

IT & Cyber Capability Assessment

Complete Questions & Answer Options

Current Version - 21/11/2025

Assessment Overview

Purpose: This document contains all current assessment questions and response options for stakeholder review.

Structure: 4 strategic capability pillars with varying question counts = 35 total questions

Answer Scale: Each question uses a 6-point maturity scale from "Not in place" (lowest) to "Mature/Optimised" (highest).

Scoring: Responses convert to numerical scores: Not in place (0), Ad hoc (20), Partially implemented (40), Defined but inconsistently applied (60), Consistently applied (80), Mature/Optimised (100).

Core IT Operations & Reliability — Questions 1–8 (8 questions)

Question 1: Device Management

Devices are centrally managed with consistent configurations and security baselines.

Answer Options:

○ **Not in place**

Not in place — Devices are unmanaged, unpatched, and configured inconsistently, with minimal visibility.

○ **Ad hoc**

Ad hoc — Some devices follow standards, but others are unmanaged or configured manually.

○ **Partially implemented**

Partially implemented — A device management tool or baseline exists, but coverage gaps or inconsistent enforcement remain.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Device standards and baselines are documented, but not applied uniformly across device types or teams.

○ **Consistently applied**

Consistently applied — Devices are managed with standardised baselines, policies, and compliance monitoring across teams.

○ **Mature / Optimised**

Mature / Optimised — Device management is automated, well-governed, and continuously improved with strong compliance tracking.

Question 2: Backup & Recovery

Backups are reliable, complete, and regularly tested for successful recovery.

Answer Options:

○ **Not in place**

Not in place — Backups are missing, unreliable, or unknown; recovery capabilities are unclear and untested.

○ **Ad hoc**

Ad hoc — Some backups exist, but coverage is inconsistent, stored informally, or rarely validated.

○ **Partially implemented**

Partially implemented — Backups cover key systems but have gaps, outdated configurations, or untested restore procedures.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Backup routines and retention policies are defined but not followed uniformly across teams or systems.

○ **Consistently applied**

Consistently applied — Backups are performed reliably with documented schedules, validated restores, and appropriate retention across teams.

○ **Mature / Optimised**

Mature / Optimised — Backup and recovery processes are regularly tested, risk-based, automated where possible, and aligned to RPO/RTO requirements.

Question 3: Monitoring & Alerting

Monitoring and alerting identify issues proactively before they impact users.

Answer Options:

○ **Not in place**

Not in place — Monitoring is minimal or absent; outages or issues are usually discovered by users.

○ **Ad hoc**

Ad hoc — Some systems generate alerts, but monitoring is inconsistent and largely reactive.

○ **Partially implemented**

Partially implemented — Monitoring covers key systems, but alert thresholds, ownership, or response workflows are inconsistent.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Monitoring standards exist, but different teams vary in coverage, configuration, and responsiveness.

○ **Consistently applied**

Consistently applied — Critical systems are monitored with actionable alerts, owned by the right teams, and responded to reliably.

○ **Mature / Optimised**

Mature / Optimised — Monitoring is comprehensive, proactively tuned, and integrated with processes for alert reduction, trend analysis, and reliability engineering.

Question 4: System Reliability & Stability

Core IT systems (network, servers, cloud, SaaS) operate reliably with minimal unplanned outages.

Answer Options:

○ **Not in place**

Not in place — Systems are unreliable with frequent outages; stability is poor and unpredictable.

○ **Ad hoc**

Ad hoc — Some systems are stable, but outages are common and resolution is often slow or inconsistent.

○ **Partially implemented**

Partially implemented — Most systems are reasonably stable, but some areas still experience regular disruptions or slow recovery.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Stability processes exist, but some systems or teams still experience more outages than expected.

○ **Consistently applied**

Consistently applied — Core systems are stable and reliable, with rare unplanned outages and fast resolution when they occur.

○ **Mature / Optimised**

Mature / Optimised — Systems are highly reliable with exceptional uptime, automated recovery, and predictable performance under load.

Question 5: Capacity & Performance

Capacity and performance are monitored and reviewed to prevent service degradation.

Answer Options:

○ **Not in place**

Not in place — There is no structured monitoring or planning for capacity or performance.

○ **Ad hoc**

Ad hoc — Teams react to capacity or performance issues as they arise, with little forward planning.

○ **Partially implemented**

Partially implemented — Basic capacity metrics or performance reports exist, but analysis and planning are inconsistent.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Capacity and performance processes are documented, but adoption varies across systems and teams.

○ **Consistently applied**

Consistently applied — Teams monitor capacity and performance proactively and plan based on usage trends and business demand.

○ **Mature / Optimised**

Mature / Optimised — Capacity and performance management is data-driven, forecasted, automated where possible, and aligned to service continuity goals.

Question 6: Standardisation & Configuration

IT standards and system configurations are defined and applied consistently across the environment.

Answer Options:

○ **Not in place**

Not in place — No standards exist; systems are configured inconsistently and documentation is minimal.

○ **Ad hoc**

Ad hoc — Some informal standards exist, but configuration varies widely and enforcement is inconsistent.

○ **Partially implemented**

Partially implemented — Basic standards are documented, but many systems still vary in configuration and compliance.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Standards are well-documented, but different teams apply them with varying degrees of consistency.

○ **Consistently applied**

Consistently applied — Standards are enforced across most systems with regular compliance checking and remediation.

○ **Mature / Optimised**

Mature / Optimised — Standards are automated, continuously monitored, and dynamically updated based on best practices and lessons learned.

Question 7: Routine IT Automation

Routine IT tasks (provisioning, checks, updates) are automated where possible.

Answer Options:

○ **Not in place**

Not in place — Routine tasks are performed manually, increasing workload and error rates.

○ **Ad hoc**

Ad hoc — Some automation exists but is created informally by individuals without standardisation.

○ **Partially implemented**

Partially implemented — A few routine tasks are automated, but coverage is limited and reliability varies.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Automation standards exist, but adoption varies across teams or systems.

○ **Consistently applied**

Consistently applied — Routine tasks are automated in line with defined standards, reducing manual effort and improving reliability.

○ **Mature / Optimised**

Mature / Optimised — Automation is strategically applied, monitored, and refined, contributing to operational efficiency and service reliability.

Question 8: Integration & Data Flow

Systems integrate effectively with clear data flows and minimal manual workarounds.

Answer Options:

○ **Not in place**

Not in place — Systems operate in isolation with frequent manual data transfer and workarounds.

○ **Ad hoc**

Ad hoc — Some basic integrations exist, but most data still moves manually or through unreliable workarounds.

○ **Partially implemented**

Partially implemented — A few key integrations operate reliably, but duplication or manual handling remains common.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Integration standards exist, but systems vary in how consistently they apply them.

○ **Consistently applied**

Consistently applied — Systems integrate cleanly with defined data flows and minimal duplication or manual handling across teams.

○ **Mature / Optimised**

Mature / Optimised — Integration architecture is well-designed, automated, monitored, and continuously improved for reliability and accuracy.

Strategic Service Management (ITSM + ESM) — Questions 9–17 (9 questions)

Question 9: Service Desk Process Consistency

Service desk processes for incident, request, and escalation are documented and consistently followed.

Answer Options:

○ **Not in place**

Not in place — No defined service desk process exists; issues are raised informally via email, chat, or verbally and may be lost or duplicated.

○ **Ad hoc**

Ad hoc — Some issues are captured in a system, but many are handled outside any formal process and there is no consistent way of working.

○ **Partially implemented**

Partially implemented — A service desk tool and basic process exist, but categories, triage rules, or workflows are incomplete or not used consistently across teams.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — The service desk process is documented and communicated, but different teams and individuals still bypass or interpret it differently.

○ **Consistently applied**

Consistently applied — The documented service desk process is followed across teams with clear triage, categorisation, and escalation, and exceptions are rare.

○ **Mature / Optimised**

Mature / Optimised — Service desk processes are consistently applied, measured, and regularly improved using data, feedback, and lessons learned.

Question 10: Incident Management Maturity

Incidents are logged, triaged, and resolved using a defined incident management framework.

Answer Options:

○ **Not in place**

Not in place — No defined service desk process exists; issues are raised informally via email, chat, or verbally and may be lost or duplicated.

○ **Ad hoc**

Ad hoc — Some issues are captured in a system, but many are handled outside any formal process and there is no consistent way of working.

○ **Partially implemented**

Partially implemented — A service desk tool and basic process exist, but categories, triage rules, or workflows are incomplete or not used consistently across teams.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Incident management processes are documented, but different teams may bypass or interpret procedures differently; Major Incident runbooks and PIRs exist but are not consistently executed or followed through with actions.

○ **Consistently applied**

Consistently applied — Incidents follow a reliable framework with consistent logging, triage, and escalation across all teams; Major Incident runbooks and PIRs are executed consistently with proper follow-through on actions.

○ **Mature / Optimised**

Mature / Optimised — Incident management is mature with strong metrics, automated workflows, and regular process improvements; Major Incident procedures and PIRs drive measurable improvements and trend analysis prevents recurring issues.

Question 11: Service Catalog & Self-Service

A clear service catalog and self-service portal is available and used effectively.

Answer Options:

○ **Not in place**

Not in place — There is no formal service catalogue; users are unsure what IT provides or how to request it.

○ **Ad hoc**

Ad hoc — Some services or request types are described informally (e.g. wiki pages or emails), but there is no structured catalogue or consistent categories.

○ **Partially implemented**

Partially implemented — A basic service and request catalogue exists, but coverage is incomplete, naming is inconsistent, and users often choose the wrong options.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Services and request categories are defined and available, but not all teams or channels use them consistently, and some services remain 'hidden'.

○ **Consistently applied**

Consistently applied — A clear, user-friendly service catalogue and request categories are published and used across channels, guiding users to the right request types.

○ **Mature / Optimised**

Mature / Optimised — The service catalogue is actively maintained, aligned to business language, and used to drive automation, routing, reporting, and continual improvement.

Question 12: Change Management Control

Changes follow a documented change management process including approvals and communication.

Answer Options:

○ **Not in place**

Not in place — Changes are made directly in production with little or no review, approval, or communication, and risk is not formally assessed.

○ **Ad hoc**

Ad hoc — Some high-risk changes are discussed or approved informally, but there is no standard change process or change record.

○ **Partially implemented**

Partially implemented — A change process exists with basic logging and approvals, but many changes still bypass it or are incompletely documented.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Change management procedures are documented but may be bypassed for urgent changes or interpreted differently across teams; Normal, Standard, and Emergency change paths are defined but not applied consistently.

○ **Consistently applied**

Consistently applied — Changes consistently follow documented procedures with proper approvals and communication; Normal, Standard, and Emergency change paths are applied reliably with rare exceptions.

○ **Mature / Optimised**

Mature / Optimised — Change management is data-driven with mature Normal, Standard, and Emergency processes; CAB reviews, success metrics, and automated workflows drive continuous refinement and risk reduction.

Question 13: Knowledge Management

Knowledge articles are documented, updated, and used to support consistent service delivery.

Answer Options:

- **Not in place**

Not in place — There is no central knowledge base; support relies on individual memory and undocumented 'tribal knowledge'.

- **Ad hoc**

Ad hoc — Some notes or documents exist, often in personal drives or ad hoc locations, but they are incomplete, outdated, or hard to find.

- **Partially implemented**

Partially implemented — A knowledge repository exists with useful content, but coverage is patchy and many key procedures are still undocumented or out of date.

- **Defined but inconsistently applied**

Defined but inconsistently applied — Standards for knowledge articles are defined, but not all teams contribute or maintain content, leading to mixed quality and trust.

- **Consistently applied**

Consistently applied — Knowledge and support documentation is maintained in a central location, kept reasonably current, and used regularly by staff.

- **Mature / Optimised**

Mature / Optimised — Knowledge management is embedded in daily work, with articles regularly reviewed, improved, and linked to tickets, and coverage measured and actively managed.

Question 14: Workflow Automation Adoption

Manual processes have been identified and prioritised for automation.

Answer Options:

○ **Not in place**

Not in place — Processes are fully manual, relying on staff to complete repetitive actions.

○ **Ad hoc**

Ad hoc — Some automation exists, usually created by individuals without structure or standardisation.

○ **Partially implemented**

Partially implemented — Basic automations exist for certain processes, but coverage is limited and inconsistent.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Automation standards and tools are defined, but teams vary widely in adoption and usage.

○ **Consistently applied**

Consistently applied — Automations are consistently used to reduce manual steps, improve accuracy, and speed up workflows.

○ **Mature / Optimised**

Mature / Optimised — Automation is strategically applied, monitored for effectiveness, and continuously expanded based on data and improvement opportunities.

Question 15: SLAs & Performance Visibility

SLAs, KPIs, and service performance metrics are tracked and reviewed regularly.

Answer Options:

○ **Not in place**

Not in place — Service performance is not measured; there are no defined SLAs, KPIs, or regular performance reports.

○ **Ad hoc**

Ad hoc — Some metrics or ad hoc reports exist, but they are produced irregularly and are not used in structured reviews or decisions.

○ **Partially implemented**

Partially implemented — Key SLAs or KPIs are defined and measured for some services, but data quality is variable and reporting is inconsistent.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Standard performance dashboards or reports exist, but not all services are covered and regular review meetings only happen in some areas.

○ **Consistently applied**

Consistently applied — Service performance is measured using agreed SLAs and KPIs, reported regularly, and discussed in structured reviews with clear follow-up actions.

○ **Mature / Optimised**

Mature / Optimised — Performance metrics are trusted, reviewed at multiple levels, used to drive improvement initiatives, and aligned to business outcomes and customer experience.

Question 16: Continual Service Improvement

Continuous improvement practices are embedded into service management operations.

Answer Options:

○ **Not in place**

Not in place — There is no structured approach to service improvement; issues are fixed only when they become urgent.

○ **Ad hoc**

Ad hoc — Improvements are made reactively or driven by individuals, with no central list, prioritisation, or tracking.

○ **Partially implemented**

Partially implemented — Some recurring issues and improvement opportunities are captured, but follow-through is inconsistent and many actions stall.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — A continual improvement register or process exists, but its use varies by team and outcomes are not always tracked or reported.

○ **Consistently applied**

Consistently applied — Continual improvement is part of regular operations, with identified actions, owners, and timeframes, and progress is reviewed.

○ **Mature / Optimised**

Mature / Optimised — Continuous improvement is embedded culturally, supported by data and feedback, with clear prioritisation, benefits tracking, and visible outcomes.

Question 17: Cross-team Workflows

Cross-team workflows are well-defined and minimise handoff delays.

Answer Options:

○ **Not in place**

Not in place — Handoffs are informal or unclear; work is frequently delayed, duplicated, or lost between teams.

○ **Ad hoc**

Ad hoc — Some handoff steps exist, but they rely heavily on individuals and are often incomplete or inconsistent.

○ **Partially implemented**

Partially implemented — Basic handoff processes or tools exist, but roles, responsibilities, or timing remain unclear in many cases.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Handoff expectations are documented, but teams vary in how reliably they follow them.

○ **Consistently applied**

Consistently applied — Cross-team handoffs are clear, predictable, and completed as part of standard workflows with minimal friction.

○ **Mature / Optimised**

Mature / Optimised — Handoffs are streamlined, measured, and continuously improved, with strong coordination and minimal rework across teams.

Information Security & Governance — Questions 18–26 (9 questions)

Question 18: MFA and Identity Protections

Multi-factor authentication (MFA) is enforced for all staff and all administrator accounts.

Answer Options:

☐ **Not in place**

Not in place — MFA is largely absent; most users and admins authenticate with only a username and password.

☐ **Ad hoc**

Ad hoc — MFA is enabled for some systems or user groups, but coverage is limited and there is no clear policy or standard.

☐ **Partially implemented**

Partially implemented — MFA is enabled for many staff or key applications, but significant gaps remain, especially for privileged accounts or legacy systems.

☐ **Defined but inconsistently applied**

Defined but inconsistently applied — An MFA and identity security policy is defined, but enforcement is inconsistent across applications, user groups, or environments.

☐ **Consistently applied**

Consistently applied — MFA and identity protections are applied in line with policy across staff and administrators for most critical systems, with few exceptions.

☐ **Mature / Optimised**

Mature / Optimised — Identity security is robust, with comprehensive MFA coverage, conditional access, regular access reviews, and alignment with best-practice frameworks.

Question 19: Identity & Access Management

Identity and access management is centralised with strong lifecycle processes.

Answer Options:

○ **Not in place**

Not in place — Joiner, mover, leaver processes are largely manual or absent; access is created and removed inconsistently.

○ **Ad hoc**

Ad hoc — Some lifecycle steps occur (e.g., manual deprovisioning), but accuracy and timing vary significantly.

○ **Partially implemented**

Partially implemented — Basic IAM processes exist, but access reviews, provisioning accuracy, or timely deprovisioning are inconsistent.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — IAM policies and lifecycle steps are defined, but teams differ in how reliably they follow them.

○ **Consistently applied**

Consistently applied — IAM processes are standardised, timely, audited, and followed reliably across teams.

○ **Mature / Optimised**

Mature / Optimised — IAM is automated, secure, and well-governed, with regular access reviews and alignment to least-privilege principles.

Question 20: Admin Rights and Least Privilege

Admin rights are restricted, monitored, and follow least-privilege principles.

Answer Options:

○ **Not in place**

Not in place — Privileged accounts are unmanaged, widely shared, or used without oversight.

○ **Ad hoc**

Ad hoc — Some privileged accounts are restricted, but access is inconsistent and rarely reviewed.

○ **Partially implemented**

Partially implemented — Controls exist for privileged access, but coverage gaps, shared credentials, or outdated permissions remain.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Policies for privileged access and reviews exist, but teams vary in how reliably they follow them.

○ **Consistently applied**

Consistently applied — Privileged access is role-based, properly assigned, monitored, and regularly reviewed across teams.

○ **Mature / Optimised**

Mature / Optimised — Privileged access management is strong, with automated workflows, just-in-time access, audit trails, and continuous review.

Question 21: Endpoint Protection (EDR/XDR)

Endpoint protection (EDR or next-gen antivirus) is deployed across laptops, workstations, and servers.

Answer Options:

○ **Not in place**

Not in place — Endpoints have no standard protection beyond basic OS defaults, and there is no central visibility of threats or activity.

○ **Ad hoc**

Ad hoc — Some devices have antivirus or protection tools installed, but coverage is incomplete and not centrally managed.

○ **Partially implemented**

Partially implemented — An endpoint protection or EDR tool is deployed to many devices, but coverage gaps, inconsistent policies, or limited monitoring remain.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Standard endpoint protection policies exist and are deployed, but not all device types or locations are consistently covered or monitored.

○ **Consistently applied**

Consistently applied — Endpoint protection is deployed and managed centrally across supported devices, with standard policies and alerts monitored by appropriate teams.

○ **Mature / Optimised**

Mature / Optimised — EDR/XDR is fully embedded, with broad coverage, tuned alerts, threat hunting, and integration into wider security monitoring and incident response processes.

Question 22: Vulnerability Management

Patching and vulnerability remediation occur on a regular, enforced schedule.

Answer Options:

○ **Not in place**

Not in place — Patching is largely manual or neglected; many systems remain out of date and there is no structured approach to vulnerabilities.

○ **Ad hoc**

Ad hoc — Some critical patches are applied when issues arise or vendors prompt action, but there is no regular, planned patch cycle.

○ **Partially implemented**

Partially implemented — Basic patch schedules or tooling exist, but coverage is incomplete, exceptions are common, and vulnerability remediation is slow or inconsistent.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — A patch management process and vulnerability workflow exist, but adherence varies across systems, teams, or business units.

○ **Consistently applied**

Consistently applied — Patching and vulnerability remediation follow a defined cycle with good coverage, documented exceptions, and generally timely remediation.

○ **Mature / Optimised**

Mature / Optimised — Patch and vulnerability management are risk-based, well-governed, and measured, with rapid response to critical issues and continuous improvement of coverage and timeliness.

Question 23: Logging and SIEM

Logging, alerting, and monitoring are enabled for critical systems.

Answer Options:

○ **Not in place**

Not in place — Security logs are minimal or missing, and alerts are not monitored.

○ **Ad hoc**

Ad hoc — Some systems generate logs or alerts, but monitoring is inconsistent and largely reactive.

○ **Partially implemented**

Partially implemented — Key systems produce logs and alerts, but coverage is incomplete and many events go unreviewed.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — A monitoring process exists, but teams differ in how consistently they review and respond to alerts.

○ **Consistently applied**

Consistently applied — Security logs and alerts are centrally collected, reviewed, and actioned using consistent processes.

○ **Mature / Optimised**

Mature / Optimised — Monitoring is comprehensive, integrated with SIEM/XDR, and used proactively to detect threats and drive improvements.

Question 24: Event Correlation & Root Cause Analysis

Incident patterns and root causes are identified through event correlation.

Answer Options:

○ **Not in place**

Not in place — Recurring issues go uninvestigated; only symptoms are addressed.

○ **Ad hoc**

Ad hoc — RCA occurs occasionally, usually when issues are severe or escalated, but not as routine practice.

○ **Partially implemented**

Partially implemented — Some teams perform RCA for recurring issues, but follow-through or documentation is inconsistent.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — An RCA process exists, but adoption varies and outcomes are not always reviewed or acted upon.

○ **Consistently applied**

Consistently applied — RCA is performed consistently for recurring issues, with documented actions and clear ownership.

○ **Mature / Optimised**

Mature / Optimised — RCA is proactive, data-driven, and used to prevent issues, reduce risk, and drive measurable improvements in reliability.

Question 25: Security Operations Monitoring

Systems and applications are monitored with actionable alerts.

Answer Options:

○ **Not in place**

Not in place — Monitoring is minimal or absent; outages or issues are usually discovered by users.

○ **Ad hoc**

Ad hoc — Some systems generate alerts, but monitoring is inconsistent and largely reactive.

○ **Partially implemented**

Partially implemented — Monitoring covers key systems, but alert thresholds, ownership, or response workflows are inconsistent.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Monitoring standards exist, but different teams vary in coverage, configuration, and responsiveness.

○ **Consistently applied**

Consistently applied — Critical systems are monitored with actionable alerts, owned by the right teams, and responded to reliably.

○ **Mature / Optimised**

Mature / Optimised — Monitoring is comprehensive, proactively tuned, and integrated with processes for alert reduction, trend analysis, and reliability engineering.

Question 26: Security Culture & AI-Assisted Tools

Intelligent tools (AI-assisted or advanced rules-based automation) support operational decision-making and reduce manual workload.

Answer Options:

○ **Not in place**

Not in place — Teams rely solely on manual checks and judgment; no automation or intelligence supports decisions.

○ **Ad hoc**

Ad hoc — Some tools provide basic suggestions or alerts, but usage is inconsistent and not embedded in workflows.

○ **Partially implemented**

Partially implemented — Tools with limited intelligence exist, but adoption is patchy and insights are not consistently actioned.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Intelligent tooling is available, but teams vary in how reliably they use it for operational decisions.

○ **Consistently applied**

Consistently applied — Intelligent tooling supports operations through standardised insights, alerting, and recommendations across teams.

○ **Mature / Optimised**

Mature / Optimised — Intelligent tooling is fully integrated, predictive, and used to proactively optimise operations and prevent issues.

Risk, Compliance, & Assurance — Questions 27–35 (9 questions)

Question 27: Framework Alignment (E8/ISO/SMB1001)

Cyber controls are aligned with Essential 8, ISO 27001, or SMB1001 requirements.

Answer Options:

☐ **Not in place**

Not in place — There is no structured alignment to recognised security frameworks.

☐ **Ad hoc**

Ad hoc — Some controls exist, but they have not been mapped or assessed against any framework.

☐ **Partially implemented**

Partially implemented — Initial alignment work has occurred, but gaps are significant and controls are inconsistently applied.

☐ **Defined but inconsistently applied**

Defined but inconsistently applied — A framework mapping or maturity assessment exists, but adoption and governance vary across teams.

☐ **Consistently applied**

Consistently applied — Controls are aligned to a chosen framework and applied reliably, with documented improvements underway.

☐ **Mature / Optimised**

Mature / Optimised — Security controls are fully aligned, verified regularly, and incorporated into governance, audit, and improvement cycles.

Question 28: Platform Governance

Platforms and tooling have clear governance, admin roles, and lifecycle processes.

Answer Options:

○ **Not in place**

Not in place — Tooling decisions are ad hoc; lifecycle management is largely absent.

○ **Ad hoc**

Ad hoc — Some tools follow lifecycle processes, but many are unmanaged or lack governance.

○ **Partially implemented**

Partially implemented — Governance and lifecycle processes exist, but coverage or compliance is inconsistent.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Tooling governance is documented, but different teams follow it to varying degrees.

○ **Consistently applied**

Consistently applied — Platforms and tools follow defined governance, lifecycle, renewal, and decommissioning processes reliably.

○ **Mature / Optimised**

Mature / Optimised — Tooling governance is strategic, data-driven, and ensures well-managed, cost-effective, secure platforms across the environment.

Question 29: Operational Governance

Operational reviews and governance meetings occur regularly with actionable outcomes.

Answer Options:

○ **Not in place**

Not in place — There is no formal governance structure; operational decisions are fragmented and reactive.

○ **Ad hoc**

Ad hoc — Some meetings or decision processes occur, but they lack consistency or clear purpose.

○ **Partially implemented**

Partially implemented — Governance structures exist, but participation, agendas, or follow-up actions are inconsistent.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Governance processes are documented, but teams vary in attendance, adherence, or execution.

○ **Consistently applied**

Consistently applied — Operational governance is structured, attended, and used to review performance, risks, and priorities reliably.

○ **Mature / Optimised**

Mature / Optimised — Governance is strategic, data-driven, and supports proactive decision-making with clear accountability and continual refinement.

Question 30: Resilience Strategy (Backup/DR)

Backup and disaster recovery architecture meets defined RTO/RPO requirements.

Answer Options:

○ **Not in place**

Not in place — DR plans are missing, outdated, or untested; recovery capabilities are unclear.

○ **Ad hoc**

Ad hoc — Some DR components exist, but planning and testing are inconsistent or informal.

○ **Partially implemented**

Partially implemented — DR architecture exists for key systems, but gaps, outdated components, or untested failover paths remain.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — DR plans and architectures are documented, but testing or adherence varies across teams.

○ **Consistently applied**

Consistently applied — Backup and DR architecture is aligned to RPO/RTO, tested periodically, and reliably maintained.

○ **Mature / Optimised**

Mature / Optimised — DR architecture is resilient, automated where possible, regularly tested, and improved based on lessons learned.

Question 31: Standard Operating Procedures

Standard operating procedures are well-defined and used consistently across operations.

Answer Options:

○ **Not in place**

Not in place — There are no documented SOPs; operational work is done informally and varies widely.

○ **Ad hoc**

Ad hoc — Some SOPs exist, but they are incomplete, outdated, or not widely used.

○ **Partially implemented**

Partially implemented — Core SOPs are documented, but coverage is limited and updates are inconsistent.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — SOPs are documented and accessible, but teams do not adopt them consistently, leading to variable outcomes.

○ **Consistently applied**

Consistently applied — SOPs guide daily operations, are kept current, and help ensure consistent quality across teams.

○ **Mature / Optimised**

Mature / Optimised — SOPs are well-maintained, version-controlled, aligned to best practices, and used to support continuous improvement and risk reduction.

Question 32: Process Documentation

Core business processes are documented and consistently followed.

Answer Options:

○ **Not in place**

Not in place — Processes are undocumented; staff rely on memory and informal knowledge.

○ **Ad hoc**

Ad hoc — Some processes are documented informally, but coverage and quality vary significantly.

○ **Partially implemented**

Partially implemented — Key processes are documented, but not comprehensively or consistently, and updates are irregular.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Standard documentation templates and processes exist, but teams vary in maintenance and adoption.

○ **Consistently applied**

Consistently applied — Process documentation is clear, accessible, regularly updated, and followed across teams.

○ **Mature / Optimised**

Mature / Optimised — Processes are well-defined, versioned, measured, and continuously improved through regular review cycles.

Question 33: Process Metrics & ROI

Operational processes have defined metrics and are monitored regularly.

Answer Options:

○ **Not in place**

Not in place — Metrics are not defined or measured.

○ **Ad hoc**

Ad hoc — Some metrics are collected manually, but irregularly and without analysis.

○ **Partially implemented**

Partially implemented — Key metrics are tracked, but data quality, completeness, or usage is inconsistent.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Dashboards, KPIs, or reports exist, but not all teams use them reliably to drive decisions.

○ **Consistently applied**

Consistently applied — Metrics are defined, measured, reviewed regularly, and used to guide operational decisions.

○ **Mature / Optimised**

Mature / Optimised — Metrics are robust, aligned to outcomes, used in planning, and drive structured improvement initiatives.

Question 34: Shadow IT & Vendor Risk

Approvals and authorisations use automated workflows rather than email-based processes.

Answer Options:

☐ **Not in place**

Not in place — Approvals happen informally via email or verbal agreement.

☐ **Ad hoc**

Ad hoc — Some approvals are tracked, but there is no structured workflow or automation.

☐ **Partially implemented**

Partially implemented — Basic automated approvals exist, but coverage is limited and inconsistent.

☐ **Defined but inconsistently applied**

Defined but inconsistently applied — Approval workflows are documented and available, but not all teams use them reliably.

☐ **Consistently applied**

Consistently applied — Approval workflows are automated, used across teams, and reduce delays and manual tracking.

☐ **Mature / Optimised**

Mature / Optimised — Approval automation is integrated into end-to-end processes, monitored for efficiency, and optimised regularly.

Question 35: Strategic Alignment

Process documentation and training materials are current and easily accessible.

Answer Options:

○ **Not in place**

Not in place — Training materials are missing, outdated, or scattered; new staff rely on informal guidance.

○ **Ad hoc**

Ad hoc — Some training resources exist, but they vary in quality and are not centrally managed.

○ **Partially implemented**

Partially implemented — Training materials cover core topics, but gaps exist and updates are irregular.

○ **Defined but inconsistently applied**

Defined but inconsistently applied — Training standards exist, but not all teams maintain or use materials consistently.

○ **Consistently applied**

Consistently applied — Training materials are current, clear, accessible, and used as part of onboarding and ongoing development.

○ **Mature / Optimised**

Mature / Optimised — Training is structured, regularly updated, aligned to roles, and incorporated into continuous learning frameworks.