SAMPLE REPORT - FICTIONAL ORGANISATION

GOVERNANCE DOCS

NIST SP 800-171 Revision 2

Gap Assessment Report

NIST SP 800-171 Rev 2 with DFARS 252.204-7012, 7019 and 7020

Ridgeway Aerospace Components (sample)

The systems that process, store or transmit CUI for defence contracts, including engineering workstations and the file server.

ASSESSED	25 September 2026
EDITION	Revision 2 (February 2020, updated January 2021)
IN SCOPE	123 requirements, 122 applicable
PROFILE	Manufacturing and industrial · 50 to 249 people · US Department of Defense
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 Ridgeway Aerospace Components (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Ridgeway Aerospace Components (sample) stands against NIST SP 800-171

OVERALL READINESS

55.7%

Level 2 · Developing

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

Initial | **Developing** | Established | Audit-ready

APPLICABLE	EVIDENCED	OPEN GAPS	HIGH PRIORITY
122	31	91	39

STATUS OF EVERY REQUIREMENT

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

GAPS WITH AN OWNER	WITH A TARGET DATE	NOT ANSWERED
40 of 91	18 of 91	0

WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 55.7% against NIST SP 800-171 across 122 applicable controls. 31 of them are implemented and evidenced.
- Most open gaps: 3.1 Access Control, with 22 at 22%. Strongest area: 3.9 Personnel Security at 100%.
- 29 controls are operating but not evidenced. Collecting their records alone lifts the score to 61.7% (+6.0 points), the cheapest gain available.
- 39 gaps are high priority (not started or only planned); 16 of them are in 3.1 Access Control.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	**Put an owner and date against the 16 high-priority gaps in 3.1 Access Control**	Operations Manager	3.1 Access Control Policy
2	MEDIUM	**Adopt and tailor the Procedures and Runbooks Compendium, which closes 82 open gaps**	To assign	Procedures and Runbooks Compendium
3	LOW	**Evidence the 29 controls that already operate (+6.0 points)**	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

With an overall score of 55.7% and 91 open gaps, you must first establish core access control and identification policies.

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 55.7%, placing us at Developing readiness with 91 open gaps across 122 applicable requirements. Our primary exposure lies in core operational controls, specifically Access Control and Identification and Authentication. These gaps directly impact US Department of Defense expectations. To mitigate operational risk, executive leadership must assign owners to all open gaps and allocate resources to complete required policies and technical controls across our systems.

WHERE YOU STAND

Your self-assessment shows an overall score of 55.7% with a readiness level of 2 of 4, classified as Developing. Across 122 applicable requirements, you have 91 open gaps, including 39 high priority gaps. Currently, 31 requirements are implemented and evidenced, while 29 are implemented but not evidenced. Only 40 gaps have an assigned owner and 18 gaps have a target date. The assessment indicates that your programme is under way, but material gaps remain that an auditor would find during an evaluation.

WHAT IT MEANS FOR THE ORGANIZATION

The results highlight uneven security across operational domains. While Personnel Security reached 100% and Risk Assessment scored 91.7%, foundational areas lag behind. Access Control scored 21.6% with 22 open gaps, and Awareness and Training scored 16.7% with 3 open gaps. Identification and Authentication stands at 36.4%. For a defense contractor, these shortfalls matter directly to US Department of Defense expectations. Operational practices exist without documentation, meaning that 29 requirements cannot yet be demonstrated externally.

WHERE TO FOCUS FIRST

Your immediate priority is establishing core governance documentation to resolve foundational gaps. Evidencing what already runs raises your score to 61.7%. Finishing what is partially in place brings the score to 71.1%, and implementing what is planned reaches 80.3%. You should address Access Control and Identification and Authentication first, as these domains account for critical exposure. Standardizing runbooks and formal policies across these areas establishes operational baselines, allows you to assign accountable owners, and ensures that planned security controls become verifiable practices across your infrastructure.

PRIORITIES

	PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1	**Enforce Authorised Access and Least Privilege Controls** 3.1.1 Authorised access control · 3.1.5 Least privilege	Access Control has 22 open gaps and a score of 21.6%, exposing systems to unauthorised usage and failing US Department of Defense expectations.	Draft the access control policy establishing baseline user privileges and permission review workflows.	**3.1 Access Control Policy** Comprehensive NIST SP 800-171 CUI Protection Toolkit – 33 Templates	30 DAYS
2	**Implement Multi-Factor Authentication and Password Complexity** 3.5.3 Multi-factor authentication · 3.5.7 Password complexity	Weak authentication leaves organizational boundaries vulnerable to credential compromise and unauthorized access.	Configure multi-factor authentication requirements across remote access and administrative entry points.	**3.5 Identification and Authentication Policy** Comprehensive NIST SP 800-171 CUI Protection Toolkit – 33 Templates	30 DAYS
3	**Establish Remediation Tracking and SPRS Scoring Accuracy** 3.12.2 Plans of action · DF.2 Score calculated correctly	Accurate tracking ensures progress against high priority gaps while aligning reported security scores with regulator expectations.	Populate the plan of action and milestones template with all high priority gap owners and deadlines.	**Plan of Action and Milestones POAM Template** Comprehensive NIST SP 800-171 CUI Protection Toolkit – 33 Templates	60 DAYS
4	**Strengthen Network Boundary Protection and Tunnelling Security** 3.13.1 Boundary protection · 3.13.7 Split tunnelling prevention	Inadequate boundary enforcement allows split tunnelling and uncontrolled traffic across communications infrastructure.	Review perimeter network configurations to block split tunnelling on remote client connections.	**3.13 System and Communications Protection Policy** Comprehensive NIST SP 800-171 CUI Protection Toolkit – 33 Templates	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Formally approve and publish the access control policy across all operating environments.
- Enforce multi-factor authentication across all external access pathways and administrative accounts.
- Assign named owners and target dates to all 39 high priority gaps.

DAYS 31 TO 60

- Assemble evidence for 29 implemented controls to lift assessment score to 61.7%.
- Maintain the plan of action and milestones template to track remediation progress systematically.
- Implement password complexity and inactive identifier termination rules on all systems.

DAYS 61 TO 90

- Enforce boundary protection controls and eliminate split tunnelling on remote connections.
- Deploy visitor escorting procedures and manage physical access authorization devices.
- Conduct security awareness training sessions for all personnel handling sensitive data.

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.

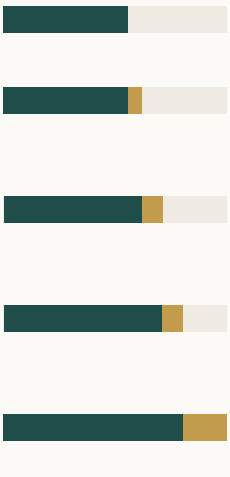
AREAS	STATUS MIX	SCORE	GAPS H · M · L
Scope and programme	1 · 2 · 1 · 1	60%	1 · 2 · 1
3.1 Access Control	13 · 3 · 2 · 4	22%	16 · 2 · 4
3.2 Awareness and Training	2 · 1	17%	2 · 1 · 0
3.3 Audit and Accountability	2 · 2 · 5	83%	0 · 2 · 2
3.4 Configuration Management	3 · 2 · 4	78%	0 · 3 · 2
3.5 Identification and Authentication	3 · 4 · 2 · 2	36%	7 · 2 · 0
3.6 Incident Response	3	75%	0 · 0 · 3
3.7 Maintenance	1 · 2 · 2 · 1	50%	1 · 2 · 2
3.8 Media Protection	1 · 3 · 5	86%	0 · 1 · 3
3.9 Personnel Security	2	100%	0 · 0 · 0
3.10 Physical Protection	2 · 1 · 1 · 2	38%	3 · 1 · 2
3.11 Risk Assessment	1 · 2	92%	0 · 0 · 1
3.12 Security Assessment	1 · 1 · 1 · 1	63%	1 · 1 · 1
3.13 System and Communications Protection	2 · 3 · 2 · 5 · 4	59%	5 · 2 · 5
3.14 System and Information Integrity	1 · 1 · 2 · 3	75%	1 · 1 · 2
DFARS obligations and SPRS	1 · 1 · 3 · 1 · 2	56%	2 · 3 · 1

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

Where the next points come from

WHERE THE NEXT POINTS COME FROM

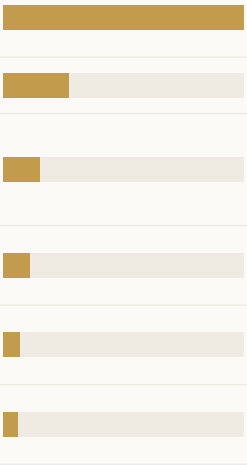
The score after each kind of work, cheapest first. Gold is what that step adds.



Today		**55.7%**
Evidence what already runs 29 requirements		**61.7%** +6.0
Finish what is partly in place 23 requirements		**71.1%** +9.4
Implement what is planned 15 requirements		**80.3%** +9.2
Start what has not begun 24 requirements		**100.0%** +19.7

DOCUMENTS THAT CLOSE THE MOST GAPS

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



Procedures and Runbooks Compendium	**82**
3.1 Access Control Policy	**22**
3.13 System and Communications Protection Policy	**12**
3.5 Identification and Authentication Policy	**9**
3.10 Physical Protection Policy	**6**
3.4 Configuration Management Policy	**5**

All of these are in the NIST SP 800-171 Toolkit (33 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 · 24**

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

Ref	Requirement	Area	Owner · target	Closes it
3.1.1	Authorised access control	3.1 Access Control	IT Manager 24 Dec 2026	3.1 Access Control Policy · Procedures and Runbooks Compendium
3.1.2	Transaction and function control	3.1 Access Control	To assign	3.1 Access Control Policy · Procedures and Runbooks Compendium
3.1.4	Separation of duties	3.1 Access Control	Operations Manager 7 Jan 2027	3.1 Access Control Policy · Procedures and Runbooks Compendium
3.1.5	Least privilege	3.1 Access Control	To assign	3.1 Access Control Policy · Procedures and Runbooks Compendium
3.1.6	Non-privileged accounts	3.1 Access Control	Risk Manager	3.1 Access Control Policy · Procedures and Runbooks Compendium
3.1.7	Preventing privileged function execution	3.1 Access Control	To assign	3.1 Access Control Policy · Procedures and Runbooks Compendium
3.1.10	Session lock	3.1 Access Control	HR Manager	3.1 Access Control Policy · Procedures and Runbooks Compendium
3.1.11	Session termination	3.1 Access Control	Compliance Lead	3.1 Access Control Policy · Procedures and Runbooks Compendium
3.1.12	Remote access monitoring and control	3.1 Access Control	HR Manager 24 Dec 2026	3.1 Access Control Policy · Procedures and Runbooks Compendium
3.1.17	Wireless protection	3.1 Access Control	Operations Manager 21 Jan 2027	3.1 Access Control Policy · Procedures and Runbooks Compendium
3.1.19	CUI encryption on mobile	3.1 Access Control	Compliance Lead	3.1 Access Control Policy · Procedures and Runbooks Compendium
3.1.20	External system connections	3.1 Access Control	Risk Manager 29 Oct 2026	3.1 Access Control Policy · Procedures and Runbooks Compendium
3.1.22	Publicly accessible content	3.1 Access Control	Operations Manager	3.1 Access Control Policy · Procedures and Runbooks Compendium

3.2.1	Security awareness	3.2 Awareness and Training	Risk Manager	3.2 Awareness and Training Policy · Training Register +1 more
3.2.2	Role-based training	3.2 Awareness and Training	Operations Manager	3.2 Awareness and Training Policy · Training Register +1 more
3.5.6	Inactive identifiers	3.5 Identification and Authentication	IT Manager	3.5 Identification and Authentication Policy · Procedures and Runbooks Compendium
3.5.7	Password complexity	3.5 Identification and Authentication	To assign	3.5 Identification and Authentication Policy · Procedures and Runbooks Compendium
3.5.10	Cryptographically protected passwords	3.5 Identification and Authentication	HR Manager	3.5 Identification and Authentication Policy · Procedures and Runbooks Compendium
3.7.1	System maintenance	3.7 Maintenance	HR Manager	3.7 Maintenance Policy · Procedures and Runbooks Compendium
3.10.3	Escorting visitors	3.10 Physical Protection	To assign	3.10 Physical Protection Policy · Procedures and Runbooks Compendium
3.10.5	Managing physical access devices	3.10 Physical Protection	To assign	3.10 Physical Protection Policy · Procedures and Runbooks Compendium
3.13.7	Split tunnelling prevention	3.13 System and Communications Protection	To assign	3.13 System and Communications Protection Policy · Procedures and Runbooks Compendium
3.13.15	Communications session authenticity	3.13 System and Communications Protection	HR Manager	3.13 System and Communications Protection Policy · Procedures and Runbooks Compendium
DF.2	Score calculated correctly	DFARS obligations and SPRS	To assign	SP 800-171A Assessment Report Template · System Security Plan SSP Template

HIGH **Planned · 15**

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

Ref	Requirement	Area	Owner · target	Closes it
SP.4	Cloud service providers	Scope and programme	Operations Manager	CUI Scoping and Boundary Guide · Vendor and Subcontractor Flowdown Register
3.1.9	Privacy and security notices	3.1 Access Control	HR Manager 26 Nov 2026	3.1 Access Control Policy · Procedures and Runbooks Compendium

3.1.14	Managed access control points	3.1 Access Control	To assign	3.1 Access Control Policy · Procedures and Runbooks Compendium
3.1.21	Portable storage on external systems	3.1 Access Control	Compliance Lead	3.1 Access Control Policy · Procedures and Runbooks Compendium
3.5.3	Multi-factor authentication	3.5 Identification and Authentication	IT Manager 26 Nov 2026	3.5 Identification and Authentication Policy · Procedures and Runbooks Compendium
3.5.5	Identifier reuse	3.5 Identification and Authentication	Operations Manager	3.5 Identification and Authentication Policy · Procedures and Runbooks Compendium
3.5.9	Temporary passwords	3.5 Identification and Authentication	To assign	3.5 Identification and Authentication Policy · Procedures and Runbooks Compendium
3.5.11	Obscured authentication feedback	3.5 Identification and Authentication	To assign	3.5 Identification and Authentication Policy · Procedures and Runbooks Compendium
3.10.2	Protecting the physical facility	3.10 Physical Protection	HR Manager	3.10 Physical Protection Policy · Procedures and Runbooks Compendium
3.12.2	Plans of action	3.12 Security Assessment	Compliance Lead 4 Feb 2027	3.12 Security Assessment Policy · Plan of Action and Milestones POAM Template +1 more
3.13.1	Boundary protection	3.13 System and Communications Protection	Compliance Lead 4 Feb 2027	3.13 System and Communications Protection Policy · CUI Scoping and Boundary Guide +1 more
3.13.2	Security engineering	3.13 System and Communications Protection	Operations Manager 26 Nov 2026	3.13 System and Communications Protection Policy · Procedures and Runbooks Compendium
3.13.6	Deny by default network traffic	3.13 System and Communications Protection	IT Manager 4 Feb 2027	3.13 System and Communications Protection Policy · Procedures and Runbooks Compendium
3.14.7	Identifying unauthorised use	3.14 System and Information Integrity	To assign	3.14 System and Information Integrity Policy · Procedures and Runbooks Compendium
DF.8	Evidence and cross-mapping	DFARS obligations and SPRS	To assign	Cross-Mapping Appendix · SP 800-171A Assessment Report Template

MEDIUM **Partially implemented · 23**

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

Ref	Requirement	Area	Owner · target	Closes it

SP.3	Roles and ownership	Scope and programme	To assign	Control RACI Master · Toolkit Overview and Document Map
SP.5	Subcontractor flow-down	Scope and programme	Risk Manager 26 Nov 2026	Vendor and Subcontractor Flowdown Register
3.1.3	Control CUI flow	3.1 Access Control	To assign	3.1 Access Control Policy · CUI Flow and Data Inventory Guidance +1 more
3.1.15	Privileged remote access	3.1 Access Control	To assign	3.1 Access Control Policy · Procedures and Runbooks Compendium
3.2.3	Insider threat awareness	3.2 Awareness and Training	To assign	3.2 Awareness and Training Policy · Training Register +1 more
3.3.4	Audit logging process failure	3.3 Audit and Accountability	IT Manager 26 Nov 2026	3.3 Audit and Accountability Policy · Procedures and Runbooks Compendium
3.3.5	Audit correlation	3.3 Audit and Accountability	Risk Manager	3.3 Audit and Accountability Policy · Procedures and Runbooks Compendium
3.4.3	Change tracking and approval	3.4 Configuration Management	To assign	3.4 Configuration Management Policy · Procedures and Runbooks Compendium
3.4.4	Security impact analysis	3.4 Configuration Management	Risk Manager	3.4 Configuration Management Policy · Procedures and Runbooks Compendium
3.4.7	Restricting nonessential functions	3.4 Configuration Management	IT Manager	3.4 Configuration Management Policy · Procedures and Runbooks Compendium
3.5.1	User and device identification	3.5 Identification and Authentication	HR Manager 12 Nov 2026	3.5 Identification and Authentication Policy · Procedures and Runbooks Compendium
3.5.2	Authentication	3.5 Identification and Authentication	To assign	3.5 Identification and Authentication Policy · Procedures and Runbooks Compendium
3.7.2	Maintenance tools control	3.7 Maintenance	Compliance Lead 4 Feb 2027	3.7 Maintenance Policy · Procedures and Runbooks Compendium
3.7.3	Sanitising equipment for off-site maintenance	3.7 Maintenance	To assign	3.7 Maintenance Policy · Procedures and Runbooks Compendium
3.8.4	Media marking	3.8 Media Protection	Risk Manager	3.8 Media Protection Policy · CUI Definition and Identification Guide +1 more
3.10.1	Physical access authorisation	3.10 Physical Protection	To assign	3.10 Physical Protection Policy · Procedures and Runbooks Compendium
3.12.3	Continuous monitoring	3.12 Security Assessment	HR Manager	3.12 Security Assessment Policy · Metrics and KPI Catalog +1 more

3.13.11	FIPS-validated cryptography	3.13 System and Communications Protection	Operations Manager 29 Oct 2026	3.13 System and Communications Protection Policy · Procedures and Runbooks Compendium
3.13.13	Mobile code	3.13 System and Communications Protection	Operations Manager	3.13 System and Communications Protection Policy · Procedures and Runbooks Compendium
3.14.6	Monitoring for attacks	3.14 System and Information Integrity	Compliance Lead 24 Dec 2026	3.14 System and Information Integrity Policy · Procedures and Runbooks Compendium
DF.1	Basic self-assessment in SPRS	DFARS obligations and SPRS	To assign	SP 800-171A Assessment Plan Template · SP 800-171A Assessment Report Template
DF.3	Plans of action	DFARS obligations and SPRS	Operations Manager	Plan of Action and Milestones POAM Template · Implementation Roadmap
DF.4	72-hour incident reporting	DFARS obligations and SPRS	Risk Manager 26 Nov 2026	3.6 Incident Response Policy · Procedures and Runbooks Compendium

LOW **Implemented, not evidenced · 29**

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
SP.1	CUI identification	Scope and programme	To assign	CUI Definition and Identification Guide · CUI Flow and Data Inventory Guidance +1 more
3.1.8	Unsuccessful logon attempts	3.1 Access Control	To assign	3.1 Access Control Policy · Procedures and Runbooks Compendium
3.1.13	Remote access confidentiality	3.1 Access Control	To assign	3.1 Access Control Policy · Procedures and Runbooks Compendium
3.1.16	Wireless authorisation	3.1 Access Control	To assign	3.1 Access Control Policy · Procedures and Runbooks Compendium
3.1.18	Mobile device connection control	3.1 Access Control	To assign	3.1 Access Control Policy · Procedures and Runbooks Compendium
3.3.7	Time synchronisation	3.3 Audit and Accountability	To assign	3.3 Audit and Accountability Policy · Procedures and Runbooks Compendium
3.3.8	Audit information protection	3.3 Audit and Accountability	To assign	3.3 Audit and Accountability Policy · Procedures and Runbooks Compendium
3.4.5	Access restrictions for change	3.4 Configuration Management	To assign	3.4 Configuration Management Policy · Procedures and Runbooks Compendium

3.4.8	Application allowlisting	3.4 Configuration Management	To assign	3.4 Configuration Management Policy · Procedures and Runbooks Compendium
3.6.1	Incident handling capability	3.6 Incident Response	To assign	3.6 Incident Response Policy · Procedures and Runbooks Compendium
3.6.2	Incident tracking and reporting	3.6 Incident Response	To assign	3.6 Incident Response Policy · Procedures and Runbooks Compendium
3.6.3	Incident response testing	3.6 Incident Response	To assign	3.6 Incident Response Policy · Procedures and Runbooks Compendium
3.7.4	Checking media for malicious code	3.7 Maintenance	To assign	3.7 Maintenance Policy · Procedures and Runbooks Compendium
3.7.5	Multifactor for nonlocal maintenance	3.7 Maintenance	To assign	3.7 Maintenance Policy · Procedures and Runbooks Compendium
3.8.1	Media protection	3.8 Media Protection	To assign	3.8 Media Protection Policy · CUI Data Register +1 more
3.8.3	Media sanitisation before disposal	3.8 Media Protection	To assign	3.8 Media Protection Policy · Procedures and Runbooks Compendium
3.8.6	Cryptographic protection during transport	3.8 Media Protection	To assign	3.8 Media Protection Policy · Procedures and Runbooks Compendium
3.10.4	Physical access audit logs	3.10 Physical Protection	To assign	3.10 Physical Protection Policy · Procedures and Runbooks Compendium
3.10.6	Alternate work sites	3.10 Physical Protection	To assign	3.10 Physical Protection Policy · Procedures and Runbooks Compendium
3.11.2	Vulnerability scanning	3.11 Risk Assessment	To assign	3.11 Risk Assessment Policy · Risk Register +1 more
3.12.4	System security plan	3.12 Security Assessment	To assign	3.12 Security Assessment Policy · System Security Plan SSP Template +1 more
3.13.4	Preventing shared resource information transfer	3.13 System and Communications Protection	To assign	3.13 System and Communications Protection Policy · Procedures and Runbooks Compendium
3.13.5	Public-access system separation	3.13 System and Communications Protection	To assign	3.13 System and Communications Protection Policy · Procedures and Runbooks Compendium
3.13.8	Transmission confidentiality	3.13 System and Communications Protection	To assign	3.13 System and Communications Protection Policy · Procedures and Runbooks Compendium

3.13.10	Cryptographic key management	3.13 System and Communications Protection	To assign	3.13 System and Communications Protection Policy · Procedures and Runbooks Compendium
3.13.14	Voice over IP	3.13 System and Communications Protection	To assign	3.13 System and Communications Protection Policy · Procedures and Runbooks Compendium
3.14.3	Security alerts and advisories	3.14 System and Information Integrity	To assign	3.14 System and Information Integrity Policy · Procedures and Runbooks Compendium
3.14.5	System and file scanning	3.14 System and Information Integrity	To assign	3.14 System and Information Integrity Policy · Procedures and Runbooks Compendium
DF.6	Alternative measures and exceptions	DFARS obligations and SPRS	To assign	Exception Register

A · ABOUT THIS REPORT

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