

GOVERNANCE DOCS

NIST SP 800-53 Rev. 5

Gap Assessment Report

NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations

Fairview County IT Services (sample)

County IT services: the data centre, the resident services portal and the employee network.

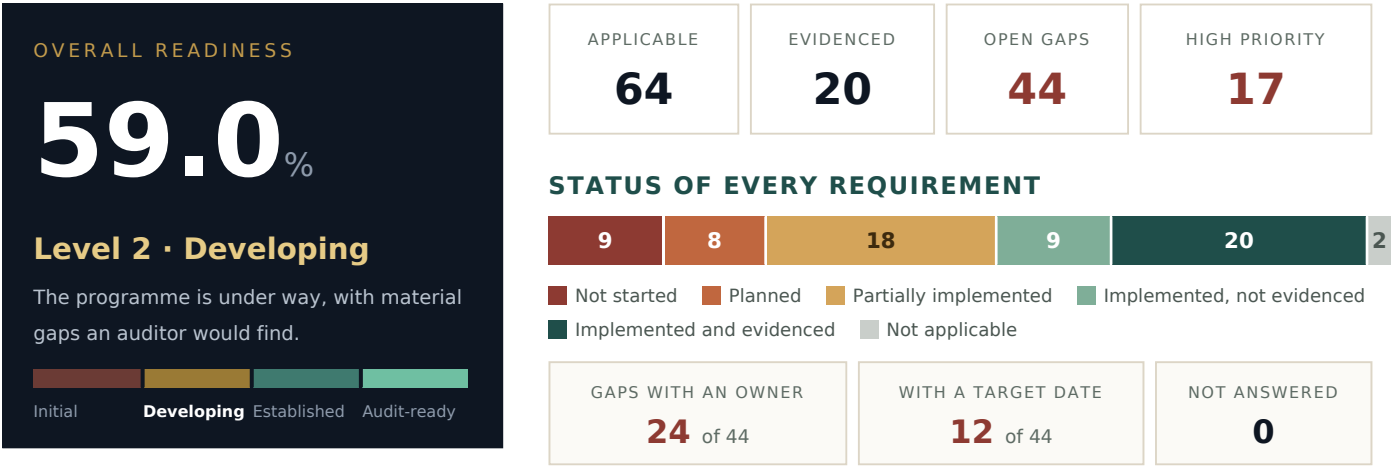
ASSESSED	25 September 2026
EDITION	Revision 5, Release 5.2.0, August 2025
IN SCOPE	66 requirements, 64 applicable
PROFILE	Government and public sector · 50 to 249 people
PREPARED BY	Governance Docs

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 Fairview County IT Services (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Fairview County IT Services (sample) stands against NIST SP 800-53



WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 59.0% against NIST SP 800-53 across 64 applicable controls. 20 of them are implemented and evidenced.
- Most open gaps: Audit and integrity, with 8 at 34%. Strongest area: Configuration and maintenance at 83%.
- 9 controls are operating but not evidenced. Collecting their records alone lifts the score to 62.5% (+3.5 points), the cheapest gain available.
- 17 gaps are high priority (not started or only planned); 5 of them are in People and physical.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	Put an owner and date against the 5 high-priority gaps in People and physical	Operations Manager	
2	LOW	Evidence the 9 controls that already operate (+3.5 points)	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

At 59% readiness, the organization should immediately address critical gaps across access control, audit logging, and personnel security.

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

Our self-assessment stands at 59%, placing us at the Developing level with 44 open gaps and 17 high-priority items. Our primary exposures lie in unstarted access controls, audit logging, and personnel oversight, leaving our systems vulnerable to undetected events. Management needs leadership support to assign clear accountability and target dates to all outstanding gaps. With focused backing to remediate high-priority controls and formalize operational evidence, we can systematically reduce these material deficiencies across our operating environment.

WHERE YOU STAND

The self-assessment places the organization at readiness level 2 of 4, rated as Developing, with an overall score of 59%. Out of 64 applicable requirements, 44 open gaps remain, including 17 high-priority gaps. Currently, 20 controls are implemented and evidenced, while 18 are partially implemented, 9 are implemented without evidence, 8 are planned, and 9 are not started. In addition, 24 gaps have an assigned owner and 12 have a target date. The lowest scoring area is People and physical at 16.7%.

WHAT IT MEANS FOR THE ORGANIZATION

The results reveal significant operational exposure in fundamental defense mechanisms. Core monitoring and authorization capabilities remain incomplete, as shown by low scores in Audit and integrity at 34.4% and Access and identity at 37.5%. Without formal evidence and completed controls, the programme contains material gaps an auditor would find. A high proportion of open gaps lack assigned target dates, meaning remediation risks losing momentum. Addressing partially implemented controls and providing evidence for existing practices would quickly stabilize the control environment.

WHERE TO FOCUS FIRST

Initial remediation must focus on unstarted high-priority controls in access, auditing, and physical security. First, establish foundational practices for Account management and Remote access to secure network perimeters. Second, activate Event logging and Log review and reporting to ensure visibility into security events. Third, address personnel controls by setting up procedures for External personnel and Role-based training. Evidencing what already runs raises the score to 62.5%, while completing partially implemented controls brings the score to 76.6%.

1 · EXECUTIVE SUMMARY

PRIORITIES

PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1 Establish account management and remote access controls AC-2 Account management · AC-17 Remote access	Uncontrolled accounts and remote connections create direct avenues for unauthorized system access. Establishing these controls ensures only approved individuals access sensitive systems.	Draft standard operating procedures for user account creation, modification, and remote connection approval.	Comprehensive NIST SP 800-53 Security Controls Toolkit – 38 Templates	30 DAYS
2 Implement event logging and review processes AU-2 Event logging · AU-6 Log review and reporting	Without active event logs and reviews, security incidents may occur without detection or investigation. Proper logging provides the trail necessary to detect and investigate threats.	Define logging baselines across servers and schedule weekly reviews of generated security logs.	Comprehensive NIST SP 800-53 Security Controls Toolkit – 38 Templates	30 DAYS
3 Formalize external personnel requirements and role training PS-7 External personnel · AT-3 Role-based training	Third-party personnel and untrained staff create severe operational vulnerabilities. Formal oversight and targeted training ensure personnel handle duties securely.	Compile a list of external contractors and define required security training modules for key roles.	Comprehensive NIST SP 800-53 Security Controls Toolkit – 38 Templates	60 DAYS
4 Deploy vulnerability scanning and flaw remediation SI-2 Flaw remediation · RA-5 Vulnerability monitoring and scanning	Unaddressed vulnerabilities expose system components to known technical exploits. Systematic monitoring and remediation prevent exploitation of software flaws.	Schedule regular vulnerability scanning on core systems and establish timelines for patching discovered flaws.	Comprehensive NIST SP 800-53 Security Controls Toolkit – 38 Templates	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Draft baseline procedures for Account management and Remote access.
- Configure Event logging standards and designate a reviewer for Log review and reporting.
- Collect and catalogue audit documentation for controls that are implemented but not evidenced.

DAYS 31 TO 60

- Establish security agreements and onboarding checks for External personnel.
- Roll out Role-based training curricula for personnel with security responsibilities.
- Assign accountable owners and completion dates to all 44 open gaps.

DAYS 61 TO 90

- Initiate scheduled Vulnerability monitoring and scanning across production environments.
- Establish formal Flaw remediation workflows and procedures for Root cause analysis on flaws.
- Advance partially implemented controls across Scoping, programme and planning to full completion.

Maturity across the standard

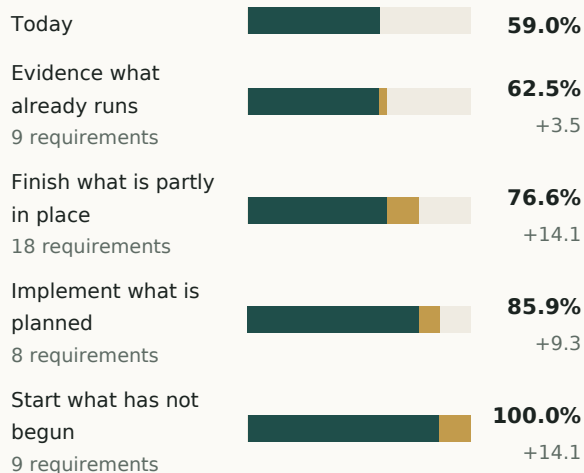
Each bar shows how the requirements in one area break down by status, weakest on the left. The score is the average across applicable requirements; the chips count open gaps by priority.

AREAS	STATUS MIX	SCORE	GAPS H · M · L
Scoping, programme and planning		75%	0 3 0
People and physical		17%	5 1 0
Risk, assessment and authorisation		50%	2 3 2
Access and identity		38%	4 3 0
Configuration and maintenance		83%	0 2 0
Audit and integrity		34%	4 1 3
Protection, media and continuity		78%	1 2 2
Acquisition, supply chain, incident and privacy		79%	1 3 2

■ 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.



DOCUMENTS THAT CLOSE THE MOST GAPS

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

All of these are in the NIST SP 800-53 Toolkit (38 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 · 9

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

Ref	Requirement	Area	Owner · target	Closes it
PS-7	External personnel	People and physical	Operations Manager	
AT-3	Role-based training	People and physical	Compliance Lead	
PE-6	Monitoring physical access	People and physical	Compliance Lead	
AC-2	Account management	Access and identity	Compliance Lead 12 Nov 2026	
AC-17	Remote access	Access and identity	Operations Manager 29 Oct 2026	
AU-2	Event logging	Audit and integrity	To assign	
AU-6	Log review and reporting	Audit and integrity	Risk Manager	
SI-2	Flaw remediation	Audit and integrity	HR Manager	
SI-2(7)	Root cause analysis on flaws	Audit and integrity	To assign	

HIGH Planned · 8

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

Ref	Requirement	Area	Owner · target	Closes it
PS	Personnel security	People and physical	Operations Manager 7 Jan 2027	
AT	Awareness and training	People and physical	To assign	
RA-5	Vulnerability monitoring and scanning	Risk, assessment and authorisation	Risk Manager 21 Jan 2027	
CA-7	Continuous monitoring	Risk, assessment and authorisation	HR Manager	
AC-4	Information flow enforcement	Access and identity	Operations Manager 10 Dec 2026	
IA-5	Authenticator management	Access and identity	Compliance Lead	
CP	Contingency planning	Protection, media and continuity	Compliance Lead	
SR-11	Component authenticity	Acquisition, supply chain, incident and privacy	Compliance Lead 10 Dec 2026	

MEDIUM Partially implemented · 18

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

Ref	Requirement	Area	Owner · target	Closes it
SCOPE-1	Security categorisation	Scoping, programme and planning	Risk Manager 29 Oct 2026	
SCOPE-2	Baseline selection	Scoping, programme and planning	IT Manager	
SCOPE-3	Organisation-defined parameters	Scoping, programme and planning	To assign	
PE	Physical and environmental protection	People and physical	Operations Manager	
RA	Risk assessment	Risk, assessment and authorisation	To assign	
CA-5	Plan of action and milestones	Risk, assessment and authorisation	HR Manager 21 Jan 2027	
CA-3	External connections	Risk, assessment and authorisation	To assign	
AC-6	Least privilege	Access and identity	Operations Manager 24 Dec 2026	
IA	Identification and authentication	Access and identity	To assign	
IA-2	Multi-factor authentication	Access and identity	To assign	
CM-6	Configuration settings	Configuration and maintenance	To assign	
CM-8	Component inventory	Configuration and maintenance	Operations Manager	
SI-4	System monitoring	Audit and integrity	Risk Manager 4 Feb 2027	
SC-7	Boundary protection	Protection, media and continuity	Risk Manager	
SC-8	Transmission protection	Protection, media and continuity	To assign	
SA-11	Developer testing and evaluation	Acquisition, supply chain, incident and privacy	HR Manager 12 Nov 2026	
IR	Incident response	Acquisition, supply chain, incident and privacy	IT Manager 10 Dec 2026	
PT-5	Privacy notice and individual rights	Acquisition, supply chain, incident and privacy	To assign	

LOW Implemented, not evidenced · 9

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
RA-7	Risk response	Risk, assessment and authorisation	To assign	
CA	Assessment, authorisation and monitoring	Risk, assessment and authorisation	To assign	
AU	Audit and accountability	Audit and integrity	To assign	
AU-9	Protection of audit information	Audit and integrity	To assign	
SI	System and information integrity	Audit and integrity	To assign	
SC-28	Protection of information at rest	Protection, media and continuity	To assign	
MP	Media protection	Protection, media and continuity	To assign	
SA-24	Design for cyber resiliency	Acquisition, supply chain, incident and privacy	To assign	
SR-6	Supplier assessments and reviews	Acquisition, supply chain, incident and privacy	To assign	

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