 hour for services classified as business-critical (organizational commitment, not an ISO-mandated figure).
Backup Architecture	Encrypted, geographically replicated backups with immutability enabled for critical databases.
Restoration Testing	Quarterly restoration testing required for business-critical databases; a secondary reporting database showed evidence gaps — see ISMS-M-006 (Section 41).
DR Exercise Programme	Annual full-failover exercise and semi-annual tabletop exercises for critical service dependencies.

Illustrative Evidence: EV-017 (Backup Test Records), EV-018 (Disaster Recovery Plan), EV-030 (Business Continuity Test Results).

31 INFORMATION SECURITY INCIDENT READINESS

This section evaluates NorthBridge's fictional overall readiness to detect, respond to, and recover from information security incidents, complementing the process review in Section 29.

- Detection readiness: centralized SIEM/EDR coverage with a documented escalation matrix supports timely detection across the in-scope environment.
- Response readiness: an incident response plan is documented, current, and was exercised through the fictional tabletop scenario noted in Section 29.
- Communication readiness: stakeholder and, where applicable, customer notification procedures are documented within the incident response plan.
- Recovery readiness: recovery procedures are integrated with the business continuity and backup restoration programmes (Section 30).

Overall incident readiness was assessed as Effective for this fictional sample. The one identified gap — documentation completeness for tabletop exercise records — is addressed as ISMS-M-004-adjacent internal audit follow-up discipline rather than a distinct incident-readiness control exception in this sample.

32 PRIVACY & DATA PROTECTION INTERFACE

Annex A.5.34 addresses identifying and meeting privacy and personal-information-protection requirements. This fictional assessment reviewed the interface between NorthBridge's ISMS and its handling of personal information belonging to customers, employees, and contacts.

- Personal information is classified consistent with the Data Classification Policy and subject to access restrictions by classification tier.
- Retention schedules for personal information are documented and reviewed alongside the broader records-retention programme (A.5.33).
- Third-party processing of personal information is governed through the supplier security programme (Section 28), with confidentiality and data-handling clauses included in applicable agreements.
- A sample review of 8 fictional data-processing workflows identified 2 instances where personal-information handling documentation had not been refreshed following a platform change — see the A.5.34 assessment in Section 56 (Annex A Control Matrix).

This section addresses the ISMS interface with privacy obligations only; it does not constitute a comprehensive privacy compliance assessment against any specific data protection regulation.

33 INTERNAL AUDIT PROGRAMME

Clause 9.2 requires the organization to conduct internal audits at planned intervals to determine whether the ISMS conforms to its own requirements and to ISO/IEC 27001:2022, and is effectively implemented and maintained. NorthBridge's fictional internal audit programme covers 12 illustrative audit areas across the assessment period, executed by an Internal Audit Lead maintaining independence from the functions audited.

Audit Area	Frequency	Scope	Result	Follow-Up
Access Control & Identity Management	Annual	Standard and privileged access provisioning, review, and termination	Partial Conformity	Scheduled Q1 2027
Risk Management & Treatment	Annual	Risk assessment methodology, register, and treatment tracking	Partial Conformity	Scheduled Q1 2027
Supplier Security Management	Annual	Onboarding due diligence, risk classification, reassessment cadence	Partial Conformity	Scheduled Q1 2027
Vulnerability & Patch Management	Semi-Annual	Scanning coverage, SLA governance, exception documentation	Partial Conformity	Scheduled Q4 2026
Backup & Business Continuity	Annual	Backup testing, restoration evidence, DR/BC test programme	Partial Conformity	Scheduled Q1 2027
Security Awareness & Training	Annual	Training assignment, completion tracking, escalation	Partial Conformity	Scheduled Q1 2027
Change Management & Secure Development	Semi-Annual	Change ticket workflow, security review evidence, SDLC controls	Partial Conformity	Scheduled Q4 2026
Physical Security	Annual	Facility access, visitor management, equipment disposal	Partial Conformity	Scheduled Q1 2027
Documented Information Control	Annual	Policy/procedure version control, approval, retention	Partial Conformity	Scheduled Q1 2027
Incident Management	Annual	Incident response plan, exercise records, lessons-learned process	Conformity	N/A
Cryptography & Key Management	Annual	Encryption standards, key lifecycle, certificate management	Conformity	N/A
Asset Management	Semi-Annual	Asset inventory accuracy, ownership, classification	Partial Conformity	Scheduled Q4 2026

34 INTERNAL AUDIT RESULTS

These classifications (Conformity / Partial Conformity / Nonconformity / Observation / Opportunity for Improvement) are illustrative consulting classifications used for this fictional sample. They do not represent an accredited certification-body determination.

Three internal audit cycles were conducted across the fictional assessment period, sampling the 12 audit areas listed in Section 33. Results are classified below.

Classification	Count	Description
Conformity	2	The sampled area met defined ISMS requirements with no exceptions identified.
Partial Conformity	10	The sampled area substantially met defined requirements with one or more evidenced exceptions requiring corrective action.
Nonconformity	0	No sampled area showed a systemic failure to meet a defined ISMS requirement in this fictional sample.
Observation	2	Forward-looking notes not tied to a documented requirement exception.
Opportunity for Improvement	3	Suggestions to strengthen an already-conforming control area.

Partial Conformity findings above correspond to the 10 Medium/High/Low-severity findings detailed in Section 41; the internal audit follow-up verification gap itself is captured as ISMS-M-004.

35 MANAGEMENT REVIEW

Clause 9.3 requires top management to review the ISMS at planned intervals to ensure its continuing suitability, adequacy, and effectiveness. NorthBridge's fictional Q3 2026 management review considered the status of previous actions, changes in context, risk status, security objectives, audit results, incidents, supplier performance, resource requirements, and improvement opportunities.

Illustrative Q3 2026 Management Review Action Table

Action Item	Owner	Target Date	Status
Approve migration of risk treatment tracking to the centralized GRC platform	GRC Manager	15 Nov 2026	Open
Approve IAM governance platform extension to privileged account tiers	IAM Program Manager	31 Oct 2026	Open
Approve automated supplier reassessment-due alerting	Procurement Lead	15 Dec 2026	Open
Review Q3 2026 security metrics dashboard and confirm KPI ownership	CISO	Completed	Closed
Confirm resourcing for 2027 internal audit programme	CEO	Completed	Closed
Evaluate automated ISMS metrics tooling for 2027 roadmap	GRC Manager	30 Jun 2027	Open

Illustrative Evidence: EV-023 (Management Review Minutes).

36 PERFORMANCE EVALUATION

Clause 9.1 requires the organization to evaluate ISMS performance and the effectiveness of the management system. This fictional assessment reviewed trend data across KPIs (Section 16), risk register status (Section 13), incident history (Section 29), vulnerability management performance (Section 26), and internal audit trends (Section 34).

- KPI trends show consistent MFA and incident-exercise completion, with developing performance in vulnerability SLA compliance and supplier reassessment coverage (Section 16).
- Risk trend analysis shows 12 tracked enterprise risks with residual risk trending toward Low/Medium as treatment actions progress (Section 13).
- Internal audit trend analysis shows a consistent 'Partial Conformity' pattern concentrated in evidence-retention and tracking discipline rather than control design (Section 34).

Performance evaluation practices themselves were assessed as Partially Effective for this fictional sample, reflecting the internal audit follow-up tracking gap (ISMS-M-004) rather than a deficiency in the evaluation methodology.

37 CONTINUAL IMPROVEMENT

Clause 10 requires the organization to continually improve the suitability, adequacy, and effectiveness of the ISMS, including through corrective action on nonconformities. This fictional assessment reviewed NorthBridge's corrective action process, root-cause analysis discipline, and use of lessons learned.

- Corrective actions are logged in a centralized register with owner, target date, and required verification evidence (Section 44).
- Root-cause analysis is performed for High-severity findings using a 5-Whys approach (Section 43).
- Lessons learned from incidents (Section 29) and internal audits (Section 34) feed into the annual policy and control review cycle.
- Two forward-looking observations in this sample (ISMS-O-013, ISMS-O-014) identify opportunities to further mature ISMS metrics automation and management review standardization.

Continual improvement practices were assessed as Partially Effective for this fictional sample, reflecting the metrics-automation and dashboard-standardization observations rather than a control exception.

38 ANNEX A CONTROL ASSESSMENT

This fictional assessment evaluated all 93 Annex A:2022 controls across the four control themes — A.5 Organizational, A.6 People, A.7 Physical, and A.8 Technological — determining applicability, implementation status, and, where applicable, illustrative testing results. The full 93-control assessment is presented in the Statement of Applicability (Section 15) and the Annex A Control Matrix (Section 56); this section summarizes results by theme and highlights representative illustrative examples.

Control Theme	Total	Applic.	N/A	Effective	Partial	Improve.
A.5 Organizational	37	37	0	33	2	2
A.6 People	8	8	0	7	1	0
A.7 Physical	14	12	2	11	1	0
A.8 Technological	34	33	1	28	3	2

A.5 Organizational: Organizational controls address policy, governance, asset management, access control policy, supplier relationships, incident management planning, business continuity, and compliance — 37 controls (A.5.1–A.5.37).

A.6 People: People controls address screening, employment terms, awareness/training, disciplinary process, remote working, and event reporting — 8 controls (A.6.1–A.6.8).

A.7 Physical: Physical controls address facility perimeters, entry control, environmental protection, equipment security, and secure disposal — 14 controls (A.7.1–A.7.14).

A.8 Technological: Technological controls address endpoint protection, access management, cryptography, operations security, network security, and secure development — 34 controls (A.8.1–A.8.34).

Representative Illustrative Testing Examples

Ref.	Control Theme	Illustrative Testing Result	Status	Finding
A.5.9	Maintaining an inventory of information and other associated assets, with owners	7 of 10 sampled asset categories reconciled to the live cloud resource inventory; 3 categories showed count variances.	Partially Effective	ISMS-M-008
A.5.22	Monitoring, reviewing and managing change in supplier service delivery	Of 12 High/Medium risk-tier suppliers due for reassessment in the period, 5 lacked a completed and retained reassessment record.	Requires Improvement	ISMS-H-003
A.6.3	Providing personnel with appropriate security awareness, education and training	Of 900 fictional personnel, completion tracking for 20 sampled overdue-training exceptions was not centrally visible to the GRC function.	Partially Effective	ISMS-M-007
A.7.2	Controlling physical entry to secure areas through appropriate entry controls	Visitor log review for a sample of 6 months found 2 months where the completed visitor-log review sign-off was not retained.	Partially Effective	ISMS-L-011
A.7.11	Protecting information-processing facilities from utility service failures	—	Not Applicable	—
A.8.2	Restricting and managing the allocation and use of privileged access rights	Of 8 quarterly privileged-access recertification cycles sampled across cloud, container and database administrative tiers, 3 cycles lacked a retained, signed reviewer attestation.	Requires Improvement	ISMS-H-002
A.8.8	Obtaining information about technical vulnerabilities and evaluating exposure	Of 6 monthly vulnerability remediation cycles sampled, 9 individual Critical/High findings exceeded the internal SLA without a retained, approved exception record.	Partially Effective	ISMS-M-005
A.8.30	Directing, monitoring and reviewing outsourced system development activity	—	Not Applicable	—

39 EVIDENCE & SAMPLING METHODOLOGY

TMG Security's fictional assessment methodology combines multiple evidence-gathering techniques to form an evidence-based, illustrative view of ISMS design and operation. All evidence referenced throughout this report is illustrative sample data — see the notice below.

All evidence referenced in this report — document excerpts, interview outcomes, technical configuration summaries, and testing results — is illustrative sample data. No actual client evidence was collected or reviewed.

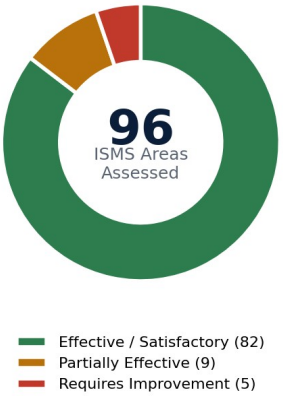
Document Review	Inspection of policies, procedures, registers, and records against the applicable clause or control requirement.
Interview	Simulated discussions with fictional role holders to corroborate documented process design and actual practice.
Observation	Simulated observation of a process being performed (for example, a change approval workflow) rather than relying on description alone.
Technical Evidence	Simulated configuration exports, scan reports, and system-generated logs supporting technical control claims.

Sampling	A defined population is identified for each tested control; a representative sample is selected (judgmental or random, as appropriate) and results are extrapolated with the sample size and rationale disclosed.
Walkthrough	Step-by-step simulated review of a process end-to-end to confirm consistency between documented and actual practice.
Configuration Review	Simulated inspection of system/application configuration settings against the applicable baseline or policy.
Testing	Structured procedures applied to a sample, with results, exceptions, and conclusions documented in the Control Testing Register (Section 53).
Management Records	Review of governance artifacts such as risk register entries, management review minutes, and corrective action records.

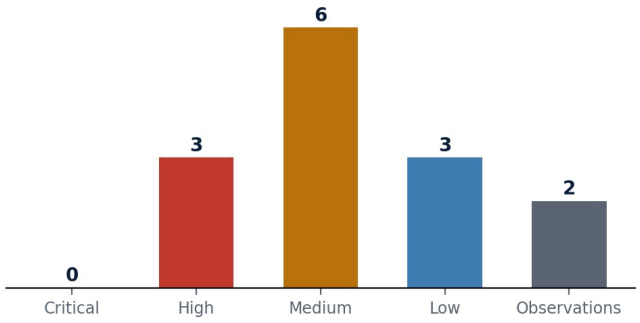
40 FINDINGS SUMMARY

This fictional sample identified 14 total findings and observations across the 96 illustrative ISMS areas assessed: 0 Critical, 3 High, 6 Medium, 3 Low, and 2 Observations. Every figure on this page reconciles to the Detailed Findings (Section 41), Finding Register (Section 54), Management Action Plan (Section 48), and Risk Heatmap (Section 42).

Illustrative ISMS Control & Area Effectiveness



Illustrative Findings by Severity (14 Total)



Findings by Clause / Annex A Area

Finding ID	Title	Clause / Annex A	Severity
ISMS-H-001	Enterprise Risk Treatment Tracking Not Consistently Updated	Clause 6.1.3	HIGH
ISMS-H-002	Privileged Access Recertification Evidence Incomplete	A.8.2 Privileged Access Rights	HIGH
ISMS-H-003	Supplier Security Reassessment Evidence Incomplete	A.5.22 Monitoring, Review and Change Management of Supplier Services	HIGH
ISMS-M-004	Internal Audit Follow-Up Tracking Inconsistent	Clause 9.2	MEDIUM
ISMS-M-005	Vulnerability Remediation Exception Documentation Incomplete	A.8.8 Management of Technical Vulnerabilities	MEDIUM
ISMS-M-006	Backup Restoration Evidence Not Consistently Retained	A.8.13 Information Backup	MEDIUM
ISMS-M-007	Security Awareness Completion Exceptions Not Centrally Tracked	A.6.3 Information Security Awareness, Education and Training	MEDIUM
ISMS-M-008	Asset Inventory Reconciliation Requires Improvement	A.5.9 Inventory of Information and Other Associated Assets	MEDIUM
ISMS-M-009	Change Management Security Review Evidence Inconsistent	A.8.32 Change Management	MEDIUM
ISMS-L-010	Document Version Metadata Inconsistency	Clause 7.5	LOW
ISMS-L-011	Physical Visitor Record Review Documentation Gap	A.7.2 Physical Entry	LOW
ISMS-L-012	Supplier Review Evidence Formatting Inconsistency	A.5.20 Addressing Information Security Within Supplier Agreements	LOW
ISMS-O-013	Opportunity to Improve ISMS Metrics Automation	Clause 9.1	OBSERVATION
ISMS-O-014	Opportunity to Improve Management Dashboard Standardization	Clause 9.3	OBSERVATION

41 DETAILED FINDINGS

Every fictional sample finding below is presented in full consulting-format detail: control objective, criteria, condition, cause, risk/business impact, evidence reference, recommendation, management response, owner, target date, status, and retest requirement. All findings, evidence, and management responses on this page are entirely fictional.

ILLUSTRATIVE EVIDENCE REFERENCE — NO ACTUAL CLIENT EVIDENCE

ISMS-H-001 — Enterprise Risk Treatment Tracking Not Consistently Updated	HIGH
Clause / Annex A Reference: Clause 6.1.3 / 8.3 — Risk Treatment (Management System Requirement)	**Illustrative Assessment Status: Requires Improvement**
Control Objective	Risk treatment actions arising from the ISMS risk assessment are tracked to completion, with current status, evidence, and residual risk maintained in the enterprise risk register.
Criteria	NorthBridge's Risk Management Policy requires the GRC Manager to update the risk treatment tracker within 10 business days of any treatment action status change, with quarterly reconciliation against the risk register.
Condition	Of 24 open risk treatment actions reviewed across the 01 Jan – 31 Aug 2026 assessment period, 9 actions had a tracker status that had not been updated for more than one full quarter, and 4 of those 9 had in fact progressed beyond the recorded status based on corroborating evidence found elsewhere (ticketing system, email confirmations).
Cause	Risk treatment status updates depend on manual entry by individual risk owners into a shared spreadsheet-based tracker; there is no automated linkage between the tracker and the underlying remediation systems (ticketing, IAM platform, vendor portal) that would otherwise reflect real-time progress.
Risk / Business Impact	Without reliable treatment tracking, ISMS leadership and, ultimately, an independent certification body reviewing this area cannot gain assurance that identified risks are being treated within intended timeframes, undermining a core Clause 6/8 expectation and increasing the likelihood that a treatment action silently stalls.
Evidence Reference	*EV-004, EV-005 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Migrate risk treatment tracking into the GRC platform already used for the corrective action register, with automated status pulls from source systems where feasible and a mandatory quarterly reconciliation workflow.
Management Response	*Agreed. NorthBridge will migrate risk treatment tracking into the centralized GRC platform, with automated status integration for ticketing-system-linked actions, by the target date below.*
Owner / Target Date / Status	**GRC Manager** | 15 Nov 2026 | **Open**
Retest Requirement	*Retest required in a follow-up assessment: sample no fewer than 15 treatment actions across at least two consecutive quarters post-remediation.*

ISMS-H-002 — Privileged Access Recertification Evidence Incomplete	HIGH
Clause / Annex A Reference: A.8.2 Privileged Access Rights / A.5.18 Access Rights	**Illustrative Assessment Status: Requires Improvement**
Control Objective	Privileged access to production systems, cloud infrastructure, and customer-data-bearing platforms is recertified on a recurring basis by an accountable owner, with retained evidence of review and disposition.
Criteria	NorthBridge's Access Control Policy requires quarterly recertification of all privileged (administrative, database, and cloud root/IAM) accounts by the applicable system owner, with a signed, retained review artifact for each cycle.
Condition	Of 8 quarterly privileged-access recertification cycles sampled across AWS IAM, Kubernetes cluster-admin, and PostgreSQL superuser account populations occurring within the 01 Jan – 31 Aug 2026 assessment period, 3 cycles lacked a retained, signed review artifact demonstrating that the assigned reviewer completed and approved the cycle.
Cause	Privileged access reviews are coordinated manually via a shared spreadsheet and email confirmation rather than a centralized, system-enforced workflow; reviewer confirmations sent by email were not consistently archived to the central evidence repository.
Risk / Business Impact	Without consistently retained recertification evidence, NorthBridge cannot demonstrate — to itself or to a future independent auditor — that privileged access to production and customer-data-bearing systems is being recertified on the defined cadence, increasing the risk that stale or excessive privileged access persists undetected.
Evidence Reference	*EV-010 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Migrate privileged-access recertification into the existing IAM governance platform used for standard user access reviews, with system-enforced reviewer attestation, automatic escalation for overdue cycles, and evidence retained natively rather than via email.

Management Response	*Agreed. NorthBridge will extend its existing IAM governance platform to cover all privileged account populations, including Kubernetes cluster-admin and database superuser roles, with attestation workflows enforced beginning Q4 2026.*
Owner / Target Date / Status	**IAM Program Manager** | 31 Oct 2026 | Open
Retest Requirement	*Retest required in a follow-up assessment: sample no fewer than 4 subsequent review cycles post-remediation for complete, system-evidenced completion.*

ISMS-H-003 — Supplier Security Reassessment Evidence Incomplete	**HIGH**
Clause / Annex A Reference: A.5.22 Monitoring, Review and Change Management of Supplier Services / A.5.19 Information Security in Supplier Relationships	**Illustrative Assessment Status: Requires Improvement**
Control Objective	Suppliers classified as High or Medium information security risk are reassessed on a defined recurring cadence, with retained evidence of the reassessment outcome.
Criteria	NorthBridge's Supplier Security Policy requires annual reassessment of High risk-tier suppliers and reassessment every 24 months for Medium risk-tier suppliers, with a completed questionnaire, evidence review, and sign-off retained per supplier.
Condition	Of 12 High and Medium risk-tier suppliers due for reassessment within the 01 Jan – 31 Aug 2026 assessment period, 5 suppliers did not have a completed and retained reassessment record as of the assessment cut-off date.
Cause	Reassessment due dates are tracked in the supplier register but are not proactively surfaced to the Procurement/GRC teams; reassessments are initiated reactively rather than on an automated due-date trigger.
Risk / Business Impact	Delayed supplier reassessment increases the risk that a material change in a supplier's security posture — such as a new subprocessor, a control regression, or an unreported incident — goes undetected by NorthBridge for an extended period, weakening the organization's supply-chain risk management posture under Clause 6 and A.5.19–A.5.22.
Evidence Reference	*EV-019 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Implement automated reassessment-due alerting from the supplier register to Procurement and GRC, with escalation if a reassessment is not initiated within 30 days of the due date, and centralize reassessment evidence retention.
Management Response	*Agreed. NorthBridge will implement automated reassessment-due reminders in the supplier register and complete the 5 overdue reassessments identified in this sample by the target date.*
Owner / Target Date / Status	**Procurement Lead** | 15 Dec 2026 | Open
Retest Requirement	*Retest required in a follow-up assessment: sample all High risk-tier suppliers due for reassessment in the subsequent period, plus a sample of Medium risk-tier suppliers.*

ISMS-M-004 — Internal Audit Follow-Up Tracking Inconsistent	**MEDIUM**
Clause / Annex A Reference: Clause 9.2 — Internal Audit (Management System Requirement)	**Illustrative Assessment Status: Partially Effective**
Control Objective	Nonconformities and observations identified during internal ISMS audits are tracked to closure, with follow-up verification evidence retained.
Criteria	NorthBridge's Internal Audit Programme requires each audit finding to be logged in the corrective action register with an owner, target date, and closure verification evidence.
Condition	Of 10 internal audit findings raised across the 3 internal audits conducted in the assessment period, 4 findings marked 'Closed' in the audit tracker lacked retained closure-verification evidence demonstrating that the underlying condition had actually been corrected.
Cause	Audit finding closure is currently self-certified by the finding owner without a mandatory independent verification step prior to marking the tracker status as 'Closed'.
Risk / Business Impact	Without independent closure verification, previously identified nonconformities may be marked resolved while the underlying control gap persists, reducing the internal audit programme's effectiveness as an early-warning mechanism ahead of a future independent certification audit.
Evidence Reference	*EV-021, EV-022, EV-024 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Require independent verification (by the Internal Audit Lead or GRC Manager) and retained evidence before an audit finding may be marked 'Closed' in the tracker.
Management Response	*Agreed. Internal Audit will introduce a mandatory independent verification step, with retained evidence, prior to closing any audit finding.*
Owner / Target Date / Status	**Internal Audit Lead** | 31 Dec 2026 | Open
Retest Requirement	*Retest required in the subsequent internal audit cycle: sample all findings closed since remediation for evidence of independent verification.*

ISMS-M-005 — Vulnerability Remediation Exception Documentation Incomplete	MEDIUM
Clause / Annex A Reference: A.8.8 Management of Technical Vulnerabilities	**Illustrative Assessment Status: Partially Effective**
Control Objective	Technical vulnerabilities exceeding NorthBridge's internal remediation SLA are governed through a documented, approved exception process with compensating controls identified where applicable.
Criteria	NorthBridge's internal Vulnerability Management SLA (organizational policy, not an ISO-mandated deadline) targets remediation of Critical findings within 15 days and High findings within 30 days; any exception requires documented risk acceptance approved by Security leadership.
Condition	Of 6 monthly vulnerability remediation cycles sampled, 9 individual Critical/High findings exceeded the internal SLA without a retained, approved exception record.
Cause	Engineering teams can defer remediation directly in the vulnerability management platform without a mandatory workflow step that routes the deferral to Security leadership for approval and documentation.
Risk / Business Impact	Unmanaged SLA exceptions mean vulnerabilities may remain unremediated beyond the organization's own risk tolerance without documented, accountable risk acceptance, weakening the technical vulnerability management control (A.8.8).
Evidence Reference	*EV-011 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Configure the vulnerability management platform to automatically generate an exception record and require Security leadership sign-off whenever a Critical/High finding exceeds SLA without remediation.
Management Response	*Agreed. Security Operations will configure automated exception-record generation and mandatory leadership sign-off for SLA-exceeding findings.*
Owner / Target Date / Status	**Security Operations Lead** | 30 Nov 2026 | **Open**
Retest Requirement	*Retest required in a follow-up assessment: sample no fewer than 3 subsequent remediation cycles for complete exception documentation.*

ISMS-M-006 — Backup Restoration Evidence Not Consistently Retained	MEDIUM
Clause / Annex A Reference: A.8.13 Information Backup	**Illustrative Assessment Status: Partially Effective**
Control Objective	Backups of critical information and systems are tested through periodic restoration, with retained evidence confirming successful, verified recovery.
Criteria	NorthBridge's Backup Policy requires quarterly restoration testing for all databases classified as business-critical, with a retained restoration test record for each cycle.
Condition	Of 10 backup restoration test records sampled across critical databases, 3 records for a secondary reporting database could not be located.
Cause	Restoration testing for the secondary reporting database is performed by a different engineering sub-team than the primary production databases, using a separate, less mature tracking process.
Risk / Business Impact	Without consistently retained restoration evidence, NorthBridge cannot demonstrate that backups for this database are actually recoverable, which is the ultimate purpose of the backup control — increasing the risk that a real restoration attempt during an incident fails or is delayed.
Evidence Reference	*EV-017 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Consolidate restoration test scheduling and evidence retention for all business-critical databases, including the secondary reporting database, under a single centrally tracked calendar and repository.
Management Response	*Agreed. Engineering will bring the secondary reporting database's restoration testing under the central backup testing calendar and evidence repository.*
Owner / Target Date / Status	**Engineering Director, Platform** | 15 Dec 2026 | **Open**
Retest Requirement	*Retest required in a follow-up assessment: sample all subsequent restoration test cycles for the affected database.*

ISMS-M-007 — Security Awareness Completion Exceptions Not Centrally Tracked	MEDIUM
Clause / Annex A Reference: A.6.3 Information Security Awareness, Education and Training	**Illustrative Assessment Status: Partially Effective**
Control Objective	Personnel complete assigned security awareness training within defined timeframes, with overdue exceptions visible to and actioned by accountable owners.

Criteria	NorthBridge's Security Awareness Policy requires annual completion of role-based training with manager escalation for any individual more than 30 days overdue.
Condition	Of approximately 900 fictional personnel, completion tracking for a sample of 20 individuals flagged as more than 30 days overdue showed that the corresponding manager-escalation notifications were generated by the learning management system (LMS) but were not visible in the centralized GRC reporting used by the security awareness programme owner.
Cause	The LMS generates overdue notifications directly to line managers but does not feed overdue-status data into the centralized GRC dashboard used for programme-level oversight and reporting.
Risk / Business Impact	Without centralized visibility into overdue-training exceptions, the security awareness programme owner cannot confirm that manager escalations are being actioned, weakening oversight of a control that directly supports the organization's human-layer security posture.
Evidence Reference	*EV-020 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Integrate LMS overdue-completion data into the centralized GRC reporting dashboard, and lower the manager-escalation threshold to improve programme-level oversight.
Management Response	*Agreed. HR and GRC will implement an LMS-to-GRC data feed for overdue training completions, with programme-level dashboard reporting.*
Owner / Target Date / Status	**HR Manager** | 31 Jan 2027 | **Open**
Retest Requirement	*Retest required in a follow-up assessment: confirm centralized visibility of overdue-completion data across at least two subsequent monthly reporting cycles.*

ISMS-M-008 — Asset Inventory Reconciliation Requires Improvement	**MEDIUM**
Clause / Annex A Reference: A.5.9 Inventory of Information and Other Associated Assets	**Illustrative Assessment Status: Partially Effective**
Control Objective	The information asset inventory accurately reflects the current population of in-scope systems, cloud resources, and associated assets, with a defined owner for each asset.
Criteria	NorthBridge's Asset Management Policy requires monthly reconciliation of the central asset inventory against the live cloud resource inventory.
Condition	A comparison of the central asset inventory against a point-in-time AWS Resource Explorer export identified 7 of 10 sampled asset categories reconciled cleanly; 3 categories showed count variances, primarily short-lived analytics-environment compute resources provisioned through auto-scaling that were not reflected in the central inventory at the time of comparison.
Cause	Auto-scaling resource provisioning in the analytics environment does not currently trigger an automatic registration event in the central asset inventory.
Risk / Business Impact	Incomplete asset inventory data reduces the reliability of downstream processes that depend on it, including vulnerability scanning scope, access control boundary definition, and risk assessment coverage.
Evidence Reference	*EV-007 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Implement automated asset-inventory registration for auto-scaled analytics resources at provisioning time, and periodically reconcile the central inventory against live cloud resource exports.
Management Response	*Agreed. Automated registration will be implemented for the analytics environment, with periodic reconciliation performed going forward.*
Owner / Target Date / Status	**Cloud Infrastructure Lead** | 31 Dec 2026 | **Open**
Retest Requirement	*Retest required in a follow-up assessment: full reconciliation of the central inventory against a live cloud resource export.*

ISMS-M-009 — Change Management Security Review Evidence Inconsistent	**MEDIUM**
Clause / Annex A Reference: A.8.32 Change Management	**Illustrative Assessment Status: Partially Effective**
Control Objective	Changes to information-processing facilities that affect the production environment receive a documented security review prior to deployment.
Criteria	NorthBridge's Change Management Policy requires a documented security-review sign-off for all changes classified as Medium risk or higher prior to production deployment.
Condition	Of 15 change-management tickets sampled, 3 tickets lacked a documented, retained security-review sign-off prior to production deployment, although all 3 changes had been peer-reviewed and tested.
Cause	The change-management tooling does not currently enforce a mandatory security-review gate; security review is expected by policy but not blocked by the workflow tool itself.
Risk / Business Impact	Without a system-enforced gate, security review can be inconsistently applied even where general engineering review occurred, increasing the risk that a security-relevant change reaches production without dedicated security evaluation.
Evidence Reference	*EV-026 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Add a mandatory security-review gate to the change-management workflow tooling that blocks production deployment for Medium-risk-or-higher changes until the review is completed and recorded.

Management Response	*Agreed. Engineering will implement a system-enforced security-review gate within the change-management tooling for the affected deployment pathway.*
Owner / Target Date / Status	**Engineering Director, Platform** | 15 Dec 2026 | Open
Retest Requirement	*Retest required in a follow-up assessment: sample no fewer than 10 subsequent change tickets for consistent, system-enforced security-review evidence.*

ISMS-L-010 — Document Version Metadata Inconsistency	**LOW**
Clause / Annex A Reference: Clause 7.5 — Documented Information (Management System Requirement)	**Illustrative Assessment Status: Partially Effective**
Control Objective	Documented information required by the ISMS is appropriately identified, version-controlled, and retains a clear approval and revision history.
Criteria	NorthBridge's Documented Information Procedure requires each controlled ISMS document to display a current version number, approval date, and approver in a consistent metadata block.
Condition	A review of 18 sampled controlled ISMS documents found 4 documents with version metadata that did not match the version history log maintained separately in the document management platform (for example, a document header showing 'v2.1' while the platform's revision log showed the current approved version as 'v2.2').
Cause	Version metadata within each document is updated manually by the document owner and is not automatically synchronized with the document management platform's revision log.
Risk / Business Impact	Minor version metadata inconsistency creates a risk that personnel reference an outdated document version, though the underlying document management platform itself retains the correct authoritative version.
Evidence Reference	*EV-001, EV-006 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Configure the document management platform to auto-populate version metadata within each document template, removing the manual synchronization step.
Management Response	*Agreed. GRC will configure automated version-metadata population within the document management platform's templates.*
Owner / Target Date / Status	**GRC Manager** | 28 Feb 2027 | Open
Retest Requirement	*No formal retest required; recommended for review during the subsequent internal audit cycle.*

ISMS-L-011 — Physical Visitor Record Review Documentation Gap	**LOW**
Clause / Annex A Reference: A.7.2 Physical Entry	**Illustrative Assessment Status: Partially Effective**
Control Objective	Visitor access to NorthBridge facilities is logged and periodically reviewed by a responsible owner to identify anomalies.
Criteria	NorthBridge's Physical Security Procedure requires a monthly review of the visitor log by the office facilities coordinator, with a retained review sign-off.
Condition	A review of visitor log records for a sample of 6 months found that 2 months lacked a retained review sign-off, although the underlying visitor log data itself was complete and no anomalies were identified upon inspection during this fictional assessment.
Cause	The monthly visitor-log review is not currently included as a discrete, tracked item on the physical security team's recurring task checklist.
Risk / Business Impact	The absence of a retained review sign-off for 2 of 6 sampled months means NorthBridge cannot demonstrate that the intended periodic anomaly-detection review actually occurred for those periods, though the underlying risk exposure is limited given the small office population.
Evidence Reference	*EV-028 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Add the monthly visitor-log review as a discrete, tracked checklist item with retained sign-off evidence.
Management Response	*Agreed. IT/Facilities will add the visitor-log review to the monthly physical security checklist.*
Owner / Target Date / Status	**IT Director** | 31 Jan 2027 | Open
Retest Requirement	*No formal retest required; recommended for review during the subsequent internal audit cycle.*

ISMS-L-012 — Supplier Review Evidence Formatting Inconsistency	**LOW**
Clause / Annex A Reference: A.5.20 Addressing Information Security Within Supplier Agreements	**Illustrative Assessment Status: Partially Effective**
Control Objective	Information security requirements agreed with suppliers are documented in a consistent, retrievable format supporting review and audit.

Criteria	NorthBridge's Supplier Security Policy expects security requirement clauses within supplier agreements to be documented using the standard supplier evidence template.
Condition	Security requirement clauses were present in 9 of 10 sampled supplier agreements reviewed; however, the supporting evidence files for 4 of those 9 suppliers used inconsistent formats (some as marked-up contract excerpts, others as separate summary memos), complicating efficient review.
Cause	The standard supplier evidence template was introduced after several existing supplier relationships were already documented using ad hoc formats, and retrofitting was not prioritized.
Risk / Business Impact	Inconsistent evidence formatting increases the time and effort required to review supplier security documentation but does not, on its own, indicate that supplier security requirements are unmet.
Evidence Reference	*EV-019 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Retrofit existing supplier evidence files to the standard template as part of the next scheduled reassessment for each affected supplier.
Management Response	*Agreed. Procurement will retrofit affected supplier evidence files to the standard template opportunistically during scheduled reassessments.*
Owner / Target Date / Status	**Procurement Lead** | 30 Jun 2027 | **Open**
Retest Requirement	*No formal retest required; recommended for review during the subsequent internal audit cycle.*

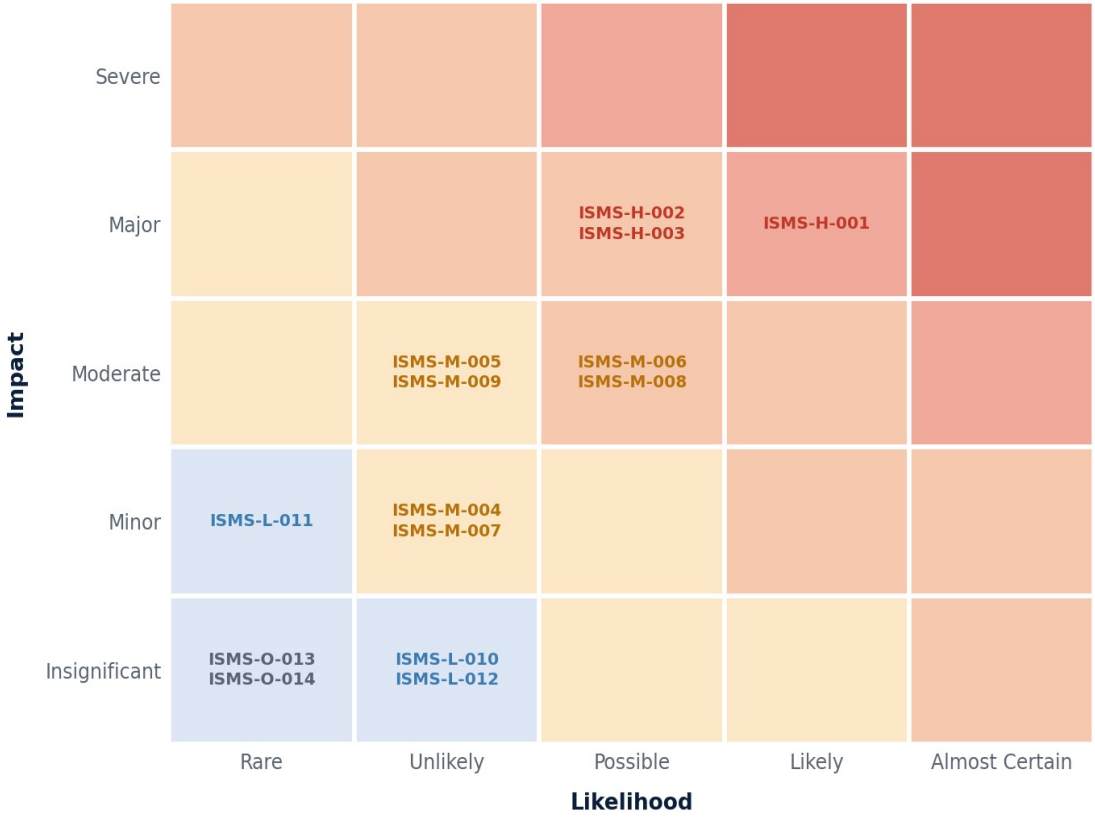
ISMS-O-013 — Opportunity to Improve ISMS Metrics Automation	**OBSERVATION**
Clause / Annex A Reference: Clause 9.1 — Monitoring, Measurement, Analysis and Evaluation (Management System Requirement)	**Illustrative Assessment Status: Effective**
Control Objective	ISMS performance metrics are collected, analyzed and reported to demonstrate the effectiveness of the management system.
Criteria	Not applicable — this is a forward-looking observation rather than a documented control exception.
Condition	Several ISMS metrics currently presented in the quarterly performance dashboard (for example, MFA coverage and vulnerability SLA compliance) are compiled through a partially manual export-and-consolidate process rather than being pulled automatically from source systems.
Cause	Metrics automation has not yet been prioritized relative to other ISMS programme investments.
Risk / Business Impact	This does not represent a control exception; it represents an opportunity to reduce manual effort and improve metric timeliness and consistency as the ISMS programme matures.
Evidence Reference	*EV-025 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Evaluate automated metrics-collection tooling that can pull ISMS performance data directly from source systems (IAM platform, vulnerability management platform, LMS) into the quarterly dashboard.
Management Response	*Agreed. GRC will evaluate automated metrics-collection tooling as part of the 2027 ISMS programme roadmap.*
Owner / Target Date / Status	**GRC Manager** | 30 Jun 2027 | **Open — Improvement Opportunity**
Retest Requirement	*No formal retest required; recommended for review during the subsequent management review cycle.*

ISMS-O-014 — Opportunity to Improve Management Dashboard Standardization	**OBSERVATION**
Clause / Annex A Reference: Clause 9.3 — Management Review (Management System Requirement)	**Illustrative Assessment Status: Effective**
Control Objective	Management review inputs are presented in a consistent format that supports efficient, informed decision-making by ISMS leadership.
Criteria	Not applicable — this is a forward-looking observation rather than a documented control exception.
Condition	Management review packages reviewed for the assessment period were complete and covered all required inputs but used varying slide/table formats across the three review cycles sampled, making period-over-period trend comparison less efficient than it could be.
Cause	No standard management review template has been formally adopted; each cycle's package is assembled independently by the GRC Manager.
Risk / Business Impact	This does not represent a control exception — all required management review inputs were present each cycle; it represents an opportunity to improve the efficiency of trend analysis across review cycles.
Evidence Reference	*EV-023 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Adopt a standardized management review template with consistent trend-visualization elements across cycles.
Management Response	*Agreed. GRC will adopt a standardized management review template beginning with the next scheduled review cycle.*
Owner / Target Date / Status	**GRC Manager** | 31 Mar 2027 | **Open — Improvement Opportunity**

Retest Requirement	*No formal retest required; recommended for review during the subsequent management review cycle.*

42 RISK HEATMAP

The 5×5 risk matrix below maps all 14 fictional findings and observations from this sample assessment by Likelihood and Impact, consistent with the rating methodology introduced in Section 12. Likelihood ranges from Rare to Almost Certain; Impact ranges from Insignificant to Severe. Cell shading reflects the highest severity finding mapped to that cell.



Illustrative 5×5 Risk Heatmap — Fictional Findings, Mapped by Likelihood × Impact

How to Read the Heatmap

- Upper-right cells (higher likelihood, higher impact) represent the fictional findings warranting the most urgent remediation attention, led by the three High-severity findings in the Possible–Likely / Major band.
- Lower-left cells represent lower-urgency items, including the two forward-looking observations, which are documentation-currency notes rather than direct control exceptions.
- The heatmap is a visualization aid; the authoritative severity rating for each finding is presented in Section 41 (Detailed Findings) and Section 54 (Finding Register).

43 ROOT CAUSE ANALYSIS

For every High-severity finding, and for a selected Medium-severity finding representative of a systemic pattern, TMG Security's fictional sample applies a 5-Whys analysis to move from the immediate condition to an underlying, addressable root cause.

ISMS-H-001 — Enterprise Risk Treatment Tracking Not Consistently Updated
Why did tracking lapse? Risk owners did not update the tracker within the 10-day window for 9 of 24 sampled actions.
Why did owners not update it? The tracker is a manually maintained spreadsheet, disconnected from the systems where the actual work happens.
Why is it disconnected? No integration was built between the GRC tracker and ticketing/IAM/vendor systems when the process was established.

Why was no integration built? The risk treatment process was designed before NorthBridge adopted its current GRC platform, and the process was never re-engineered.
Root cause: The risk treatment tracking process has not been re-engineered to take advantage of current GRC tooling and system integrations.

ISMS-H-002 — Privileged Access Recertification Evidence Incomplete
Why is recertification evidence incomplete? 3 of 8 sampled cycles lacked a retained reviewer attestation.
Why was the attestation not retained? Reviewer confirmations are sent by email rather than recorded in a system of record.
Why is email used instead of a system of record? Privileged access recertification was never migrated into the IAM governance platform used for standard user access reviews.
Why was it not migrated? Privileged account populations (cluster-admin, database superuser) were historically managed outside the primary IAM platform's scope.
Root cause: Privileged access recertification operates on a manual, email-based workflow outside the system-enforced governance platform used for standard access.

ISMS-H-003 — Supplier Security Reassessment Evidence Incomplete
Why is reassessment evidence incomplete? 5 of 12 due suppliers lacked a completed, retained reassessment record.
Why were these reassessments not completed on time? Reassessment due dates are not proactively surfaced to the teams responsible for initiating them.
Why aren't due dates surfaced proactively? The supplier register does not have automated due-date alerting configured.
Why is alerting not configured? The supplier register was implemented primarily as a system of record rather than a workflow-driving tool.
Root cause: The supplier register functions as a passive record rather than an active workflow trigger for recurring reassessment obligations.

44 CORRECTIVE ACTION PLAN

The fictional corrective action plan below consolidates the root cause, corrective action, ownership, and validation approach for each of the 14 sample findings.

Finding	Corrective Action	Owner	Priority	Target Date	Validation Method
ISMS-H-001	Migrate risk treatment tracking into the GRC platform already used for the corrective action register, with automated status pulls from source systems where feasible and a mandatory quarterly reconciliation workflow.	GRC Manager	P1	15 Nov 2026	Independent retest sample
ISMS-H-002	Migrate privileged-access recertification into the existing IAM governance platform used for standard user access reviews, with system-enforced reviewer attestation, automatic escalation for overdue cycles, and evidence retained natively rather than via email.	IAM Program Manager	P1	31 Oct 2026	Independent retest sample
ISMS-H-003	Implement automated reassessment-due alerting from the supplier register to Procurement and GRC, with escalation if a reassessment is not initiated within 30 days of the due date, and centralize reassessment evidence retention.	Procurement Lead	P1	15 Dec 2026	Independent retest sample
ISMS-M-004	Require independent verification (by the Internal Audit Lead or GRC Manager) and retained evidence before an audit finding may be marked 'Closed' in the tracker.	Internal Audit Lead	P2	31 Dec 2026	Independent retest sample
ISMS-M-005	Configure the vulnerability management platform to automatically generate an exception record and require Security leadership sign-off whenever a Critical/High finding exceeds SLA without remediation.	Security Operations Lead	P2	30 Nov 2026	Independent retest sample
ISMS-M-006	Consolidate restoration test scheduling and evidence retention for all business-critical databases, including the secondary reporting database, under a single centrally tracked calendar and repository.	Engineering Director, Platform	P2	15 Dec 2026	Independent retest sample
ISMS-M-007	Integrate LMS overdue-completion data into the centralized GRC reporting dashboard, and lower the manager-escalation threshold to improve programme-level oversight.	HR Manager	P2	31 Jan 2027	Independent retest sample
ISMS-M-008	Implement automated asset-inventory registration for auto-scaled analytics resources at provisioning time, and periodically reconcile the central inventory against live cloud resource exports.	Cloud Infrastructure Lead	P2	31 Dec 2026	Independent retest sample
ISMS-M-009	Add a mandatory security-review gate to the change-management workflow tooling that blocks production deployment for Medium-risk-or-higher changes until the review is completed and recorded.	Engineering Director, Platform	P2	15 Dec 2026	Independent retest sample
ISMS-L-010	Configure the document management platform to auto-populate version metadata within each document template, removing the manual synchronization step.	GRC Manager	P3	28 Feb 2027	Next audit cycle review
ISMS-L-011	Add the monthly visitor-log review as a discrete, tracked checklist item with retained sign-off evidence.	IT Director	P3	31 Jan 2027	Next audit cycle review
ISMS-L-012	Retrofit existing supplier evidence files to the standard template as part of the next scheduled reassessment for	Procurement Lead	P3	30 Jun 2027	Next audit cycle review

Finding	Corrective Action	Owner	Priority	Target Date	Validation Method
	each affected supplier.				
ISMS-O-013	Evaluate automated metrics-collection tooling that can pull ISMS performance data directly from source systems (IAM platform, vulnerability management platform, LMS) into the quarterly dashboard.	GRC Manager	P4	30 Jun 2027	Next audit cycle review
ISMS-O-014	Adopt a standardized management review template with consistent trend-visualization elements across cycles.	GRC Manager	P4	31 Mar 2027	Next audit cycle review

45 30-DAY REMEDIATION ROADMAP

The fictional 90-day remediation roadmap (illustrated below and detailed across Sections 45–47) sequences remediation activity, prioritizing the three High-severity findings for early closure ahead of an actual independent certification audit. All dates and timelines shown are illustrative.

Illustrative 90-Day Remediation Roadmap — Fictional Timeline

0–30 Days (Illustrative Sample Roadmap)

- Begin migration of enterprise risk treatment tracking into the centralized GRC platform, with automated status pulls where feasible (ISMS-H-001).
- Extend the IAM governance platform to cover privileged account tiers (cloud, container, database), with system-enforced attestation (ISMS-H-002).
- Complete overdue reassessments for the 5 High/Medium risk-tier suppliers identified in this sample and implement reassessment-due alerting (ISMS-H-003).

46 60-DAY REMEDIATION ROADMAP

Building on the 0–30 day priorities in Section 45, the 31–60 day window focuses on governance-process automation and evidence-consolidation activity across Medium-severity findings.

31–60 Days (Illustrative Sample Roadmap)

- Automate vulnerability exception-record generation with mandatory Security leadership sign-off for SLA-exceeding findings (ISMS-M-005).
- Consolidate backup restoration testing scheduling and evidence retention under a single centrally tracked calendar (ISMS-M-006).
- Introduce a mandatory independent verification step prior to closing internal audit findings (ISMS-M-004).
- Add a system-enforced security-review gate to the change management workflow for Medium-risk-or-higher changes (ISMS-M-009).

47 90-DAY REMEDIATION ROADMAP

The final 61–90 day window addresses the remaining Medium, Low, and Observation-level items, completing the fictional remediation cycle ahead of a final readiness review.

61–90 Days (Illustrative Sample Roadmap)

- Implement automated asset-inventory registration for auto-scaled analytics resources and complete a full inventory reconciliation (ISMS-M-008).
- Integrate LMS overdue-training data into the centralized GRC reporting dashboard (ISMS-M-007).
- Configure automated version-metadata population within the document management platform (ISMS-L-010); add the visitor-log review to the physical security checklist (ISMS-L-011); retrofit supplier evidence files to the standard template (ISMS-L-012).
- Evaluate automated ISMS metrics tooling and adopt a standardized management review template (ISMS-O-013, ISMS-O-014).
- Complete a full retest cycle across all 2026 findings ahead of engaging an accredited independent certification body for an actual ISO/IEC 27001:2022 certification audit.

ILLUSTRATIVE SAMPLE ROADMAP — all dates, phases, and sequencing shown across Sections 45–47 are fictional.

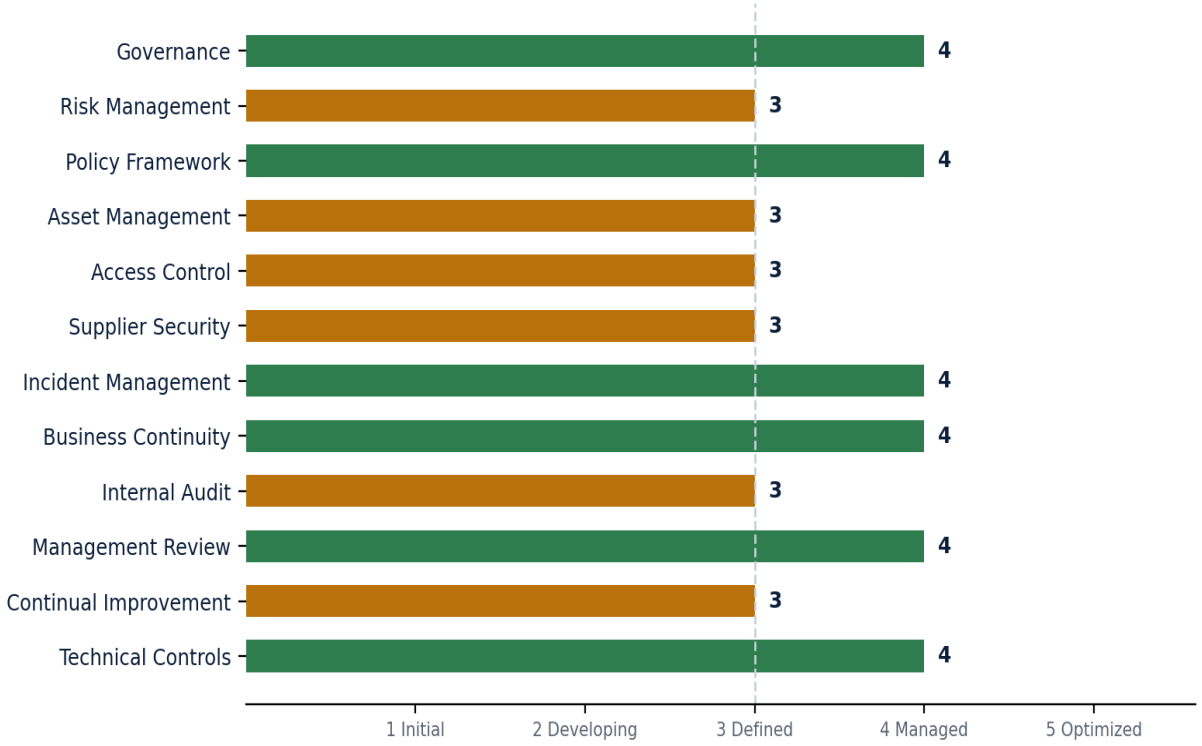
48 MANAGEMENT ACTION PLAN

NorthBridge's fictional management team has reviewed and formally accepted each sample finding below, with defined ownership and target remediation dates. This table is synchronized with Section 41 (Detailed Findings) and Section 54 (Finding Register); every finding appears exactly once.

Finding ID	Management Response	Owner	Target Date	Priority	Status
ISMS-H-001	Agreed. NorthBridge will migrate risk treatment tracking into the centralized GRC platform, with automated status integration for ticketing-system-linked actions, by the target date below.	GRC Manager	15 Nov 2026	Priority 1	Open
ISMS-H-002	Agreed. NorthBridge will extend its existing IAM governance platform to cover all privileged account populations, including Kubernetes cluster-admin and database superuser roles, with attestation workflows enforced beginning Q4 2026.	IAM Program Manager	31 Oct 2026	Priority 1	Open
ISMS-H-003	Agreed. NorthBridge will implement automated reassessment-due reminders in the supplier register and complete the 5 overdue reassessments identified in this sample by the target date.	Procurement Lead	15 Dec 2026	Priority 1	Open
ISMS-M-004	Agreed. Internal Audit will introduce a mandatory independent verification step, with retained evidence, prior to closing any audit finding.	Internal Audit Lead	31 Dec 2026	Priority 2	Open
ISMS-M-005	Agreed. Security Operations will configure automated exception-record generation and mandatory leadership sign-off for SLA-exceeding findings.	Security Operations Lead	30 Nov 2026	Priority 2	Open
ISMS-M-006	Agreed. Engineering will bring the secondary reporting database's restoration testing under the central backup testing calendar and evidence repository.	Engineering Director, Platform	15 Dec 2026	Priority 2	Open
ISMS-M-007	Agreed. HR and GRC will implement an LMS-to-GRC data feed for overdue training completions, with programme-level dashboard reporting.	HR Manager	31 Jan 2027	Priority 2	Open
ISMS-M-008	Agreed. Automated registration will be implemented for the analytics environment, with periodic reconciliation performed going forward.	Cloud Infrastructure Lead	31 Dec 2026	Priority 2	Open
ISMS-M-009	Agreed. Engineering will implement a system-enforced security-review gate within the change-management tooling for the affected deployment pathway.	Engineering Director, Platform	15 Dec 2026	Priority 2	Open
ISMS-L-010	Agreed. GRC will configure automated version-metadata population within the document management platform's templates.	GRC Manager	28 Feb 2027	Priority 3	Open
ISMS-L-011	Agreed. IT/Facilities will add the visitor-log review to the monthly physical security checklist.	IT Director	31 Jan 2027	Priority 3	Open
ISMS-L-012	Agreed. Procurement will retrofit affected supplier evidence files to the standard template opportunistically during scheduled reassessments.	Procurement Lead	30 Jun 2027	Priority 3	Open
ISMS-O-013	Agreed. GRC will evaluate automated metrics-collection tooling as part of the 2027 ISMS programme roadmap.	GRC Manager	30 Jun 2027	Priority 4	Open — Improvement Opportunity
ISMS-O-014	Agreed. GRC will adopt a standardized management review template beginning with the next scheduled review cycle.	GRC Manager	31 Mar 2027	Priority 4	Open — Improvement Opportunity

49 ISMS MATURITY ASSESSMENT

The fictional maturity model below rates 12 ISMS domains on a 5-level scale (1 Initial, 2 Developing, 3 Defined, 4 Managed, 5 Optimized). Scores are illustrative and reflect the fictional findings identified throughout this sample.



Illustrative ISMS Maturity Model — Fictional Scores by Domain

Domain	Level	Note
Governance	4 — Managed	Governance structure, roles, and executive engagement are well established and consistently operating.
Risk Management	3 — Defined	Methodology is defined and applied consistently; treatment tracking discipline needs improvement (ISMS-H-001).
Policy Framework	4 — Managed	Comprehensive policy set in place, reviewed on a defined cycle.
Asset Management	3 — Defined	Inventory process defined; reconciliation automation still developing (ISMS-M-008).
Access Control	3 — Defined	Strong standard-access discipline; privileged access evidence maturity lags (ISMS-H-002).
Supplier Security	3 — Defined	Onboarding due diligence is mature; reassessment cadence enforcement is developing (ISMS-H-003).
Incident Management	4 — Managed	Documented, exercised programme with defined escalation and lessons-learned process.
Business Continuity	4 — Managed	BIA, recovery objectives and testing programme are well established.
Internal Audit	3 — Defined	Programme is well designed; independent closure verification is developing (ISMS-M-004).
Management Review	4 — Managed	Consistent cadence and complete inputs; template standardization is an improvement opportunity (ISMS-O-014).
Continual Improvement	3 — Defined	Corrective action process is operating; automation of metrics is an improvement opportunity (ISMS-O-013).
Technical Controls	4 — Managed	Strong technical control baseline across identity, monitoring, and cloud security domains.

50 AUDIT / READINESS CONCLUSION

ILLUSTRATIVE READINESS CONCLUSION

PARTIALLY READY FOR FORMAL CERTIFICATION AUDIT

This conclusion is illustrative only. It is not an ISO certification decision. A formal certification decision must be made by an appropriately accredited independent certification body.

Executive Conclusion

This fictional assessment demonstrates that NorthBridge has established an ISMS foundation with major governance processes in place: leadership commitment is visible, risk management is operational, the Statement of Applicability is comprehensive, and a substantial majority of Annex A:2022 controls — 79 of 90 applicable controls — were assessed as Effective in this sample. Certain gaps require remediation and evidence consistency should improve: privileged access

recertification evidence, supplier reassessment cadence enforcement, and enterprise risk treatment tracking discipline chief among them.

None of the fictional findings in this report indicate an absent control program; rather, they reflect documentation, consistency, and evidence-retention gaps within an otherwise well-designed ISMS — the pattern TMG Security would expect to identify and help remediate during a readiness engagement conducted ahead of an organization's first, or a subsequent, independent ISO/IEC 27001:2022 certification audit. Corrective actions identified in this sample, particularly the three High-severity items, should be completed and validated before NorthBridge engages an accredited certification body for an actual certification audit.

Strengths (Fictional)

- Visible executive leadership commitment and a well-structured governance and reporting model.
- Comprehensive, current information security policy framework reviewed on a defined annual cycle.
- Mature technical control baseline: enforced MFA/SSO, centralized SIEM/EDR, strong cryptography and key management practices.
- Documented, exercised incident management and business continuity/disaster recovery programmes.
- A comprehensive, well-justified Statement of Applicability covering all 93 Annex A:2022 controls.

Improvement Areas (Fictional)

- Enterprise risk treatment tracking evidence and cross-system status reconciliation.
- Privileged access recertification evidence retention across cloud, container, and database administrative tiers.
- Supplier security reassessment cadence enforcement for High/Medium risk-tier suppliers.
- Internal audit finding closure — independent verification prior to marking findings resolved.
- Vulnerability remediation exception governance, backup restoration evidence, and change-management security-review consistency.

This conclusion, and every figure, finding, and status referenced above, is entirely fictional and constructed for demonstration purposes only. It does not describe the security, availability, or ISMS posture of any real organization, and does not constitute an ISO/IEC 27001 certificate, certification decision, or independent certification audit report.

51 EVIDENCE REGISTER

The register below lists all 30 illustrative evidence references cited throughout this fictional sample. No actual client evidence was collected or reviewed; every entry is a fictional evidence reference constructed for demonstration purposes.

ID	Description	Type	Owner
EV-001	Information Security Policy	Policy Document	GRC Manager
EV-002	ISMS Scope Statement	Governance Document	CISO
EV-003	Risk Assessment Methodology	Methodology Document	GRC Manager
EV-004	Enterprise Risk Register	Register / Tracker	GRC Manager
EV-005	Risk Treatment Plan	Planning Document	GRC Manager
EV-006	Statement of Applicability	Governance Document	CISO
EV-007	Asset Inventory	Register / Export	Cloud Infrastructure Lead
EV-008	Access Review Records	Review Artifact	IAM Program Manager
EV-009	MFA Configuration	Technical Configuration	Security Operations Lead
EV-010	Privileged Access Review	Review Artifact	IAM Program Manager
EV-011	Vulnerability Scan Reports	Technical Report	Security Operations Lead
EV-012	Penetration Test Reports	Technical Report	Security Operations Lead
EV-013	SIEM Configuration	Technical Configuration	Security Operations Lead
EV-014	EDR Configuration	Technical Configuration	Security Operations Lead
EV-015	Incident Response Plan	Plan Document	Security Operations Lead
EV-016	Incident Exercise Records	Exercise Record	Security Operations Lead
EV-017	Backup Test Records	Test Record	Engineering Director, Platform
EV-018	Disaster Recovery Plan	Plan Document	Business Continuity Lead
EV-019	Supplier Security Assessments	Assessment Record	Procurement Lead
EV-020	Security Awareness Records	Training Record	HR Manager
EV-021	Internal Audit Programme	Programme Document	Internal Audit Lead
EV-022	Internal Audit Reports	Audit Report	Internal Audit Lead
EV-023	Management Review Minutes	Meeting Minutes	CISO
EV-024	Corrective Action Register	Register / Tracker	GRC Manager
EV-025	Security Metrics Dashboard	Dashboard Export	GRC Manager
EV-026	Change Management Records	Ticketing Record	Engineering Director, Platform
EV-027	Secure Development Records	SDLC Record	Engineering Director, Platform
EV-028	Physical Security Procedures	Procedure Document	IT Director
EV-029	Cryptographic Key Management Records	Technical Record	Security Operations Lead
EV-030	Business Continuity Test Results	Test Record	Business Continuity Lead

ILLUSTRATIVE EVIDENCE REFERENCE — NO ACTUAL CLIENT EVIDENCE

52 INTERVIEW REGISTER

The fictional interviews below simulate the discussions TMG Security would conduct with role holders during an actual ISMS readiness engagement. No real interviews occurred.

INT-01 — Chief Information Security Officer (Security / GRC)	
Objective	Understand ISMS governance, leadership commitment, and scope rationale.
Topics	Policy approval process, resourcing, governance forum cadence, scope boundary rationale.
Evidence Correlated	EV-001, EV-002, EV-006
Illustrative Outcome	*Corroborated governance structure and leadership commitment described in documentation.*

INT-02 — GRC Manager (Security / GRC)	
Objective	Understand risk management methodology and treatment tracking practices.
Topics	Risk identification process, treatment tracker maintenance, SoA update cadence.
Evidence Correlated	EV-003, EV-004, EV-005
Illustrative Outcome	*Confirmed methodology; corroborated tracker maintenance gap consistent with ISMS-H-001.*

INT-03 — IAM Program Manager (Security Operations)	
Objective	Understand access provisioning, recertification, and privileged access governance.
Topics	Joiner/mover/leaver workflow, standard vs. privileged access review cadence, evidence retention.
Evidence Correlated	EV-008, EV-010
Illustrative Outcome	*Confirmed standard access review discipline; corroborated privileged recertification evidence gap (ISMS-H-002).*

INT-04 — Security Operations Lead (Security Operations)	
Objective	Understand vulnerability management, monitoring, and incident response operations.
Topics	Scanning cadence, SLA governance, SIEM/EDR coverage, incident escalation.
Evidence Correlated	EV-011, EV-013, EV-014, EV-015
Illustrative Outcome	*Confirmed monitoring coverage; corroborated vulnerability exception documentation gap (ISMS-M-005).*

INT-05 — Engineering Director, Platform (Engineering)	
Objective	Understand change management, secure development, and backup practices.
Topics	Change ticket workflow, security review gate, CI/CD controls, backup/restoration testing.
Evidence Correlated	EV-017, EV-026, EV-027
Illustrative Outcome	*Confirmed general SDLC discipline; corroborated change security-review and backup evidence gaps (ISMS-M-009, ISMS-M-006).*

INT-06 — Procurement Lead (Procurement / Vendor Management)	
Objective	Understand supplier onboarding, risk classification, and reassessment practices.
Topics	Supplier risk tiering, due diligence process, reassessment scheduling, contractual requirements.
Evidence Correlated	EV-019
Illustrative Outcome	*Confirmed onboarding rigor; corroborated reassessment scheduling and evidence gaps (ISMS-H-003, ISMS-L-012).*

INT-07 — HR Manager (Human Resources)	
Objective	Understand onboarding, screening, and security awareness training operations.
Topics	Background screening, training assignment, completion tracking, escalation procedures.
Evidence Correlated	EV-020
Illustrative Outcome	*Confirmed training programme design; corroborated centralized visibility gap for overdue completions (ISMS-M-007).*

INT-08 — IT Director (IT / Facilities)	
Objective	Understand physical security procedures and asset lifecycle management.
Topics	Facility access control, visitor management, equipment disposal, endpoint management.
Evidence Correlated	EV-028
Illustrative Outcome	*Confirmed physical control design; corroborated visitor-log review sign-off gap (ISMS-L-011).*

INT-09 — Internal Audit Lead (Internal Audit)	
Objective	Understand the internal audit programme, sampling approach, and follow-up tracking.
Topics	Audit planning, auditor independence, finding classification, follow-up verification.
Evidence Correlated	EV-021, EV-022, EV-024
Illustrative Outcome	*Confirmed programme design; corroborated follow-up verification gap (ISMS-M-004).*

INT-10 — Business Continuity Lead (Engineering / Operations)	
Objective	Understand business continuity planning, disaster recovery, and testing practices.
Topics	Business impact analysis, recovery objectives, DR test scenarios, lessons-learned process.
Evidence Correlated	EV-018, EV-030
Illustrative Outcome	*Confirmed BC/DR programme maturity; no exceptions identified in this sample beyond documentation-consistency items.*

53 CONTROL TESTING REGISTER

The fictional control testing register below documents illustrative ISMS control testing procedures, samples, and results applied across 14 representative Annex A and management-system controls in this sample assessment.

TST-01 — A.8.2	Exception: Yes — 3 of 8
Test Objective	Verify quarterly privileged-access recertification is completed and evidenced.
Population	24 quarterly recertification cycles across AWS IAM, Kubernetes cluster-admin, and PostgreSQL superuser populations (Jan–Aug 2026)

Sample Size	8 cycles
Evidence	Recertification tracker, exported account listing, reviewer attestation
Procedure	Inspect the review tracker and request the underlying review workpaper for each sampled cycle; corroborate reviewer identity against the IAM group population.
Result	5 of 8 cycles evidenced complete; 3 of 8 lacked a retained attestation.
Finding Reference	ISMS-H-002

TST-02 — A.5.22	**Exception: Yes — 5 of 12**
Test Objective	Verify High/Medium risk-tier suppliers are reassessed on the defined cadence.
Population	12 High/Medium risk-tier suppliers due for reassessment (Jan–Aug 2026)
Sample Size	12 suppliers (full population)
Evidence	Supplier register, reassessment questionnaires, sign-off records
Procedure	Compare the supplier register's due-date field against the retained reassessment evidence for each supplier.
Result	7 of 12 suppliers evidenced a completed reassessment; 5 of 12 did not.
Finding Reference	ISMS-H-003

TST-03 — Clause 6.1.3 / 8.3	**Exception: Yes — 9 of 24**
Test Objective	Verify risk treatment actions are tracked to completion with current status.
Population	24 open risk treatment actions (Jan–Aug 2026)
Sample Size	24 actions (full population)
Evidence	Risk treatment tracker, corroborating system records
Procedure	Compare tracker status to corroborating evidence in ticketing, IAM, and vendor systems for each action.
Result	15 of 24 actions had current, accurate tracker status; 9 of 24 were stale by more than one quarter.
Finding Reference	ISMS-H-001

TST-04 — Clause 9.2	**Exception: Yes — 4 of 10**
Test Objective	Verify internal audit findings are independently verified prior to closure.
Population	10 internal audit findings closed in the assessment period
Sample Size	10 findings (full population)
Evidence	Audit tracker, closure verification workpapers
Procedure	Inspect each 'Closed' finding for retained independent verification evidence.
Result	6 of 10 findings had retained verification evidence; 4 of 10 relied on owner self-certification only.
Finding Reference	ISMS-M-004

TST-05 — A.8.8	**Exception: Yes — 9 findings**
Test Objective	Verify vulnerability remediation SLA exceptions are documented and approved.
Population	6 monthly vulnerability remediation cycles (Mar–Aug 2026)
Sample Size	6 cycles (full population)
Evidence	Vulnerability scan reports, exception register
Procedure	Identify Critical/High findings exceeding the internal SLA and inspect for a retained, approved exception record.
Result	Of the SLA-exceeding population, 9 individual findings lacked a retained exception record.
Finding Reference	ISMS-M-005

TST-06 — A.8.13	**Exception: Yes — 3 of 10**
Test Objective	Verify backup restoration testing is performed and evidenced for business-critical databases.
Population	40 quarterly restoration test cycles across 10 business-critical databases (Jan–Aug 2026)
Sample Size	10 records
Evidence	Backup restoration test records
Procedure	Request the restoration test record for each sampled database/cycle combination and inspect for a documented, successful result.
Result	7 of 10 records located and evidenced success; 3 of 10 (secondary reporting database) could not be located.
Finding Reference	ISMS-M-006

TST-07 — A.6.3	**Exception: Yes — 20 of 20 (systemic integration gap)**
Test Objective	Verify overdue security awareness training completions are tracked and escalated.
Population	Personnel flagged more than 30 days overdue on assigned training (Jan–Aug 2026)
Sample Size	20 personnel records
Evidence	LMS completion export, GRC dashboard export
Procedure	Compare LMS overdue-escalation records to centralized GRC dashboard visibility for each sampled individual.
Result	LMS escalations generated for all 20 sampled records; GRC dashboard visibility confirmed for 0 of 20 at the time of testing.
Finding Reference	ISMS-M-007

TST-08 — A.5.9	**Exception: Yes — 3 of 10**
Test Objective	Verify the asset inventory reconciles to the live cloud resource inventory.

Population	10 asset categories within the central inventory
Sample Size	10 categories (full population)
Evidence	Asset inventory export, AWS Resource Explorer export
Procedure	Compare category counts between the central asset inventory and a point-in-time cloud resource export.
Result	7 of 10 categories reconciled cleanly; 3 of 10 (auto-scaled analytics resources) showed count variances.
Finding Reference	ISMS-M-008

TST-09 — A.8.32	**Exception: Yes — 3 of 15**
Test Objective	Verify production changes receive a documented security review prior to deployment.
Population	Change tickets classified Medium risk or higher (Jan–Aug 2026)
Sample Size	15 tickets
Evidence	Change management tickets, security review sign-off records
Procedure	Inspect each sampled ticket for a documented, retained security-review sign-off prior to production deployment.
Result	12 of 15 tickets evidenced a retained sign-off; 3 of 15 did not (though all were peer-reviewed and tested).
Finding Reference	ISMS-M-009

TST-10 — Clause 7.5	**Exception: Yes — 4 of 18**
Test Objective	Verify controlled ISMS documents display version metadata consistent with the platform revision log.
Population	Controlled ISMS documents within the document management platform
Sample Size	18 documents
Evidence	Document headers, platform revision history log
Procedure	Compare each sampled document's header version metadata to the platform's authoritative revision log entry.
Result	14 of 18 documents matched; 4 of 18 showed a metadata/log mismatch.
Finding Reference	ISMS-L-010

TST-11 — A.7.2	**Exception: Yes — 2 of 6**
Test Objective	Verify the monthly visitor log review is performed and evidenced.
Population	8 monthly review periods (Jan–Aug 2026)
Sample Size	6 months
Evidence	Visitor log, review sign-off records
Procedure	Inspect each sampled month for a retained review sign-off by the facilities coordinator.
Result	4 of 6 months evidenced a retained sign-off; 2 of 6 did not.
Finding Reference	ISMS-L-011

TST-12 — A.5.20	**Exception: Yes — 4 of 9 formatting inconsistency**
Test Objective	Verify supplier agreements document agreed security requirements using the standard template.
Population	Active supplier agreements with security requirement clauses
Sample Size	10 suppliers
Evidence	Supplier agreements, supplier evidence files
Procedure	Inspect each sampled supplier's evidence file for use of the standard evidence template.
Result	Security clauses present for 9 of 10; template format used consistently for 5 of those 9.
Finding Reference	ISMS-L-012

TST-13 — A.8.5 / A.5.16	**Exception: No**
Test Objective	Verify MFA is enforced for standard user access to in-scope systems.
Population	All active workforce identities in the enterprise identity provider
Sample Size	30 identities
Evidence	IdP configuration export, MFA enrollment report
Procedure	Inspect the IdP configuration and a sample of active identities for enforced MFA enrollment.
Result	30 of 30 sampled identities showed enforced MFA enrollment with no exceptions.
Finding Reference	No finding raised — no exception identified

TST-14 — A.8.16	**Exception: No**
Test Objective	Verify security monitoring alerts are triaged within the defined escalation window.
Population	SIEM-generated alerts classified High or Critical (a representative month)
Sample Size	25 alerts
Evidence	SIEM alert log, triage/escalation records
Procedure	Inspect timestamps between alert generation and initial analyst triage for each sampled alert.
Result	25 of 25 sampled alerts were triaged within the defined escalation window.
Finding Reference	No finding raised — no exception identified

54 FINDING REGISTER

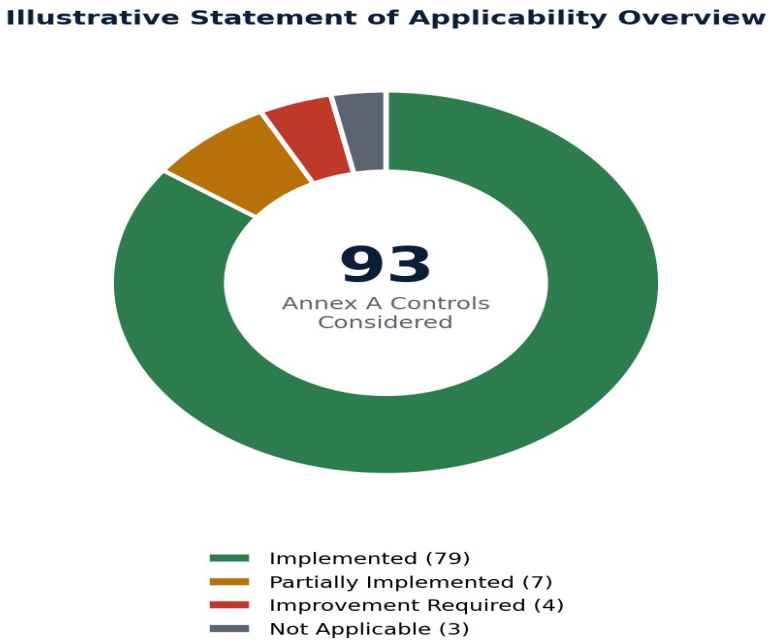
The consolidated finding register below lists all 14 fictional findings and observations with their clause/Annex A reference, severity, owner, target date, and status — synchronized with Sections 40, 41, and 48.

ID	Title	Reference	Severity	Owner	Status
ISMS-H-001	Enterprise Risk Treatment Tracking Not Consistently Updated	Clause 6.1.3	HIGH	GRC Manager	Open
ISMS-H-002	Privileged Access Recertification Evidence Incomplete	A.8.2 Privileged Access Rights	HIGH	IAM Program Manager	Open
ISMS-H-003	Supplier Security Reassessment Evidence Incomplete	A.5.22 Monitoring, Review and Change Management of Supplier Services	HIGH	Procurement Lead	Open
ISMS-M-004	Internal Audit Follow-Up Tracking Inconsistent	Clause 9.2	MEDIUM	Internal Audit Lead	Open
ISMS-M-005	Vulnerability Remediation Exception Documentation Incomplete	A.8.8 Management of Technical Vulnerabilities	MEDIUM	Security Operations Lead	Open
ISMS-M-006	Backup Restoration Evidence Not Consistently Retained	A.8.13 Information Backup	MEDIUM	Engineering Director, Platform	Open
ISMS-M-007	Security Awareness Completion Exceptions Not Centrally Tracked	A.6.3 Information Security Awareness, Education and Training	MEDIUM	HR Manager	Open
ISMS-M-008	Asset Inventory Reconciliation Requires Improvement	A.5.9 Inventory of Information and Other Associated Assets	MEDIUM	Cloud Infrastructure Lead	Open
ISMS-M-009	Change Management Security Review Evidence Inconsistent	A.8.32 Change Management	MEDIUM	Engineering Director, Platform	Open
ISMS-L-010	Document Version Metadata Inconsistency	Clause 7.5	LOW	GRC Manager	Open
ISMS-L-011	Physical Visitor Record Review Documentation Gap	A.7.2 Physical Entry	LOW	IT Director	Open
ISMS-L-012	Supplier Review Evidence Formatting Inconsistency	A.5.20 Addressing Information Security Within Supplier Agreements	LOW	Procurement Lead	Open
ISMS-O-013	Opportunity to Improve ISMS Metrics Automation	Clause 9.1	OBSERVATION	GRC Manager	Open — Improvement Opportunity
ISMS-O-014	Opportunity to Improve Management Dashboard Standardization	Clause 9.3	OBSERVATION	GRC Manager	Open — Improvement Opportunity

55 STATEMENT OF APPLICABILITY SUMMARY

The table below summarizes the fictional Statement of Applicability presented in full in Section 15, covering all 93 Annex A:2022 controls considered for NorthBridge's illustrative environment.

Total Controls Considered	**93**
Applicable	**90**
Not Applicable	**3**
Implemented (Effective)	**79**
Partially Implemented (Partially Effective)	**7**
Improvement Required	**4**



Illustrative Statement of Applicability Overview — Fictional Sample

56 ANNEX A CONTROL MATRIX

The matrix below maps all 93 illustrative Annex A:2022 controls tested in this sample assessment to their theme, illustrative operating-effectiveness status, related finding, and recommended action.

Ref.	Theme	Control Description (TMG Summary)	Status	Finding	Recommended Action
A.5.1	5 Organizational	Establishing and maintaining a top-level information security policy set, approved by management	Effective	—	Maintain current control operation.
A.5.2	5 Organizational	Defining and allocating information security roles and responsibilities across the organization	Effective	—	Maintain current control operation.
A.5.3	5 Organizational	Segregating conflicting duties and areas of responsibility to reduce misuse opportunity	Effective	—	Maintain current control operation.
A.5.4	5 Organizational	Management reinforcing security expectations through visible ongoing direction and support	Effective	—	Maintain current control operation.
A.5.5	5 Organizational	Maintaining appropriate contact with relevant authorities (law enforcement, regulators)	Effective	—	Maintain current control operation.
A.5.6	5 Organizational	Maintaining contact with security interest groups, forums and professional associations	Effective	—	Maintain current control operation.
A.5.7	5 Organizational	Collecting and analyzing threat intelligence relevant to the organization's environment	Effective	—	Maintain current control operation.
A.5.8	5 Organizational	Embedding information security considerations into project management practices	Effective	—	Maintain current control operation.
A.5.9	5 Organizational	Maintaining an inventory of information and other associated assets, with owners	Partially Effective	ISMS-M-008	Automate weekly inventory reconciliation between the asset register and cloud resource exports.
A.5.10	5 Organizational	Defining acceptable use rules for information and associated assets	Effective	—	Maintain current control operation.
A.5.11	5 Organizational	Ensuring personnel and third parties return organizational assets upon change or termination	Effective	—	Maintain current control operation.
A.5.12	5 Organizational	Classifying information according to confidentiality, integrity and availability needs	Effective	—	Maintain current control operation.
A.5.13	5 Organizational	Labelling information consistently with its classification scheme	Effective	—	Maintain current control operation.
A.5.14	5 Organizational	Protecting information during transfer, internally and with external parties	Effective	—	Maintain current control operation.
A.5.15	5 Organizational	Establishing rules to control logical and physical access based on business need	Effective	—	Maintain current control operation.
A.5.16	5 Organizational	Managing the full lifecycle of identities used to access organizational systems	Effective	—	Maintain current control operation.
A.5.17	5 Organizational	Controlling allocation and management of authentication information	Effective	—	Maintain current control operation.
A.5.18	5 Organizational	Provisioning, reviewing, modifying and revoking access rights per business need	Effective	—	Maintain current control operation.
A.5.19	5 Organizational	Managing information security risk associated with the use of supplier products and services	Effective	—	Maintain current supplier risk classification cadence.
A.5.20	5 Organizational	Agreeing relevant security requirements with each supplier based on risk	Partially Effective	ISMS-L-012	Standardize the supplier evidence template used to document agreed security requirements.
A.5.21	5 Organizational	Managing information security risk within the ICT supply chain	Effective	—	Maintain current control operation.
A.5.22	5 Organizational	Monitoring, reviewing and managing change in supplier service delivery	Requires Improvement	ISMS-H-003	Implement automated reassessment-due alerting and centralize supplier evidence retention.
A.5.23	5 Organizational	Managing information security for the acquisition and use of cloud services	Effective	—	Maintain current control operation.
A.5.24	5 Organizational	Planning and preparing for the management of information security incidents	Effective	—	Maintain current control operation.
A.5.25	5 Organizational	Assessing and deciding the classification of information security events	Effective	—	Maintain current control operation.
A.5.26	5 Organizational	Responding to information security incidents per documented procedures	Effective	—	Maintain current control operation.
A.5.27	5 Organizational	Using knowledge gained from incidents to strengthen controls	Effective	—	Maintain current control operation.
A.5.28	5 Organizational	Establishing procedures for the identification, collection and preservation of evidence	Effective	—	Maintain current control operation.
A.5.29	5 Organizational	Maintaining an appropriate level of information security during disruption	Effective	—	Maintain current control operation.
A.5.30	5 Organizational	Planning ICT readiness to support business continuity objectives	Effective	—	Maintain current control operation.
A.5.31	5 Organizational	Identifying and meeting legal, statutory, regulatory and contractual security requirements	Effective	—	Maintain current control operation.
A.5.32	5 Organizational	Protecting intellectual property rights relevant to the organization	Effective	—	Maintain current control operation.
A.5.33	5 Organizational	Protecting records from loss, destruction, falsification and unauthorized access	Effective	—	Maintain current control operation.
A.5.34	5 Organizational	Identifying and meeting privacy and personal-information-protection requirements	Requires Improvement	—	Refresh personal-information processing documentation as part of the standard change-management workflow.
A.5.35	5 Organizational	Conducting independent review of the information security approach	Effective	—	Maintain current control operation.
A.5.36	5 Organizational	Verifying compliance with information security policies, rules and standards	Effective	—	Maintain current control operation.
A.5.37	5 Organizational	Documenting and maintaining operating procedures for information-processing facilities	Effective	—	Maintain current control operation.
A.6.1	6 People	Performing background verification checks on candidates prior to employment	Effective	—	Maintain current control operation.
A.6.2	6 People	Stating personnel and contractor security responsibilities in terms of employment	Effective	—	Maintain current control operation.
A.6.3	6 People	Providing personnel with appropriate security awareness, education and training	Partially Effective	ISMS-M-007	Route overdue-training exceptions from the LMS into the centralized GRC tracking platform automatically.
A.6.4	6 People	Maintaining a formal, communicated process for addressing policy violations	Effective	—	Maintain current control operation.
A.6.5	6 People	Defining security responsibilities and duties that remain valid after termination or change	Effective	—	Maintain current control operation.
A.6.6	6 People	Identifying and applying confidentiality or non-disclosure agreements	Effective	—	Maintain current control operation.
A.6.7	6 People	Applying security measures when personnel work remotely	Effective	—	Maintain current control operation.
A.6.8	6 People	Providing a mechanism for personnel to report observed or suspected security events	Effective	—	Maintain current control operation.
A.7.1	7 Physical	Defining and using security perimeters to protect areas containing information assets	Effective	—	Maintain current control operation.
A.7.2	7 Physical	Controlling physical entry to secure areas through appropriate entry controls	Partially Effective	ISMS-L-011	Add visitor-log review sign-off to the monthly physical security checklist with retained evidence.
A.7.3	7 Physical	Designing and applying physical security for offices, rooms and facilities	Effective	—	Maintain current control operation.
A.7.4	7 Physical	Monitoring premises continuously for unauthorized physical access	Effective	—	Maintain current control operation.

Ref.	Theme	Control Description (TMG Summary)	Status	Finding	Recommended Action
A.7.5	7 Physical	Designing and implementing protection against physical and environmental threats	Effective	—	Maintain current control operation.
A.7.6	7 Physical	Designing and applying security measures for working in secure areas	Effective	—	Maintain current control operation.
A.7.7	7 Physical	Defining clear desk and clear screen rules for information and associated assets	Effective	—	Maintain current control operation.
A.7.8	7 Physical	Siting and protecting equipment appropriately	Effective	—	Maintain current control operation.
A.7.9	7 Physical	Protecting off-site assets, taking into account differing off-premises risks	Effective	—	Maintain current control operation.
A.7.10	7 Physical	Managing storage media through its lifecycle in line with the classification scheme	Effective	—	Maintain current control operation.
A.7.11	7 Physical	Protecting information-processing facilities from utility service failures	Not Applicable	—	—
A.7.12	7 Physical	Protecting cabling carrying power or data from interception, interference or damage	Not Applicable	—	—
A.7.13	7 Physical	Maintaining equipment correctly to ensure availability, integrity and confidentiality	Effective	—	Maintain current control operation.
A.7.14	7 Physical	Verifying that storage media are securely disposed of or re-used	Effective	—	Maintain current control operation.
A.8.1	8 Technological	Protecting information stored on, processed by or accessible via user endpoint devices	Effective	—	Maintain current control operation.
A.8.2	8 Technological	Restricting and managing the allocation and use of privileged access rights	Requires Improvement	ISMS-H-002	Migrate privileged-access recertification to a centralized IAM governance platform with system-enforced evidence retention.
A.8.3	8 Technological	Restricting access to information and associated assets per the access control policy	Effective	—	Maintain current control operation.
A.8.4	8 Technological	Appropriately managing read and write access to source code, tools and libraries	Effective	—	Maintain current control operation.
A.8.5	8 Technological	Implementing secure authentication technologies and procedures	Effective	—	Maintain current control operation.
A.8.6	8 Technological	Monitoring and adjusting resource use in line with current and expected capacity needs	Effective	—	Maintain current control operation.
A.8.7	8 Technological	Implementing protection against malware, supported by user awareness	Effective	—	Maintain current control operation.
A.8.8	8 Technological	Obtaining information about technical vulnerabilities and evaluating exposure	Partially Effective	ISMS-M-005	Automate exception-register creation upon SLA breach, with mandatory Security leadership sign-off.
A.8.9	8 Technological	Managing configurations, including security configurations, for hardware and software	Requires Improvement	—	Incorporate baseline documentation updates as a mandatory step within the change-management workflow.
A.8.10	8 Technological	Deleting information held in systems, devices or storage media when no longer required	Effective	—	Maintain current control operation.
A.8.11	8 Technological	Using data masking in line with the access control policy and business requirements	Effective	—	Maintain current control operation.
A.8.12	8 Technological	Applying measures to detect and prevent unauthorized disclosure of information	Effective	—	Maintain current control operation.
A.8.13	8 Technological	Maintaining and regularly testing backup copies of information, software and systems	Partially Effective	ISMS-M-006	Consolidate backup restoration test scheduling and evidence retention under a single centrally tracked calendar.
A.8.14	8 Technological	Implementing redundancy sufficient to meet availability requirements	Effective	—	Maintain current control operation.
A.8.15	8 Technological	Producing, storing, protecting and analyzing logs of relevant activity	Effective	—	Maintain current control operation.
A.8.16	8 Technological	Monitoring networks, systems and applications for anomalous behaviour	Effective	—	Maintain current control operation.
A.8.17	8 Technological	Synchronizing clocks of information-processing systems to approved time sources	Effective	—	Maintain current control operation.
A.8.18	8 Technological	Restricting and tightly controlling the use of privileged utility programs	Effective	—	Maintain current control operation.
A.8.19	8 Technological	Controlling the installation of software on operational systems	Effective	—	Maintain current control operation.
A.8.20	8 Technological	Managing and controlling networks and network devices to protect information	Effective	—	Maintain current control operation.
A.8.21	8 Technological	Identifying, implementing and monitoring security mechanisms for network services	Effective	—	Maintain current control operation.
A.8.22	8 Technological	Segregating groups of information services, users and systems on networks	Effective	—	Maintain current control operation.
A.8.23	8 Technological	Managing access to external websites to reduce exposure to malicious content	Effective	—	Maintain current control operation.
A.8.24	8 Technological	Defining and implementing rules for the effective use of cryptography	Effective	—	Maintain current control operation.
A.8.25	8 Technological	Applying rules for the secure development of software and systems	Effective	—	Maintain current control operation.
A.8.26	8 Technological	Identifying and specifying information security requirements for applications	Effective	—	Maintain current control operation.
A.8.27	8 Technological	Establishing and applying secure system engineering principles	Effective	—	Maintain current control operation.
A.8.28	8 Technological	Applying secure coding principles to software development	Effective	—	Maintain current control operation.
A.8.29	8 Technological	Defining and implementing security testing processes in the development lifecycle	Effective	—	Maintain current control operation.
A.8.30	8 Technological	Directing, monitoring and reviewing outsourced system development activity	Not Applicable	—	—
A.8.31	8 Technological	Separating development, test and production environments	Effective	—	Maintain current control operation.
A.8.32	8 Technological	Subjecting changes to information-processing facilities to formal change control	Partially Effective	ISMS-M-009	Add a mandatory security-review gate to the change-management workflow tooling, blocking deployment until completed.
A.8.33	8 Technological	Selecting, protecting and managing test information appropriately	Effective	—	Maintain current control operation.
A.8.34	8 Technological	Planning and agreeing audit and assurance testing to minimize disruption to production	Effective	—	Maintain current control operation.

57 REGULATORY / STANDARDS WATCH — 2026

This section provides a short, professional look at 2026 considerations relevant to organizations maintaining or pursuing an ISO/IEC 27001 ISMS. It does not introduce new mandatory ISO/IEC 27001 requirements; organizations should continue to monitor evolving assurance, cybersecurity, privacy, cloud, and AI-related expectations that may inform future context analysis and risk assessment inputs, independent of this sample.

ISO/IEC 27001:2022/Amendment 1:2024 — Climate Action Considerations

ISO/IEC 27001:2022/Amendment 1:2024 introduced targeted climate-action considerations into the standard's context and planning clauses. Without reproducing the copyrighted amendment text, the amendment's practical effect is that an organization's context analysis (Clause 4.2, interested parties) and risk-planning process (Clause 6.1.3, risk treatment) should consider whether climate change is a relevant issue for the ISMS. The table below illustrates how this fictional consideration was applied for NorthBridge.

Climate-Related External Issue	Increasing frequency of extreme-weather events potentially affecting cloud region availability, supplier operations, and workforce continuity (fictional, illustrative).
Potential Information-Security Relevance	Regional service disruption could affect availability commitments; workforce disruption could affect incident response and change-management staffing continuity.
Interested-Party Expectations	Enterprise customers increasingly ask about multi-region resilience and business continuity planning as part of vendor due diligence.
ISMS Consideration	Climate-related disruption scenarios are considered within NorthBridge's fictional business impact analysis and business continuity planning (Section 30), alongside more conventional technical and operational disruption scenarios.
Evidence	EV-018 (Disaster Recovery Plan), EV-030 (Business Continuity Test Results) — illustrative evidence reference only.
Illustrative Conclusion	NorthBridge's fictional ISMS context analysis and business continuity planning give appropriate, proportionate consideration to climate-related disruption; this is not a compliance gap area in this sample and no finding is raised against it.

This treatment of Amendment 1:2024 is illustrative and intentionally does not overstate the amendment's scope. It affects context and planning considerations; it does not add new mandatory Annex A controls.

Broader 2026 Considerations (Illustrative, Non-Exhaustive)

- Continued regulatory attention to cloud service resilience and concentration risk across critical sectors.
- Growing customer and contractual expectations around AI system governance intersecting with existing information security risk management practices.
- Ongoing evolution of sector-specific privacy and data protection expectations relevant to the interface addressed in Section 32.

These broader considerations are forward-looking context notes, not new assessed ISO/IEC 27001:2022 requirements, and are clearly separated here from the current Annex A:2022 control set assessed throughout this report.

58 ASSESSMENT LIMITATIONS

This fictional sample assessment is subject to the following limitations, each of which should be read together with the Important Disclaimer (Section 02):

- NorthBridge Digital Services, Inc. is fictional; no real organization was assessed.
- No real systems, networks, or production environments were accessed, scanned, or tested.
- No real evidence was collected, and no real personnel interviews occurred.
- No actual information security incidents occurred; the tabletop scenario in Section 29 is entirely fictional.
- No actual vulnerabilities were discovered; vulnerability findings referenced throughout are illustrative sample data.
- All metrics, KPIs, maturity scores, and dashboard figures are illustrative and fictional.
- All findings, risk ratings, and control statuses are fictional and were constructed for demonstration purposes.
- No actual ISO/IEC 27001 certification audit was performed, and no certification decision was made.
- No ISO/IEC 27001 certificate was issued as a result of, or in connection with, this document.
- This document is not evidence of ISO/IEC 27001 certification for any organization.
- This document is not legal, regulatory, or compliance advice.
- This document is not an accreditation or certification-body opinion of any kind.
- TMG Security is not an accredited ISO/IEC 27001 certification body.

- A formal certification decision, if pursued, must be made by an appropriately accredited independent certification body following an actual certification audit.
- This report should not be relied upon as evidence of compliance, certification, assurance, or security posture of any real organization.
- Findings, evidence references, and testing results represent an illustrative point-in-time construction and do not reflect an actual, ongoing assessment engagement.

59 GLOSSARY

ISMS	Information Security Management System — the overall system of policies, processes, and controls an organization uses to manage information security risk.
SoA	Statement of Applicability — the documented list of Annex A controls, their applicability, justification, and implementation status.
Risk Treatment	The process of selecting and implementing measures to modify (reduce, avoid, transfer, or accept) information security risk.
Information Asset	Information, or a system/component that stores, processes, or transmits information, that has value to the organization.
Interested Party	A person or organization that can affect, be affected by, or perceive itself to be affected by the ISMS.
Nonconformity	Non-fulfilment of a requirement — used in this report's illustrative internal audit classification, not as a certification-body determination.
Corrective Action	Action taken to eliminate the cause of a nonconformity and prevent recurrence.
Internal Audit	A planned, independent review to determine whether the ISMS conforms to its own requirements and to ISO/IEC 27001.
Management Review	A planned, periodic review by top management of the ISMS's continuing suitability, adequacy, and effectiveness.
Annex A	The normative annex to ISO/IEC 27001:2022 listing the 93 information security controls organized into four themes (A.5–A.8).
Certification Audit	A formal audit performed by an accredited independent certification body resulting in a certification decision. Not performed as part of this sample.
Readiness Assessment	A pre-certification evaluation, such as this sample, intended to identify gaps before a formal certification audit.
Statement of Applicability	See SoA above.
Residual Risk	The risk remaining after risk treatment has been applied.
Risk Owner	The individual accountable for managing a specific risk and its treatment.
Control Objective	The intended outcome a control is designed to achieve.
Inherent Risk	The level of risk before considering the effect of existing controls.
Trust Services / Clause	A defined section of the ISO/IEC 27001:2022 management-system requirements (Clauses 4–10).
Subservice / Supplier Organization	A third-party vendor whose services are part of, or support, the assessed environment.
Opportunity for Improvement	A suggestion to strengthen an already-conforming control area, used as an illustrative consulting classification in this sample.

60 CONTACT & FINAL DISCLAIMER

Cybersecurity | *SOC* | *VAPT* | *GRC* | *MDR* | *Compliance Solutions* | *Corporate Trainings*

Web: www.tmgsec.com **Email:** security@tmgsec.com
USA Office: 117 South Lexington Street, STE 100, Harrisonville, MO 64701
Support: support@tmgsec.com | **Phone:** +1 (816) 793-1929
WhatsApp: +1 (480) 680-0342

Final Disclaimer

FICTIONAL SAMPLE REPORT — NOT AN ACTUAL ISO/IEC 27001 CERTIFICATION AUDIT

This document was created by TMG Security solely to demonstrate information security management system assessment methodology, audit-readiness analysis, and professional GRC reporting standards. NorthBridge Digital Services, Inc. is fictional. No actual ISO/IEC 27001 audit, certification audit, certification decision, or certificate issuance was performed or issued. All findings, evidence references, assessment results, metrics, interview records, and management responses are illustrative.