LanGuard

CASE STUDY

GFI LanGuard and Saudi NCA ECC-2:2024: Control mapping

1. In brief

→ **NCA certifies organizations, not products.**
A tool only counts as evidence that Astra has implemented a control.

→ **GFI LanGuard is strongest in vulnerability management (ECC 2-10) and patching (2.3.3.3).**
It performs these activities itself and produces the records an auditor asks for.

→ **Ratings apply to the asset types GFI LanGuard supports (Section 6).**
Every Direct row names what is out of scope.

What we rated: 100 of the 176 items an auditor checks in ECC.
These cover the vulnerability and patch areas plus the related areas where GFI LanGuard data serves as evidence (Section 3).

Results:	Direct 6	Partial 15	Supporting 28	Not covered 27	Organizational 24

→ **GFI LanGuard does not cover:**
Network-device firmware patching, SIEM and log monitoring, multi-factor authentication (MFA) and privileged access management (PAM), segmentation, penetration testing, and blocking (not just detecting) USB media and applications.

→ **Some design facts (Section 6):**

- Each GFI LanGuard installation supports up to 3,000 machines, so 10,000+ endpoints need several installations.
- Connecting GFI LanGuard to GFI AppManager AI or using WAN agents sends data through GFI cloud services, which brings ECC 4-1 and 4-2 into scope.
- The console has no separate user accounts, so GFI LanGuard cannot show which person ran a scan or remediation.

2. NCA and ECC

NCA is the National Cybersecurity Authority,
Saudi Arabia's cybersecurity regulator.

ECC-2:2024 is NCA's baseline control set:
4 domains, 28 subdomains, 108 main controls and 92 subcontrols.

- It is mandatory for government bodies, their affiliated companies, and operators of Critical National Infrastructure.
- All other organizations are "strongly encouraged" to adopt it.

How compliance is checked:
Self-assessment, NCA's compliance tool, and/or field audits. ECC 1-8-2 also requires an independent review.

Numbering:
Main controls use dashes (2-10-3); subcontrols use dots (2.10.3.1).

3. Ratings and selection

Rating	Meaning
Direct	GFI LanGuard performs the activity itself and records it, for the asset types it supports. The row names what is out of scope.
Partial	GFI LanGuard performs part of the activity, or detects the condition. The gap is named.
Supporting	GFI LanGuard supplies evidence. A policy, a person or another tool meets the control.
Not covered	A technical control outside GFI LanGuard's scope.
Organizational	Astra must define, approve, document or train. No tool can do this.

How the 100 items were chosen:

Where a main control only introduces subcontrols, the auditor checks the subcontrols. That gives 108 + 92 − 24 = **176 assessable items.**

Step	ECC areas	Items
Core	2-10 Vulnerability management; 2-3 Systems protection (includes patching)	15
Related	1-5 Risk; 1-6 IT projects; 1-8 Review and audit; 2-1 Assets; 2-2 Identity and access; 2-5 Network; 2-6 Mobile; 2-8 Cryptography; 2-9 Backup; 2-11 Penetration testing; 2-12 Logs and monitoring; 2-13 Incidents	85
Rated		**100**
Not rated: no role for a scanning tool	1-1 to 1-4, 1-7, 1-9, 1-10 (governance, HR, training); 2-4 Email; 2-7 Data protection; 2-14 Physical; 2-15 Web applications; 3-1 Business continuity; 4-1 Third parties; 4-2 Cloud	76

Email (2-4) can be addressed with GFI MailEssentials AI and GFI Archiver AI. 4-1 and 4-2 come into scope if GFI AppManager AI or WAN agents are used.

Result by area:

Area	Items	Direct	Partial	Supporting	Not covered	Organizational
2-10 Vulnerability management	8	5	1	1	0	1
2-3 Systems protection	7	0	4	2	0	1
1-5 Risk	7	0	0	2	2	3
1-6 IT projects	9	1	2	1	3	2
1-8 Review and audit	3	0	0	2	0	1
2-1 Assets	6	0	3	1	0	2
2-2 Identity and access	8	0	1	4	2	1

Result by area:

Area	Items	Direct	Partial	Supporting	Not covered	Organizational
2-5 Network	12	0	2	2	7	1
2-6 Mobile	7	0	0	3	2	2
2-8 Cryptography	6	0	0	3	2	1
2-9 Backup	6	0	0	3	2	1
2-11 Penetration testing	5	0	0	0	4	1
2-12 Logs and monitoring	8	0	2	3	2	1
2-13 Incidents	8	0	0	1	1	6
Total	**100**	**6**	**15**	**28**	**27**	**24**

In the core areas, 10 of 15 items are Direct or Partial. Three are Supporting and two are Organizational.

4. Mapping

To produce any report named below: open **Reports**, select the computer or group, select the report, then click **Generate report**. To schedule a report: **Reports > Actions > New scheduled report**.

4.1 Direct

Control	How GFI LanGuard does it	Out of scope	See it
2.10.3.1 Periodic vulnerability assessment	Scheduled agentless scans of IP ranges, computer lists or AD organizational units. Windows agents also audit their own machine, daily by default. Identifies 60,000+ vulnerabilities using OVAL definitions, cross-referenced with NVD for severity ratings. Definitions are updated twice a week.	Web applications, OT devices, cloud services	**Configuration > Scheduled Scans; Dashboard > computer > Properties > Agent Status; Scan History** report
2.10.3.2 Classify by severity	Each finding is rated High, Medium or Low using NVD CVSS scores.	Findings from other scanners	**Dashboard > Vulnerabilities; Vulnerability Status** report
2.10.3.3 Remediate by severity and risk	Deploys patches, removes unauthorized applications and runs scripts; can run automatically after a scan.	GFI LanGuard does not remediate vulnerabilities that have no associated patch (KB 122677).	**Remediate > Remediation Jobs; Remediation History** report
2.10.3.4 Patch after verifying in non-production	Patches can be approved one at a time once tested; Microsoft updates are not approved for automatic deployment by default. Always test patches in a test environment before deployment. A rescan confirms each patch is installed.	The test environment and test sign-off are Astra's records.	**Configuration > Software Updates > Patch Auto-Deployment > Manual approval**

Control	How GFI LanGuard does it	Out of scope	See it
2.10.3.5 Trusted vulnerability sources	Vulnerability and patch definitions update automatically from GFI; vulnerability definitions are updated twice a week.	NCA and vendor advisories, which Astra subscribes to	**Configuration > Program Updates**
1.6.2.1 Vulnerability assessment and remediation in projects	Scan before go-live, fix, rescan.	As 2.10.3.3	**Vulnerability Status** before and after the change

4.2 Partial

Control	How GFI LanGuard does it, and the gap	See it
2.3.3.3 Patch management	Patches Windows, Linux and macOS, plus third-party applications, with approval and rollback. **Gap:** no network-device firmware, so Astra's Ruckus and Cisco estate needs the vendors' tools.	**Remediation Center > Deploy Software Updates; Patching Status**
2-10-2, 2-3-2 Implement vulnerability management and system protection	Runs Astra's scan, patch and approval schedules. **Gap:** policy and non-GFI LanGuard assets.	**Scheduled scans; Patching Status**
2.3.3.1 Malware protection	Checks antivirus status, and can start scans where antivirus is installed. **Gap:** it is not an anti-malware engine.	**Antivirus Applications**
2.3.3.2 Restrict external media	Lists USB devices and flags named ones. **Gap:** detects; does not block.	**USB Devices**
2-1-2 Implement asset management	Hardware and software inventory; AD sync. **Gap:** assets it cannot reach.	**Hardware Audit, Software Audit**
2-1-4 Implement acceptable use	Detects, and can uninstall, unauthorized applications; flags blacklisted USB devices. **Gap:** software and devices only.	**Unauthorized Applications, USB Devices**
2-1-5 Classify assets	Owner and criticality recorded as attributes. **Gap:** Astra approves the classification.	**Computer > Properties > Attributes**
1.6.2.2, 1.6.3.5 Review configuration before launch	Compares targets with a reference computer Astra chooses. **Gap:** sign-off is Astra's.	**Baseline Comparison**
2.2.3.5 Review access rights	Account and group changes between audits. **Gap:** Windows only; the decision is a person's.	**Network Security History**
2.5.3.4 Wireless security	Lists wireless adapters and can alert on them. **Gap:** does not assess wireless encryption.	**Scanning Profile Editor > Devices**
2.5.3.5 Restrict ports and services	Reports open ports, services and shares. **Gap:** does not restrict them.	**Open Ports, Services**
2.12.3.1, 2.12.3.2 Turn on security event logs	Reads and pushes Windows audit policy. **Gap:** Windows only.	**Scan Results Overview > right-click the computer > Enable auditing on**

4.3 Supporting

Control	How GFI LanGuard supports it	See it
2-10-4 Review vulnerability management	Trend reports support the review.	**Vulnerability Status trend**
2.3.3.4 Clock synchronization	Records each target's time; does not synchronize clocks.	**Scan result > Remote TOD**
1.5.3.2, 1.5.3.4 Risk assessment before major changes and new services	Severity, missing patches and open ports feed Astra's risk method.	**Network Security Overview**
1.6.3.3 Security testing of software	Scan results are one input to Astra's testing.	**Vulnerability Status**
1-8-1, 1-8-2 Internal and independent review	Scheduled, repeatable evidence.	**Scan History, Network Security History**
2-1-6 Review assets	New devices since the last audit, and change history.	**New Devices; Dashboard > History**
2.2.3.1 Password authentication	Audits the Windows password policy.	**Scan result > Password Policy**
2.2.3.3 Least privilege	Lists users, groups and shares, including Administrators.	**Groups and Users, Open Shares**
2.6.3.2 Restrict mobile devices	Windows laptops with an agent keep auditing themselves while off the company network and send the results when they reconnect. Phones and tablets are listed from Exchange, Office 365, Google Apps or Apple Profile Manager; GFI LanGuard reads the list from that source and does not scan the devices.	**Mobile Devices Audit**
2.8.3.3 Encryption	Detects whether disk-encryption software is installed.	**Dashboard > Software** (Disk Encryption category); **Software Audit** report
2.9.3.1 Backups of critical assets	Detects backup software; does not test restores.	**Software Audit** (Backup)
2.12.3.5 Retain security event logs for at least 12 months	Scan history can be kept for more than 12 months, subject to database space. It gives Astra supporting evidence of each machine's vulnerability and patch state over time. **Gap:** scan history is not a security event log, and keeping event logs needs a SIEM.	**Configuration > Database Maintenance Options > Database backend settings > Retention**; Scan History report
2-13-2 Implement incident management	Inventory, patch status and fast push of a fix.	**Remediation Center > Deploy Custom Software**
2-2-2, 2-2-4, 2-3-4, 2-5-2, 2-5-4, 2-6-2, 2-6-4, 2-8-2, 2-8-4, 2-9-2, 2-9-4, 2-12-2, 2-12-4 Implement and review each area	The reports above, scheduled, evidence the technical part.	**Same reports, on a schedule**

4.4 Not covered

Control	Why, and what covers it
1.5.3.1 Risk assessment at a project's start	Nothing to scan before the assets exist. Astra's risk process.
1.5.3.3 Third-party risk	Supplier risk process
1.6.3.1, 1.6.3.2, 1.6.3.4 Secure development	Secure development lifecycle with code and dependency testing
2.2.3.2 MFA	Identity provider with MFA
2.2.3.4 Privileged access management	A PAM vault. GFI LanGuard's own service account needs this treatment (Section 6).
2.5.3.1–2.5.3.3, 2.5.3.6–2.5.3.9 Segmentation, firewalls, DNS, intrusion prevention (IPS)	Firewalls, IPS and DNS security. GFI LanGuard scans across segments; it does not separate them.
2.6.3.1, 2.6.3.3 Mobile encryption and wipe	A mobile device management (MDM) service
2.8.3.1, 2.8.3.2 Crypto standards; key management	Key-management and encryption tooling
2.9.3.2, 2.9.3.3 Recovery; restore tests	Backup and recovery platform
2-11-2, 2-11-4, 2.11.3.1, 2.11.3.2 Penetration testing	A qualified testing team. A vulnerability scan is not a penetration test.
2.12.3.3, 2.12.3.4 SIEM and monitoring	A SIEM with at least 12 months' retention
2.13.3.5 Threat intelligence	A threat-intelligence process or service. A vulnerability feed is not threat intelligence.

4.5 Organizational

Control	Astra must
1-5-1, 1-6-1, 2-1-1, 2-2-1, 2-3-1, 2-5-1, 2-6-1, 2-8-1, 2-9-1, 2-10-1, 2-11-1, 2-12-1, 2-13-1	Define and approve each area's requirements
1-5-2, 1-5-4, 1-6-4, 1-8-3	Run and review the risk method and project requirements; report audit results to the committee
2-1-3	Define the acceptable-use policy for assets
2.6.3.4	Train mobile-device users
2-13-4, 2.13.3.1–2.13.3.4	Incident plans, classification, reporting to NCA, alert sharing

5. Evidence pack

Schedule these reports and file each one under its control ID.

Report	Controls	Frequency
Vulnerability Status, Network Security Overview	2.10.3.1, 2.10.3.2, 1.6.2.1	Monthly, and around each change
Patching Status, Missing Security Updates	2.3.3.3, 2-3-2, 2-10-2	Monthly
Remediation History (each approved deployment)	2.10.3.3, 2.10.3.4	Each patch cycle
Scan History, plus a screenshot of the scan schedule and program-update settings	2.10.3.1, 2.10.3.5	Quarterly
Hardware Audit, Software Audit, New Devices, Network Security History	2-1-2, 2-1-5, 2-1-6	Monthly
Baseline Comparison	1.6.2.2, 1.6.3.5	Quarterly, and before go-live
USB Devices, Antivirus Applications, Groups and Users, Open Ports	2.2.3.3, 2.3.3.1, 2.3.3.2, 2.5.3.5	Quarterly

GFI LanGuard has no NCA report template. Its ISO 27001/27002 reports can serve as a cross-reference.

Evidence the auditor is most likely to ask for, for the Direct items:

- 2.10.3.1: a scope statement listing what GFI LanGuard scans, and how web applications and cloud services are scanned.
- 2.10.3.3: how vulnerabilities without a patch are handled.
- 2.10.3.4: Astra's test record alongside the Remediation History.

6. Design facts

What GFI LanGuard covers, by asset type:

Asset type	Discover and scan	Patch
Windows clients and servers	Yes	Yes: Microsoft and third-party applications
Linux	Yes	Yes, over SSH through each machine's own package manager. Needs internet access to the distribution's repositories.
macOS	Yes	Yes, over SSH using macOS's built-in update tools. Patches come from the GFI LanGuard server or a relay, so internet access is not required.
Routers, switches, printers	Discovered and assessed	No firmware patching
Phones and tablets	Listed from Exchange, Office 365, Google Apps or Apple Profile Manager; not scanned directly	No: GFI LanGuard has no remediation for mobile devices (KB 122388).

Asset type	Discover and scan	Patch
OT controllers (PLC, RTU, SIS)	Not covered	No
Web applications, cloud services	Not covered	No

1. **Scale:** each GFI LanGuard installation supports up to 3,000 machines (KB 122363).
   - 10,000+ endpoints therefore need several installations.
   - For one view across installations, GFI LanGuard connects to GFI AppManager AI, GFI's cloud console, with no additional license. It shows vulnerability and patch data from each installation (see point 3 on cloud data). Scans and patches can also be started from GFI AppManager AI, with fewer options than the console. If cloud use is not acceptable, Central Management Server is the on-premises option, but it "is used only for reporting."
2. **Multiple sites:** place a relay agent at each site, so each patch is downloaded once.
3. **Cloud data paths (ECC 4-1 and 4-2):** two optional features send data through GFI cloud services. If Astra uses neither, scan results are stored in Astra's own database.
   - **GFI AppManager:** since 12.15, vulnerability and patch data appears in the GFI AppManager AI console.
   - **WAN agents:** these talk to the console "using AWS" on outbound ports 443, 8443 and 8883, with a tenant ID issued by GFI.
4. **No console user accounts:** the console has no feature for adding separate user accounts (KB 122322). It runs under the Attendant service account. GFI LanGuard cannot show which person ran a scan or remediation.
   - The service account holds administrator rights on every target, so treat the GFI LanGuard server as a privileged system under 2.2.3.4.
5. **Retention:** scan history can be kept for more than 12 months, subject to database space (Configuration > Database Maintenance Options > Database backend settings > Retention). This is separate from event-log retention, which is a SIEM function.

7. Sources

NCA:

ECC-2:2024 nca.gov.sa

GFI product:

GFI LanGuard product page Releases 12.15–12.17 GFI AppManager integration CMS reports
Overview and 3,000-machine limit How GFI LanGuard works and CMS WAN agents via AWS
Configuration overview (CMS reporting only; no mobile remediation) No separate console user accounts

Scanning:

Scheduled scans Agent scan schedule Activity Monitor Severity via CVSS Definition updates
Vulnerability databases (OVAL, NVD) Software audit categories Device scanning options Mobile devices
Evaluation guide (agents offline) Attributes AD sync History view Audit policies

Remediation:

Remediation Center Remediation jobs Patch auto-deployment Auto-remediation notes
No fix without a patch Linux and macOS Malware protection Relay agents

Reporting and data:

Default reports Generating reports Scheduling reports Database and retention

Copyright © GFI USA, LLC, All rights reserved.