

GOVERNANCE DOCS

NCA Essential Cybersecurity Controls

Gap Assessment Report

Saudi National Cybersecurity Authority Essential Cybersecurity Controls (ECC-2:2024)

Al Wadi Health Services (sample)

Cybersecurity for the hospital group's IT and medical device networks across three hospitals.

ASSESSED	25 September 2026
EDITION	ECC-2:2024
IN SCOPE	44 requirements, 42 applicable
PROFILE	Healthcare and life sciences · 250 to 999 people · National Cybersecurity Authority (NCA)
PREPARED BY	Governance Docs

CONTENTS

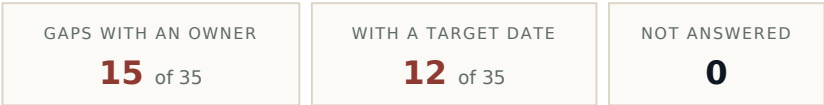
1	Executive summary
2	Readiness by area and where the next points come from
3	Remediation plan
A	About this report

Confidential. Prepared for Al Wadi Health Services (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Al Wadi Health Services (sample) stands against NCA ECC



STATUS OF EVERY REQUIREMENT



WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 56.0% against NCA ECC across 42 applicable controls. 7 of them are implemented and evidenced.
- Most open gaps: 2 - Cybersecurity Defence, with 13 at 38%. Strongest area: Scope and applicability at 92%.
- 13 controls are operating but not evidenced. Collecting their records alone lifts the score to 63.7% (+7.7 points), the cheapest gain available.
- 10 gaps are high priority (not started or only planned); 6 of them are in 2 - Cybersecurity Defence.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	Put an owner and date against the 6 high-priority gaps in 2 - Cybersecurity Defence	Compliance Lead	Policy – Asset Management (Template)
2	MEDIUM	Adopt and tailor the Policy - Corporate Cybersecurity (Template), which closes 2 open gaps	To assign	Policy – Corporate Cybersecurity (Template)
3	LOW	Evidence the 13 controls that already operate (+7.7 points)	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

With an overall score of 56% and 35 open gaps, your priority is establishing foundational governance and core defence controls.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

The organization's self-assessment under the NCA Essential Cybersecurity Controls shows readiness level 2 of 4 with a score of 56%. The main exposure stems from 10 high priority gaps in risk management, asset protection, and operational resilience. Meeting the expectations of the National Cybersecurity Authority (NCA) requires leadership to designate accountability, allocate remediation resources, and mandate that all 35 open gaps receive assigned owners and target delivery dates.

WHERE YOU STAND

Your self-assessment against the NCA Essential Cybersecurity Controls shows an overall score of 56% and places you at readiness level 2 of 4, defined as Developing. Out of 42 applicable requirements, you recorded 35 open gaps, including 10 high priority gaps. Only 15 gaps have an assigned owner and 12 gaps have a target date. Control areas show uneven progress: Scope and applicability scored 91.7%, while Cybersecurity Resilience scored 25% and Cybersecurity Defence scored 38.5%. Currently, 7 requirements are not started and 13 are implemented without formal evidence.

WHAT IT MEANS FOR THE ORGANIZATION

The results indicate that while technical safeguards exist across parts of the environment, formal governance and operational documentation lag behind. Having 13 requirements marked as implemented but not evidenced exposes the organization during regulatory scrutiny by the National Cybersecurity Authority (NCA). Because 10 high priority gaps remain open, critical capabilities such as risk management, asset management, and access controls lack formal operational backing. Gaps without assigned owners or completion dates increase operational uncertainty and prevent repeatable practices across teams.

WHERE TO FOCUS FIRST

You should focus first on resolving the 10 high priority gaps that have not started or are merely planned. Immediate attention belongs to Risk management, Asset management, and Identity and access management within Cybersecurity Governance and Cybersecurity Defence. You should also gather evidence for the 13 requirements where controls already function, which raises the score from 56% to 63.7%. Assigning distinct owners and target dates to all 35 open gaps ensures accountable execution across upcoming operational milestones.

PRIORITIES

PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1 Establish the cybersecurity risk management framework 1-5 Risk management	Risk management is not started and represents a high priority gap under Cybersecurity Governance. Unmanaged cyber risks leave executive decision-makers without visibility into operational vulnerabilities.	Approve and adapt the cybersecurity risk management policy and register templates.	Policy - Cybersecurity Risk Management (Template) NCA Cybersecurity Toolkit	30 DAYS
2 Define governance structures and operational responsibilities 1-4 Roles and responsibilities · 1-2 Cybersecurity management	Roles and responsibilities remains in a planned status while only 15 gaps have an assigned owner. Formal governance structures are needed to steer cross-departmental remediation.	Adopt the cybersecurity roles matrix and charter the steering committee.	Cybersecurity Roles and Responsibilities (Template) NCA Cybersecurity Toolkit	30 DAYS
3 Formalize asset management and access control standards 2-1 Asset management · 2-2 Identity and access management	Asset management and Identity and access management are both unstarted high priority gaps in Cybersecurity Defence. Weak visibility and access governance expose core infrastructure to unauthorized changes and breach risks.	Draft the asset classification standard and review privileged access rules.	Policy - Asset Management (Template) NCA Cybersecurity Toolkit	60 DAYS
4 Strengthen business continuity resilience and backup processes 3-1 Resilience aspects of business continuity · 2-9 Backup and recovery management	Cybersecurity Resilience scored 25%, with resilience aspects of business continuity and backup management not started. Service interruptions cannot be mitigated without validated recovery policies.	Review backup schedules and initiate the business continuity policy draft.	Policy - Cybersecurity Business Continuity (Template) NCA Cybersecurity Toolkit	60 DAYS
5 Compile control evidence and formalize remediation tracking RP.2 Evidence maintained · RP.4 Remediation plan	Currently 13 requirements are implemented without evidence, leaving substantial progress unverified for supervisory reviews. Documenting evidence immediately lifts assessment scores.	Assemble operational evidence files and publish the remediation roadmap.	Cybersecurity Strategy and Roadmap (Template) NCA Cybersecurity Toolkit	90 DAYS

30 / 60 / 90-DAY ROADMAP**FIRST 30 DAYS**

- Assign formal owners and target completion dates to all 35 open gaps.
- Adopt the risk management policy and register templates to establish baseline risk assessments.
- Charter the steering committee and finalize defined roles and responsibilities across business units.

DAYS 31 TO 60

- Implement asset management standards and establish verified identity and access management controls.
- Deploy cybersecurity business continuity procedures and validate data backup recovery testing standards.
- Address mobile device security policies and define cloud cybersecurity control standards.

DAYS 61 TO 90

- Gather and catalog audit evidence for the 13 controls currently running without documentation.
- Complete testing for incident management and web application security requirements.
- Publish key performance indicator reports and update the formal remediation roadmap for leadership.

Maturity across the standard

Each bar shows how the requirements in one area break down by status, weakest on the left. The score is the average across applicable requirements; the chips count open gaps by priority.

AREAS	STATUS MIX	SCORE	GAPS H · M · L
Scope and applicability		92%	
1 - Cybersecurity Governance		50%	
2 - Cybersecurity Defence		38%	
3 - Cybersecurity Resilience		25%	
4 - Third-Party and Cloud Computing		63%	
Other NCA control sets		75%	
Assessment and reporting		63%	

■ Not started
 ■ Planned
 ■ Partially implemented
 ■ Implemented, not evidenced
 ■ Implemented and evidenced
 ■ Not applicable

WHERE THE NEXT POINTS COME FROM

The score after each kind of work, cheapest first. Gold is what that step adds.

Today		56.0%
Evidence what already runs 13 requirements		63.7% +7.7
Finish what is partly in place 12 requirements		78.0% +14.3
Implement what is planned 3 requirements		83.3% +5.3
Start what has not begun 7 requirements		100.0% +16.7

DOCUMENTS THAT CLOSE THE MOST GAPS

Each bar counts the open gaps that name the document as the way to close them.

Policy – Corporate Cybersecurity (Template)		2
Policy – Human Resources (Template)		2
Cybersecurity Roles and Responsibilities (Template)		2
Cybersecurity Strategy and Roadmap (Template)		2
Procedure – Cybersecurity Document Development (Template)		2
Policy – Compliance with Cybersecurity Legislation and Regulations (Template)		2

All of these are in the NCA Cybersecurity Toolkit (86 documents).

Every open gap, grouped by what has to happen next

Work from the top. Requirements not yet started or only planned are the ones a certification auditor reaches first; the last group already operates and needs only its records.

HIGH Not started · 7

Start from a documented baseline: adopt and tailor the document named below, then put it into operation.

Ref	Requirement	Area	Owner · target	Closes it
1-5	Risk management	1	Risk Manager 4 Feb 2027	Policy – Cybersecurity Risk Management (Template) · Procedure – Cybersecurity Risk Management (Template) +1 more
2-1	Asset management	2	Compliance Lead	Policy – Asset Management (Template) · Standard – Asset Management (Template) +1 more
2-2	Identity and access management	2	To assign	Policy – Identity and Access Management (Template) · Standard – Identity and Access Management (Template) +1 more
2-8	Cryptography	2	To assign	Policy – Cryptography (Template) · Standard – Cryptography (Template) +1 more
2-9	Backup and recovery management	2	IT Manager 29 Oct 2026	Policy – Backup and Recovery (Template) · Standard – Backup and Recovery (Template)
2-14	Physical security	2	Compliance Lead 7 Jan 2027	Policy – Physical Security (Template) · Standard – Physical Security (Template)
3-1	Resilience aspects of business continuity	3	Compliance Lead 12 Nov 2026	Policy – Cybersecurity Business Continuity (Template)

HIGH Planned · 3

Move from plan to implementation. Assign an owner and a date, then put the control into operation.

Ref	Requirement	Area	Owner · target	Closes it
1-4	Roles and responsibilities	1	IT Manager 7 Jan 2027	Cybersecurity Roles and Responsibilities (Template)
2-6	Mobile device security	2	IT Manager 10 Dec 2026	Policy – Workstations, Mobile Devices and BYOD Security (Template) · Standard – Mobile Device Security (Template)

EX.1	Cloud Cybersecurity Controls	Other NCA control sets	Risk Manager 21 Jan 2027	Policy – Cloud Computing and Hosting Cybersecurity (Template)
-------------	------------------------------	------------------------	-----------------------------	---

MEDIUM Partially implemented · 12

Extend the existing approach to the whole scope and apply it consistently, then evidence it.

Ref	Requirement	Area	Owner · target	Closes it
1-2	Cybersecurity management	1	To assign	Cybersecurity Steering Committee Regulating Document (Template) · Cybersecurity Organizational Structure (Template)
1-3	Policies and procedures	1	Compliance Lead 29 Oct 2026	Policy – Corporate Cybersecurity (Template) · Procedure – Cybersecurity Document Development (Template)
1-6	Cybersecurity in IT projects	1	To assign	Checklist – Cybersecurity Requirements in IT Projects and Change Management (Template)
1-8	Periodic review and audit	1	Risk Manager 24 Dec 2026	Policy – Cybersecurity Review and Audit (Template) · Procedure – Cybersecurity Audit (Template) +2 more
1-9	Cybersecurity in human resources	1	Operations Manager	Policy – Human Resources (Template) · Form – Confidentiality Agreement (Template) +1 more
2-13	Incident and threat management	2	HR Manager 24 Dec 2026	Policy – Cybersecurity Incident and Threat Management (Template) · Standard – Advanced Persistent Threat (APT) (Template)
2-15	Web application security	2	Operations Manager	Policy – Web Application Protection (Template) · Standard – Web Application Protection (Template) +1 more
3-1b	Continuity testing	3	To assign	Policy – Cybersecurity Business Continuity (Template) · Standard – Backup and Recovery (Template)
4-1	Third-party cybersecurity	4	Risk Manager 7 Jan 2027	Policy – Third-Party Cybersecurity (Template)
RP.2	Evidence maintained	Assessment and reporting	To assign	Procedure – Cybersecurity Document Development (Template)
RP.3	Performance reporting	Assessment and reporting	Compliance Lead 4 Feb 2027	Report – Key Performance Indicator Report (Template)

RP.4	Remediation plan	Assessment and reporting	To assign	Cybersecurity Strategy and Roadmap (Template) · Register – Cybersecurity Audit Plan (Template)
-------------	------------------	--------------------------	-----------	--

LOW Implemented, not evidenced · 13

Collect and file evidence an auditor can sample. The control is operating; what is missing is the record of it.

Ref	Requirement	Area	Owner · target	Closes it
SC.2	Version in use	Scope and applicability	To assign	Policy – Corporate Cybersecurity (Template)
SC.5	Saudi cybersecurity workforce	Scope and applicability	To assign	Policy – Human Resources (Template) · Cybersecurity Roles and Responsibilities (Template)
1-1	Cybersecurity strategy	1	To assign	Cybersecurity Strategy and Roadmap (Template)
1-7	Compliance with legislation and regulations	1	To assign	Policy – Compliance with Cybersecurity Legislation and Regulations (Template)
1-10	Awareness and training	1	To assign	Program – Cybersecurity Awareness Program (Template)
2-3	Information system and processing facilities protection	2	To assign	Standard – Secure Configuration and Hardening (Template) · Standard – Endpoint Detection and Response (EDR) (Template) +1 more
2-4	Email protection	2	To assign	Policy – Email Security (Template) · Standard – Email Protection (Template)
2-5	Network security management	2	To assign	Policy – Network Security (Template) · Standard – Network Security (Template) +2 more
2-11	Penetration testing	2	To assign	Policy – Penetration Testing (Template) · Standard – Penetration Testing (Template)
2-12	Event logs and monitoring	2	To assign	Policy – Cybersecurity Event Logging and Monitoring Management (Template) · Standard – Cybersecurity Event Logging and Monitoring Management (Template)
4-2	Cloud computing and hosting	4	To assign	Policy – Cloud Computing and Hosting Cybersecurity (Template)
EX.2	Critical Systems Cybersecurity Controls	Other NCA control sets	To assign	Policy – Compliance with Cybersecurity Legislation and Regulations (Template)
EX.5	Telework and social media controls	Other NCA control sets	To assign	Policy – Workstations, Mobile Devices and BYOD Security (Template) · Standard – Social Media Security (Template)

How it was scored

STATUS WEIGHTS

Status	Weight	Meaning
■ Not started	0.00	No policy, process or activity exists for this requirement.
■ Planned	0.25	Approach agreed and scheduled, but nothing is in place yet.
■ Partially implemented	0.50	In place for part of the scope, or inconsistently applied.
■ Implemented, not evidenced	0.75	Operating as intended, but you could not prove it to an auditor today.
■ Implemented and evidenced	1.00	Operating as intended, with records an auditor can sample.
■ Not applicable	—	A justified exclusion. Removed from the score - record why in your notes.

READINESS LEVELS

1 • Initial (0%+)

Most requirements are not yet in place. Build the foundations before thinking about an audit.

2 • Developing (40%+)

The programme is under way, with material gaps an auditor would find.

3 • Established (65%+)

Most controls operate. Remaining work is closing specific gaps and evidencing what runs.

4 • Audit-ready (85%+)

Controls operate and are evidenced. Ready for an internal audit and a certification body.

WHAT THIS REPORT IS

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The scores, readiness levels, gaps, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

A control that is running but cannot be evidenced scores 0.75, not 1.00. Auditors sample records, not intentions. Closing that distance is usually the fastest route to a higher score.

All assessment questions and guidance are original wording by Governance Docs. Clause and control references are used as identifiers; no text from the standard is reproduced. You need your own licensed copy of the standard to implement it.

YOUR WORKBOOK

The Excel workbook that comes with this report follows the same sections and colours. Dashboard: sections 1 and 2, recalculated live. Assessment: every requirement; change a status and every score, chart and level updates. Remediation Plan: section 3, with owners, dates and progress since this report. How it was scored: this page.

Governance Docs · governancedocs.com