SAMA Examination Evidence Index

An independent, illustrative evidence guide: what a supervisory examination typically requests, control area by control area. The artifact, its owner, the cadence that makes it credible, the form it is accepted in, and the question asked in the room. 38 control areas mapped across NCA ECC-2:2024, SAMA CSF v1.0, and SAMA ITGF.

Provenance: framework references are carried verbatim from the Security Lab crosswalks (author-reviewed, checked against the official NCA and SAMA publications). The five practice columns are authored judgement from generic supervisory-examination experience. Framework references were checked in an AI-assisted review pass (last pass 2026-08-09) with Mohammed AlYahya as the domain expert of record. References are control-area anchors, not equivalence claims: mapping strength (Direct / Partial / None) is in the Excel register and the per-row rationale in the three-way crosswalk.

What this is not: this guide is not issued, endorsed or reviewed by SAMA or the NCA, and it is not a definitive or exhaustive list of examination requests. Actual requests vary with institution size, maturity target and examination scope. No row describes any institution's examination or predicts a supervisory outcome.

How to use it: read your row, pull the artifact, check it against the "form examiners accept" column, and close the gap before the request letter arrives. The most common failure is not a missing control. It is a real control whose artifact cannot prove it: undated, unsigned, batch-produced, or owned by nobody.

Control area	Artifact an examination requests	Owner	Cadence	Form examiners accept	Common examiner challenge
GOVERNANCE: 11 CONTROL AREAS					
1-1-1 Cybersecurity strategy defined, documented, approved `ECC 1-1-1 · CSF 3.1.2 · ITGF 3.1.2`	Strategy document with approval evidence, plus the linked implementation roadmap with a current-to-target gap analysis	CISO / Head of Cybersecurity	Annual review	Approved by the authority the applicable framework mandates: approval date visible, minutes referenced, roadmap items dated and owned	"Show me the roadmap line that this year's budget actually funded."
1-2-1 Independent cybersecurity department established `ECC 1-2-1 · CSF 3.1.1 · ITGF 3.1.1`	Approved organisation chart with reporting lines, the head-of-function appointment letter and job description, and the charter evidencing a reporting line outside IT operations. On the ITGF line, the CIO appointment file: full-time senior manager, Saudi national, qualification evidence, and SAMA's written no-objection obtained before the assignment	HR + CISO	On appointment + annual confirmation	A dated, board-approved chart version with the appointment and no-objection letters filed alongside it. Independence of the function is evidenced by the performance-management and remuneration records, not by the	"Show me the delegation that sets who appraises the head of cybersecurity, then the last appraisal record and the remuneration approval that went with it."

Control area	Artifact an examination requests	Owner	Cadence	Form examiners accept	Common examiner challenge
				chart, which shows reporting lines only	
1-2-3 Cybersecurity supervisory committee ECC 1-2-3 · CSF 3.1.1 · ITGF 3.1.1	Committee charter or terms of reference with membership and quorum, dated minutes covering the last twelve months, and evidence that decisions and risks were escalated to the board. On the ITGF line, the ITSC charter tested against the five elements 3.1.1 enumerates, its board mandate, and attendance for the CRO, CISO, compliance officer, business heads and CIO	Committee secretary (CISO / CIO for the ITSC)	Quarterly minimum	Minutes recording decisions and attendance against the quorum the charter sets, plus evidence the required cadence was met across the period. Where a meeting was deferred or short of quorum, examiners look for the rationale recorded, the escalation made, and where those decisions were subsequently ratified, with board escalation traceable into a board pack	"Pick any meeting in the period. Show me attendance against the charter's quorum, and where quorum was short, the rationale recorded and where those decisions were ratified."
1-3-1 Policies and procedures documented and approved ECC 1-3-1 · CSF 3.1.3 · ITGF 3.1.4	Policy register: version, approving authority, approval date, next review date, plus staff acknowledgement or controlled-distribution records	Governance lead	Approved review interval + event-driven on material regulatory, risk or operating change	Register plus approval minutes; an undated policy cannot evidence when it took effect or which version staff acknowledged. CSF 3.1.3 requires the policy to be defined, approved and communicated with supporting procedures (3.1.3.3(b)); the ITGF 3.1.4 lifecycle supplies the review-cadence detail examiners ask for on this row.	"Pick any policy from the register. Show me its approval record, its next-review date, and what flags it when that date passes."
1-5-1 Risk-management methodology approved	Approved methodology with impact/likelihood scales and risk-appetite thresholds;	Head of Technology Risk	Quarterly committee	The register extract and the minutes must agree. A	"Point to a risk the committee rejected or re-

Control area	Artifact an examination requests	Owner	Cadence	Form examiners accept	Common examiner challenge
ECC 1-5-1 · CSF 3.2.1 · ITGF 3.2.1	register extract with owners, treatments, due dates; committee minutes showing risks actually discussed			register nobody discusses is a spreadsheet, not a process	scored. If none, who is challenging the first line?"
1-7-1 Compliance with nationally approved international commitments ECC 1-7-1 · CSF 3.2.2 · ITGF 3.1.6	Regulatory-obligations register mapped to internal controls and owners (the ITGF names it outright as an up-to-date log of legal, regulatory and contractual requirements with impact and required actions), the latest compliance assessment against it, and the remediation tracker for identified gaps	Head of Compliance + Legal	Continuous monitoring + event-driven updates + defined completeness review	Entries dated to when the obligation took effect, not when the register was tidied, each with a named owner and the document version that changed as a result. On the CSF side, 3.2.2 covers regulatory compliance generally but does not name nationally approved international commitments, so the ITGF update obligation still carries most of the SAMA-side evidence for this row	"Take an obligation that came into force during the period. Show me its register entry, the impact assessment, and the document version that changed as a result."
1-8-1 Periodic internal cybersecurity review ECC 1-8-1 · CSF 3.2.4	Approved annual review plan, control self-assessment workpapers with the evidence behind each maturity rating, and a findings log with remediation status and re-test results. Add the KPI catalogue with targets and thresholds, the deviation analysis, the reporting pack to senior management and the ITSC, and the completed SAMA self-assessment questionnaire	Cybersecurity governance lead	Annual review + quarterly KPIs	A rating is only as good as the workpaper behind it: sampled evidence, tester, date. The ITGF names no cybersecurity self-review subdomain, so the CSF review obligation plus the framework's own self-assessment questionnaire are what examiners test against	"Pick a domain rated at the same level as last cycle. Show me the evidence re-tested this time, and what would have to be true for that rating to move down."
1-8-2 Independent cybersecurity audit	Cybersecurity-scoped audit plan and report by an independent function,	Head of Internal Audit	Per audit plan	Closure evidence that addresses the root cause and	"Choose a closed finding from the tracker. Show me

Control area	Artifact an examination requests	Owner	Cadence	Form examiners accept	Common examiner challenge
ECC 1-8-2 · CSF 3.2.5 · ITGF 3.1.7	evidence of auditor independence and conflict-of-interest handling, findings tracker with closure evidence			shows the control operating, not only that a document changed, with the retest or validation recorded against the finding	the closure evidence, how it addresses the root cause, and what testing confirmed the control now operates."
1-9-1 Personnel cybersecurity requirements defined ECC 1-9-1 · CSF 3.3.1 · ITGF 3.1.8	HR procedure showing the security steps at joiner, mover and leaver stages, sample onboarding and termination checklists, and access-revocation records timed against leaving dates. On the ITGF line, the critical-IT-role register, evidence no critical role rests on one individual, the required-certification list against certifications held, and the IT succession plan agreed with HR	HR + IAM lead	Per joiner/mover/leaver + annual review	Revocation timestamps measured against the HR leaving date, not the date the ticket was raised. The gap between the two is the control. Checklists need the name, the date, and a signature from someone other than the leaver	"Take a sample of leavers I choose. How long from last working day to account disable, and who measures that interval?"
1-9-3 Pre-employment requirements (NDA clauses, screening/vetting) ECC 1-9-3 · CSF 3.3.1	Signed confidentiality and non-disclosure undertakings on file, background-screening records for staff and contractors in technology and security roles, and employment contracts evidencing the security clauses	HR + vendor mgmt (contractors)	Pre-hire + contractor onboarding/renewal	Screening dated before the start date and reaching contractors and outsourced staff, not employees only. An undated NDA, or one signed after access was granted, evidences paperwork rather than control. The ITGF states no screening or staff-NDA requirement, so the CSF human-resources subdomain is the only SAMA anchor	"Pick a contractor with privileged access to a critical system. Show me the screening record dated before access was granted, and who accepted it."
1-10-1 Awareness program developed and approved	Approved awareness plan or calendar, completion statistics by population including senior management and third	Awareness lead (under CISO)	Annual plan + per campaign	Completion broken out by population, with senior management and	"Show me completion for senior management and for contractors as

Control area	Artifact an examination requests	Owner	Cadence	Form examiners accept	Common examiner challenge
ECC 1-10-1 · CSF 3.1.6 · ITGF 3.1.8	parties, phishing-simulation results with the follow-up training given, and dated copies of the materials used. On the ITGF line, the approved annual IT training plan with its periodic review, delivery records for existing and new IT staff and contractors, and specialist training for critical-role, development and risk-assessment staff			contractors shown separately. An aggregate percentage hides exactly the groups examiners ask about. Phishing results need the action taken on repeat clickers, not only the click rate	separate populations, and for repeat clickers in the last simulation, the follow-up action recorded."
DEFENSE: 21 CONTROL AREAS					
2-1-1 Asset-management requirements defined ECC 2-1-1 · CSF 3.3.3 · ITGF 3.3.1	Asset inventory or CMDB extract showing owner, classification, location and criticality; reconciliation between the inventory and network-discovery output; and the lifecycle procedure from acquisition to disposal. The ITGF is unusually prescriptive here, so the register is tested against the seventeen fields 3.3.1 enumerates: PCI scope flag, acceptable downtime aligned to the BCM impact analysis, financial impact per hour of downtime among them	Asset/config manager + asset owners	Yearly refresh + on every add or removal	The reconciliation is the evidence, not the inventory: a discovery scan run against the register with every unmatched item explained. Accountability must be traceable to a named person or a defined role. A generic department with nobody accountable behind it does not evidence ownership	"Run your inventory-to-discovery reconciliation for a date I pick. For anything unmatched, tell me the accountable owner and whether it is in PCI scope."
2-1-3 Acceptable-use policy defined and communicated ECC 2-1-3 · ITGF 3.3.6	Approved acceptable-use policy showing its review date, signed user acknowledgements for a sample of staff and contractors, and evidence of communication to all users. On the ITGF line, the approved network architecture policy carrying the acceptable-use stance, the secure-use rules for specific network resources and services, and the stated	Governance lead + HR	Per policy cycle + on revision	Acknowledgements traceable to the policy version the user actually signed, and a coverage rate that includes contractors. The CSF names no acceptable-use subdomain, so the ITGF network architecture policy carries the row and its acceptable-use	"Take the current policy version. Show me acknowledgement coverage against it for staff and for contractors, and how users were re-acknowledged after the last revision."

Control area	Artifact an examination requests	Owner	Cadence	Form examiners accept	Common examiner challenge
	consequences of non-compliance			clauses are read as the requirement	
2-1-5 Assets classified, labeled, and handled per regulation ECC 2-1-5 · CSF 3.3.3 · ITGF 3.3.1	Approved classification scheme with the handling matrix per level, labelling evidence on a sample of documents, systems and removable media, and data-owner sign-off on the classification of critical repositories. On the ITGF line, asset-owner sign-off on classification and labelling per sampled asset, alignment of that classification with cyber security controls, and controlled secure-disposal records	Data owners + governance lead	At onboarding + annual re-validation	A classification is credible only where the handling matrix visibly changes something: encryption, access, disposal route. Identical handling at every level is a label, not a control	"Pick two assets at different classification levels. Show me what the handling matrix makes technically different between them."
2-2-1 IAM requirements defined ECC 2-2-1 · CSF 3.3.5 · ITGF 3.3.1	Access-control policy and the role-to-entitlement matrix, joiner/mover/leaver request and approval tickets, and periodic user-access review records signed off by system or data owners. On the ITGF line, asset-owner evidence of defining and reviewing access rights per asset, and the documented authorization profile matrix supporting segregation of duties within infrastructure components	IAM lead + system owners	Event-driven on JML + periodic standard-access review + quarterly privileged review	The matrix must reconcile to what the directory actually holds for a sampled role. A policy describing roles the systems never implemented is a document, not an access model. Approval has to come from the resource owner, not the requester's manager alone	"Pick a role from your matrix. Pull its live group memberships in production and reconcile them against the matrix line by line."
2-2-3 Minimum IAM requirements (authentication, MFA, least privilege, PAM, periodic review) ECC 2-2-3 · CSF 3.3.5 · ITGF 3.3.6	Privileged-account inventory with vaulting and session-recording evidence; MFA configuration for remote and privileged access; dated periodic access-review records	IAM lead + app owners	Quarterly reviews	Reviews spaced across the period, each with reviewer, date, and the action taken on exceptions. Four reviews dated in the same week is one review	"Choose a privileged user who left this year. Show me when each entitlement ended, and who signed the removal."
2-3-1 System-protection requirements defined	Approved hardening baselines per platform, anti-malware coverage reconciled	Platform engineering +	Baselines annual + monthly compliance scan	A baseline that has been measured: scan output with	"Take your build standard for one platform. What

Control area	Artifact an examination requests	Owner	Cadence	Form examiners accept	Common examiner challenge
ECC 2-3-1 · CSF 3.3.8 · ITGF 3.3.11	to the asset inventory, and configuration-compliance scan results with approved exceptions. On the ITGF line, the approved minimum baseline security standards for virtual and container components with evidence of application, the CMDB with configuration-item criticality and interrelationships, and the periodic configuration-item verification records	Technology Risk		per-platform pass rates, every deviation either remediated or carrying a dated, approved exception with an expiry. Baselines exist on paper far more often than they exist on hosts	proportion of production hosts pass it today, where does that number come from, and who approves the deviations?"
2-3-3 Minimum system protection (anti-malware, external media, patching, clock sync) ECC 2-3-3 · CSF 3.3.8 · ITGF 3.4.9	Patch-compliance report by severity with aging against the remediation SLA, anti-malware console coverage and signature-currency report, removable-media restriction evidence at both policy and technical level, and the time-synchronisation standard with a sample of configured hosts. On the ITGF line, the cyber security sign-off on patch impact assessments, test-environment evidence before production deployment, patch windows communicated in advance and outside freezing periods, and vendor-feed monitoring records	Infrastructure lead + endpoint team	Monthly cycle + out-of-cycle for critical	Aging measured from patch or advisory release to deployment, not from ticket creation. Coverage must reconcile to the asset register, because the hosts missing an agent are precisely the hosts missing from the console	"Choose a critical patch from the last cycle. Show me its release date, the impact assessment, the test evidence, the change record that deployed it, and how the elapsed time compares with your SLA."
2-4-1 Email-protection requirements defined ECC 2-4-1 · CSF 3.3.8	Email gateway configuration for anti-spam, anti-malware and attachment sandboxing; the sender-authentication records (SPF, DKIM, DMARC) published for the institution's domains; and phishing-report and blocking statistics for the period	Messaging platform owner + SOC	Config annual + monthly statistics	DNS records as actually published and resolvable, with the DMARC policy value visible and its enforcement level a recorded decision rather than a default, and gateway settings evidenced by exported configuration rather than console	"Walk me through your published DMARC posture and its SPF and DKIM alignment. What enforcement level did you settle on, on what rationale, and what happens to mail that fails authentication?"

Control area	Artifact an examination requests	Owner	Cadence	Form examiners accept	Common examiner challenge
				screenshots. The ITGF states no email requirement at all, so the CSF infrastructure-security subdomain is the only SAMA-side anchor	
2-5-1 Network-security requirements defined `ECC 2-5-1 · CSF 3.3.8 · ITGF 3.3.6`	Approved network architecture and topology diagrams showing security zones, the firewall rulebase with business justification per rule and the date of its last review, and the network-segmentation standard. On the ITGF line, the approved network architecture policy itself, a current complete network diagram, and the per-gateway service access rules ensuring only authorised traffic passes	Network architecture lead + CISO	Annual policy + semi-annual rule review	A diagram dated inside the period that matches what the firewalls enforce for a sampled zone pair, and rule justifications naming a business owner and a review date. A rule still justified as "temporary" long after it was raised needs a current owner and rationale	"Take the current network diagram. Show me how it is kept current against the change record, then pick a zone pair with me and demonstrate the deployed rules match it."
2-5-3 Minimum network security (segmentation, secure browsing, wireless, IPS, DNS, DDoS) `ECC 2-5-3 · CSF 3.3.8 · ITGF 3.3.6`	Segmentation and DMZ design evidence with zone-to-zone rule matrices, firewall rule-review reports, IPS and anti-DDoS configuration with tuning records, wireless authentication configuration, and DNS filtering or proxy policy with block-category evidence. On the ITGF line, the two-firewall path to the DMZ, proxy-enforced authenticated outbound browsing, visitor network isolation, active-scanning alert and block at the DMZ perimeter, and the WAF in front of customer-facing applications	Network security lead + SOC	Semi-annual rule review + continuous tuning	Configuration exports plus a tested path, not a design document: segmentation is proven by a blocked connection attempt between two zones, and IPS by signatures in prevent rather than detect mode	"Pick a segment. Tell me whether the IPS there is in blocking or alert-only mode, and show me the last event it acted on."
2-6-1 Mobile/BYOD security requirements defined	Mobile-device-management enrolment report reconciled to the device inventory, the	End-user computing lead + Legal	Continuous enrolment + annual policy review	Enrolment reconciled against people rather than	"If a personal handset carrying corporate mail is

Control area	Artifact an examination requests	Owner	Cadence	Form examiners accept	Common examiner challenge
ECC 2-6-1 · CSF 3.3.10	BYOD policy with signed user consent, and configuration evidence for containerisation, encryption and remote wipe including a sample wipe record			devices (the population that matters is staff with mail on a personal handset), and a wipe capability credible only once you can show it executed. The ITGF addresses neither mobile nor BYOD, so the CSF BYOD subdomain is the only SAMA-side anchor	lost tonight, who wipes it, on whose consent, and where is that consent signed?"
2-7-1 Data-protection requirements defined per legal requirements ECC 2-7-1 · CSF 3.3.3 · ITGF 3.3.1	Data-protection standard tied to each classification level, the DLP rule-set with blocked-event and incident reports, retention and secure-disposal records, and the data inventory or record of processing for personal data. On the ITGF line, the data-privacy entry in the compliance log, retention periods set against legal and regulatory requirements in the backup strategy, and evidence that only sanitized data is used in test environments	Privacy lead / DPO + data owners	Annual standard + monthly DLP review	DLP evidence must show what happened to the blocked events. A monitor-mode rule whose alerts nobody reviews evidences telemetry, not control. Test-data evidence means a masking or sanitisation job record for a named non-production environment	"Does any non-production environment hold live customer data? If so, show me the masking or sanitisation job and when it last ran."
2-8-1 Cryptography requirements defined ECC 2-8-1 · CSF 3.3.9	Approved cryptographic standard listing permitted algorithms, key lengths and prohibited primitives; key-management procedures with custodian assignment and dual-control records; inventories of keys, certificates and algorithms in use with the approved-exception register and certificate-expiry monitoring; and, where the architecture uses hardware key stores,	Key custodians (under CISO)	Annual standard + per crypto-period rotation	Key-ceremony records signed by two named custodians wherever hardware key stores are in use, and a certificate register whose expiries are monitored by something other than a person remembering. Where the standard prohibits a primitive,	"Pick a prohibited primitive from your own standard. Show me the inventory or scan that evidences where it is still in use, and who reviews that."

Control area	Artifact an examination requests	Owner	Cadence	Form examiners accept	Common examiner challenge
	the HSM inventory with its key-ceremony and custodian records			examiners look for the inventory or scan evidencing where it is and is not still in use. The ITGF carries no cryptography or key-management requirement whatsoever, so the CSF Cryptography subdomain stands alone on this row	
2-9-1 Backup-and-recovery requirements defined ECC 2-9-1 · CSF 3.3.8 · ITGF 3.3.10	Backup policy stating RPO/RTO by system tier; success/failure reports for the period; restore-test reports with dates and outcomes; offsite or immutable-copy evidence	Infrastructure lead	Stated job-monitoring frequency + restore-test interval by criticality, aligned with BCM exercises	A restore-test report with a date, a scope, an outcome, and a signature. Backup logs alone prove backups, not recovery	"Pick a tier-1 system from your own policy. When did you last restore it, and how long did it take against the stated RTO?"
2-10-1 Vulnerability-management requirements defined ECC 2-10-1 · CSF 3.3.17 · ITGF 3.4.9	Vulnerability-management procedure with severity-based remediation SLAs, scan reports evidencing coverage of the full asset estate including externally facing systems, and the remediation-aging and exception register with approved compensating controls. On the ITGF line, the periodic scan or inspection records for outdated patches and vulnerabilities, vendor and third-party feed monitoring, and the change records through which remediation was deployed	Vuln management lead + platform owners	Monthly scans + continuous feeds	Coverage reconciled to the asset register, and the scan mode stated: a remediation rate quoted over part of the estate is a scoping statement, and unauthenticated scans understate what is there	"Reconcile your latest scan coverage against the asset register. For anything the scan did not reach, tell me why, and whether it ran authenticated."
2-11-1 Penetration-testing requirements defined ECC 2-11-1 · CSF 3.3.17 · ITGF 3.4.5	Annual penetration-test plan and scope covering internet-facing and critical internal systems, the independent tester's report, retest	CISO + Technology Risk	At least annual + after material change	Scope statement, tester identity and qualifications, and a retest report. Without a retest, a	"Take this year's test scope. Show me how it was set against your critical-systems list, who approved

Control area	Artifact an examination requests	Owner	Cadence	Form examiners accept	Common examiner challenge
	evidence closing high and critical findings, and the tester's independence and qualification records. On the ITGF line, security-testing evidence inside the change record for a sample of changes, the approved test cases including negative scenarios, and the cyber security function's review and approval before CAB submission			remediation ticket's status is the only evidence that anything closed. Exclusions must be named and justified in the plan, not discovered in the report's appendix	each exclusion, and the rationale recorded for it."
2-12-1 Logging-and-monitoring requirements defined ECC 2-12-1 · CSF 3.3.14 · ITGF 3.3.6	Logging standard listing mandatory event sources, event types and retention periods; the SIEM use-case and alert inventory; log-source coverage reconciled to the critical-asset list; and log-integrity protection configuration. On the ITGF line, the centralised log server collecting from all network devices, administrative and login trail configuration, resource-utilisation monitoring, and virtual-machine audit logging covering root and administrative activity	SOC manager + platform owners	Annual standard + quarterly use-case review	The standard must name event types per source, and coverage must be a reconciliation against the critical-asset list rather than a list of what happens to be onboarded. Log integrity is demonstrated (write-once storage, restricted access), not asserted	"Pick a critical database. Show me the privileged and root activity your own standard requires, for a date I choose, and where those events are retained."
2-12-3 Minimum logging (critical assets, privileged/remote access, SIEM, continuous monitoring, 12-month retention) ECC 2-12-3 · CSF 3.3.14 · ITGF 3.3.6	SIEM onboarding list with log-source health report; evidence that logs are retained, integrity-protected and retrievable for the required period, with the documented online-versus-archive split and the retrieval time the institution commits to; monitoring coverage and shift-handover records; sampled alert-to-ticket trail	SOC manager	Continuous + monthly health check	Two or three alerts traced end-to-end from trigger to closure. A dashboard screenshot is a picture, not a trail. Retention is met by retrievability within the stated SLA, not by everything staying live-searchable	"Take your log-source health report for the period. Show me any source that stopped reporting, how long detection took, and the ticket that recorded it."

Control area	Artifact an examination requests	Owner	Cadence	Form examiners accept	Common examiner challenge
2-13-1 Incident-and-threat-management requirements defined ECC 2-13-1 · CSF 3.3.15 · ITGF 3.3.8	IR plan with severity matrix and the regulatory notification timelines; incident-register extract with detection/containment/closure timestamps; post-incident review reports	IR lead	Per incident + annual exercise	The severity matrix must name the regulator-notification triggers and clocks explicitly: "we would notify promptly" is not a timeline	"Take an incident from the register at the severity where notification is triggered. Walk me through who made that decision, when the clock started, and what records it."
2-14-1 Physical-security requirements defined ECC 2-14-1 · CSF 3.3.2 · ITGF 3.3.5	Data-centre access list with periodic recertification, badge-access logs and visitor register for a sample period, CCTV retention configuration, environmental maintenance and test records for power, cooling and fire suppression, and secure media-destruction certificates. On the ITGF line, each of the eight controls 3.3.5 names tested directly, the escorted-visitor logs, and where the data centre is outsourced the documented business case and the defined nature and type of provider access	Data-centre / facilities manager	Quarterly recertification + per maintenance schedule	Badge logs compared against the authorised access list for the same dates, with any entry not on the list explained. CCTV counts only with retention configured and footage retrievable for a date the examiner picks	"Pull the badge log for a date I choose. For every name on it, show me the entry on the approved access list."
2-15-1 Web-application-security requirements defined ECC 2-15-1 · CSF 3.3.6 · ITGF 3.4.4	SDLC procedure showing the security gates and who signs them, the secure-coding standard, pre-go-live application security test results (static, dynamic and where applicable penetration test), WAF configuration and rule-tuning evidence, and the release approval records. The ITGF names two artifacts precisely: the secure code review report, or an independent assurance statement where the institution does not hold the source code, and the WAF in	AppSec lead + dev managers	Per release + annual standard review	The security gate evidenced inside the release record for a sampled release, signed by someone outside the delivery team. A WAF is credible in blocking mode with tuning history; in detection-only mode it is telemetry	"Pick a release from the last quarter. Show me the security testing evidence in its record, the defects it raised, how each was remediated or formally excepted, and who outside the delivery team approved the release."

Control area	Artifact an examination requests	Owner	Cadence	Form examiners accept	Common examiner challenge
	front of customer-facing applications				
RESILIENCE: 2 CONTROL AREAS					
3-1-1 Resilience requirements within BCM defined ECC 3-1-1 · CSF 3.1.3 · ITGF 3.3.2	Business impact analysis covering critical systems with RTO and RPO, approved business-continuity and disaster-recovery plans with approval dates, and evidence that cyber scenarios such as ransomware sit inside the BCM scope. On the ITGF line, the critical-asset interdependency register, the governance model covering interdependencies with service providers and government institutions, BCP test evidence exercising interdependency scenarios, and the resilience measures recorded for critical assets	BCM lead + asset owners	Annual BIA + approved exercise interval + retest after material change or unmet objective	A BIA whose RTOs the technology side has actually agreed to, and an exercise report where a cyber scenario was played rather than listed in the plan's scenario catalogue. On the CSF side, 3.1.3.4(f)(8) only requires cyber security to be reflected in BCM, so the ITGF interdependency requirements and the separate SAMA BCM Framework carry the documented-and-approved part of this row	"Which of your exercises assumed the backups themselves were compromised?"
3-1-3 Minimum resilience requirements (continuity of security systems, incident response plans, DRP) ECC 3-1-3 · CSF 3.3.15 · ITGF 3.3.10	Approved continuity, incident-response and disaster-recovery requirements and plans covering cybersecurity systems, with owners and review dates; exercise reports carrying the recovery evidence and the RTO and RPO actually achieved against target; the dependency map for the cybersecurity tooling itself; and approved exceptions with their remediation retests	BCM lead + CISO, with IT service, infrastructure and application owners	Annual review + scheduled exercises + post-change testing + remediation retests	Plans with owners and review dates, and exercise reports that state achieved against target rather than pass or fail. On the ITGF line examiners also test defined RTOs for the security stack itself. Who defends you while you recover?	"Name a cybersecurity tool you would need during a recovery. What is its own RTO, and where is that written?"
THIRD-PARTY & CLOUD: 4 CONTROL AREAS					
4-1-1 Third-party contract cybersecurity requirements defined	Third-party register with criticality tiering, pre-onboarding due-diligence and	Vendor mgmt + Technology Risk	Pre-onboarding + annual by tier	Tiering that changes what the process demands: identical	"Show me a vendor you rated critical, then show me what your

Control area	Artifact an examination requests	Owner	Cadence	Form examiners accept	Common examiner challenge
ECC 4-1-1 · CSF 3.4.1 · ITGF 3.3.3	security-assessment records, the contract template carrying the security clause set, and ongoing monitoring or SLA review reports. On the ITGF line, the signed SLA itself, the procurement-stage risk assessment, the confidentiality-integrity-availability safeguard clauses, and the periodic review and evaluation of agreed SLA requirements including the escalation process on breach			due diligence for a critical technology provider and a low-impact supplier does not evidence tiering. Clause evidence comes from executed contracts, never from the template	process did differently because of that rating."
4-1-2 Minimum third-party contract clauses (NDA/secure removal, incident communication, policy compliance) ECC 4-1-2 · CSF 3.4.1 · ITGF 3.3.3	A sample of executed contracts evidencing confidentiality, right-to-audit, incident-notification and secure data-return or destruction clauses, plus destruction certificates obtained at contract exit. On the ITGF line, the exit, termination and renewal clauses including escrow where applicable, the framework-compliance clause naming the SAMA CSF, BCM and ITGF, and the onsite-support undertaking with its defined response timeline	Legal / procurement + Technology Risk	Per signature + at renewal	Signed, executed copies with the security schedule attached. A clause library proves drafting, not contracting. Where an arrangement has ended, examiners look for the data-return or destruction certificate, dated and naming what was covered	"Pick a contract that ended or was renewed in the period. Show me the executed security schedule, and where it ended, the data-return or destruction certificate and who verified it."
4-1-3 Outsourcing/managed-services requirements (pre-contract risk assessment, KSA-located managed SOCs) ECC 4-1-3 · CSF 3.4.2 · ITGF 3.3.3	Pre-contract outsourcing risk assessment and business case; regulatory notification or no-objection correspondence where the arrangement is material; agreement clauses on subcontracting and data location; evidence of where the provider and any managed SOC actually operate, with the subcontractor and onward-transfer records; the provider's independent	Vendor mgmt + Technology Risk	Pre-contract + annual review	The risk assessment must be dated before signature. A post-signature assessment evidences paperwork, not diligence. Location is evidenced from the provider's own operating records and the subcontractor chain, not from a	"Take a material outsourcing arrangement. Show me the risk assessment and the signature dates side by side, the regulatory correspondence, and where the service and any managed SOC are physically operated from."

Control area	Artifact an examination requests	Owner	Cadence	Form examiners accept	Common examiner challenge
	assurance report (for example ISAE 3402 or SOC 2) with the institution's review notes; and ongoing service and control reviews			contractual statement alone	
4-2-1 Cloud/hosting cybersecurity requirements defined ECC 4-2-1 · CSF 3.4.3 · ITGF 3.3.5	Cloud-service register recording the data classification hosted in each service, cloud risk assessments and provider due-diligence, data-residency evidence for in-Kingdom workloads, the signed shared-responsibility matrix, configuration-baseline or CSPM reports, and the documented exit and portability plan. On the ITGF line, the documented business case for any outsourced data centre, the defined nature and type of provider access, and evidence of compliance with the SAMA Outsourcing Rules and Cybersecurity Framework the subdomain points to	Cloud platform owner + Technology Risk	Pre-adoption + annual, CSPM continuous	A register reconciled against independent discovery sources rather than self-declaration, since the services nobody declared are the ones that matter. Residency evidenced from the provider's region configuration, and the shared-responsibility matrix signed by both sides rather than downloaded from the vendor's website	"Show me the discovery sources you reconcile the cloud register against (egress, expense and identity-provider records), what the last reconciliation left unmatched, and how those items were closed."