

GOVERNANCE DOCS

NIST Cybersecurity Framework 2.0

Gap Assessment Report

NIST Cybersecurity Framework (CSF) 2.0

Riverbend Credit Union (sample)

All member-facing services, core banking and the corporate network across four branches.

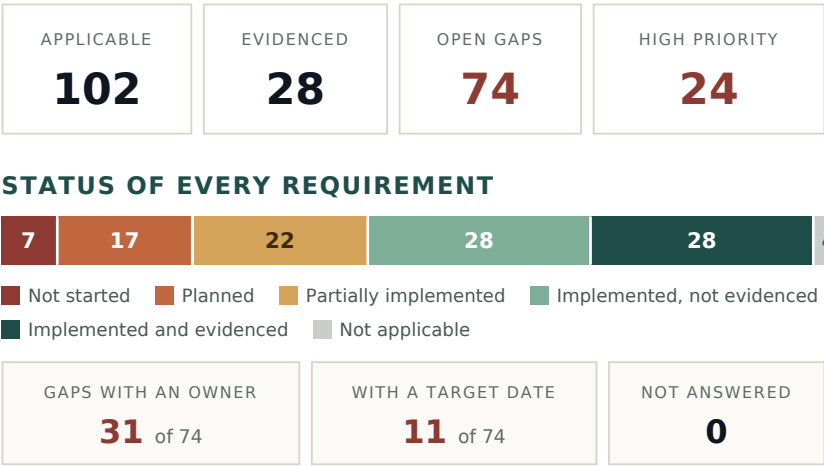
ASSESSED	25 September 2026
EDITION	CSWP 29, February 2024
IN SCOPE	106 requirements, 102 applicable
PROFILE	Banking and financial services · 50 to 249 people
PREPARED BY	Governance Docs

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 Riverbend Credit Union (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Riverbend Credit Union (sample) stands against NIST CSF 2.0



WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 63.0% against NIST CSF 2.0 across 102 applicable controls. 28 of them are implemented and evidenced.
- Most open gaps: GV.SC - Supply chain risk management, with 7 at 75%. Strongest area: RC.RP - Incident recovery plan execution at 85%.
- 28 controls are operating but not evidenced. Collecting their records alone lifts the score to 69.9% (+6.9 points), the cheapest gain available.
- 24 gaps are high priority (not started or only planned); 5 of them are in ID.AM - Asset management.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	Put an owner and date against the 5 high-priority gaps in ID.AM - Asset management	Operations Manager	Asset Criticality and Prioritisation Procedure
2	MEDIUM	Adopt and tailor the Incident Triage and Categorisation Procedure, which closes 3 open gaps	To assign	Incident Triage and Categorisation Procedure
3	LOW	Evidence the 28 controls that already operate (+6.9 points)	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

With a 63% score at the Developing level, the organization must prioritize evidencing existing controls and resolving 24 high-priority gaps.

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 cybersecurity self-assessment against NIST CSF 2.0 scores our readiness at 63%, placing us at level 2 of 4, or Developing. Our primary exposures lie in technology infrastructure resilience, asset management, and unevidenced operational controls. We currently carry 74 open gaps, including 24 high priority gaps. To reduce operational exposure, leadership needs board support to enforce accountability, mandate formal ownership and remediation dates for all open gaps, and prioritize documentation for our incident management and recovery processes.

WHERE YOU STAND

Your self-assessment against the NIST Cybersecurity Framework 2.0 places you at readiness level 2 of 4, named Developing, with an overall score of 63%. Out of 102 applicable requirements, you have 74 open gaps, including 24 high priority gaps. While 28 requirements are implemented and evidenced, another 28 are implemented but lack documentation. Across the program, 31 gaps have an assigned owner and 11 have a target date. The lowest-scoring control areas are Incident recovery communication at 12.5%, Technology infrastructure resilience at 25%, and Asset management at 28.6%.

WHAT IT MEANS FOR THE ORGANIZATION

The assessment indicates that the organization operates key defenses in practice but lacks formal proof and complete coverage. Operating 28 controls without evidence exposes the business to scrutiny, as unrecorded practices cannot be verified during reviews. Material exposures exist in Technology infrastructure resilience and Asset management, where critical systems and operational capacity lack formal prioritization. Furthermore, because only 11 open gaps have set deadlines and 31 have designated owners, accountability remains incomplete across operational units, which slows remediation efforts.

WHERE TO FOCUS FIRST

Initial efforts should focus on closing the 24 high priority gaps and documenting implemented controls to raise the score toward 69.9%. Immediate work must address baseline operational structures, beginning with formal procedures for incident handling and asset prioritization. Establishing documentation such as the Incident Triage and Categorisation Procedure directly addresses multiple gaps. Additionally, leadership should assign clear owners and target dates to all unassigned open gaps to ensure accountability across technical and governance workstreams.

1 · EXECUTIVE SUMMARY

PRIORITIES

PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1 Formalize incident triage and validation procedures RS.MA-02 Triage and validation	Unstructured incident response leads to delays in handling security events and increases potential downtime. Establishing clear triage ensures adverse events are categorized swiftly.	Draft the triage procedure using standard event severity criteria.	Incident Triage and Categorisation Procedure NIST CSF Toolkit – 164 Cybersecurity Framework 2.0 Templates	30 DAYS
2 Establish hardware inventory and asset prioritisation ID.AM-05 Asset prioritisation · ID.AM-01 Hardware inventory	Lack of asset classification makes it difficult to protect core systems or determine critical recovery paths. Knowing asset priority protects vital banking operations.	Compile existing hardware records into a centralized inventory list.	Asset Criticality and Prioritisation Procedure NIST CSF Toolkit – 164 Cybersecurity Framework 2.0 Templates	30 DAYS
3 Define resilience mechanisms and capacity management PR.IR-03 Resilience mechanisms · PR.IR-04 Capacity	Without redundancy and capacity planning, critical systems risk unexpected outages during disruptions. This limits operational continuity across services.	Review current operational capacity limits and redundancy configurations.	Resilience and Redundancy Architecture Statement NIST CSF Toolkit – 164 Cybersecurity Framework 2.0 Templates	60 DAYS
4 Structure incident recovery communication and public updates RC.CO-04 Public updates · RC.CO-03 Recovery communication to stakeholders	Disorganized communications during a recovery effort can cause confusion among stakeholders and the public. Clear communication templates protect organizational trust.	Prepare message templates for public and stakeholder notifications.	Public and Stakeholder Communication Templates NIST CSF Toolkit – 164 Cybersecurity Framework 2.0 Templates	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Assign designated owners and delivery dates to all remaining unassigned open gaps.
- Implement the Incident Triage and Categorisation Procedure to structure event handling.
- Consolidate hardware records to begin building the hardware asset inventory.
- Document evidence for the 28 implemented controls currently lacking proof.

DAYS 31 TO 60

- Complete the Asset Criticality and Prioritisation Procedure across critical systems.
- Draft the Resilience and Redundancy Architecture Statement for core technology components.
- Establish the Capacity and Availability Management Procedure to monitor infrastructure thresholds.

DAYS 61 TO 90

- Develop the Recovery Communication Procedure and Public and Stakeholder Communication Templates.
- Formalize the Event Impact and Scope Assessment Procedure for adverse events.
- Review remediation progress across all 24 high priority gaps.

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.

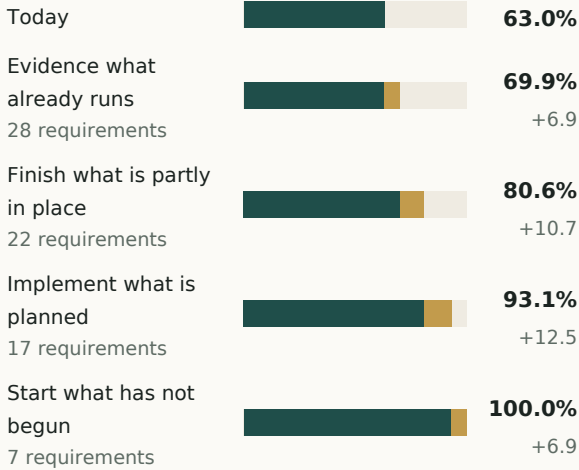
AREAS	STATUS MIX	SCORE	GAPS H · M · L
GV.OC - Organizational context	1 2 1 1	35%	3 1 1
GV.RM - Risk management strategy	2 3 1 1	71%	0 2 3
GV.RR - Roles, responsibilities and authorities	1 1 2	75%	1 0 1
GV.PO - Policy	1 1	75%	0 1 0
GV.OV - Oversight	2 1	83%	0 0 2
GV.SC - Supply chain risk management	3 4 3	75%	0 3 4
ID.AM - Asset management	1 4 2	29%	5 2 0
ID.RA - Risk assessment	2 6	80%	1 2 1
ID.IM - Improvement	1 2 1	75%	0 1 2
PR.AA - Identity, authentication and access control	1 2 3	83%	0 1 2
PR.AT - Awareness and training	1 1	75%	0 1 0
PR.DS - Data security	1 1 1 1	63%	1 1 1
PR.PS - Platform security	1 3 1 1	75%	0 1 3
PR.IR - Technology infrastructure resilience	2 1 1	25%	3 0 1
DE.CM - Continuous monitoring	2 2 1	63%	0 2 2
DE.AE - Adverse event analysis	2 1 1 1 1	42%	3 1 1
RS.MA - Incident management	1 2 2	75%	1 0 2
RS.AN - Incident analysis	3 1	31%	3 1 0
RS.CO - Incident response reporting	1 1	75%	0 1 0
RS.MI - Incident mitigation	1 1	50%	1 0 1
RC.RP - Incident recovery plan execution	1 1 3 1	85%	0 1 1
RC.CO - Incident recovery communication	1 1	13%	2 0 0

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

Where the next points come from

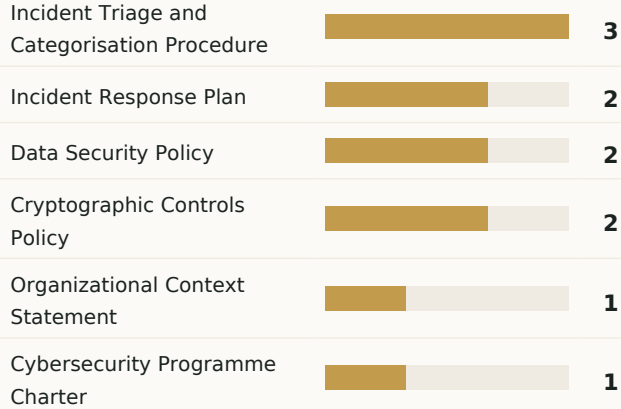
WHERE THE NEXT POINTS COME FROM

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



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 CSF Toolkit (164 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
GV.OC-02	Internal and external stakeholders	GV.OC	To assign	Mission and Stakeholder Expectations Analysis
ID.AM-05	Asset prioritisation	ID.AM	To assign	Asset Criticality and Prioritisation Procedure
PR.IR-03	Resilience mechanisms	PR.IR	To assign	Resilience and Redundancy Architecture Statement
PR.IR-04	Capacity	PR.IR	IT Manager	Capacity and Availability Management Procedure
DE.AE-02	Adverse event analysis	DE.AE	Risk Manager	Adverse Event Analysis Procedure
DE.AE-04	Impact and scope	DE.AE	Compliance Lead	Event Impact and Scope Assessment Procedure
RC.CO-04	Public updates	RC.CO	Operations Manager	Public and Stakeholder Communication Templates

HIGH Planned · 17

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

Ref	Requirement	Area	Owner · target	Closes it
GV.OC-01	Organizational mission	GV.OC	To assign	Organizational Context Statement · Cybersecurity Programme Charter
GV.OC-03	Legal and regulatory requirements	GV.OC	HR Manager	Legal Regulatory and Contractual Requirements Register
GV.RR-01	Leadership accountability	GV.RR	Operations Manager	Leadership Accountability Statement
ID.AM-01	Hardware inventory	ID.AM	To assign	Hardware Asset Inventory
ID.AM-03	Network and data flows	ID.AM	Operations Manager	Network and Data Flow Documentation Procedure
ID.AM-04	Inventory of services from suppliers	ID.AM	To assign	Supplier-Provided Services Inventory
ID.AM-08	Asset lifecycle management	ID.AM	Operations Manager	Asset Lifecycle and Secure Disposal Procedure
ID.RA-02	Threat intelligence	ID.RA	Operations Manager	Threat Intelligence Procedure

PR.DS-01	Data at rest	PR.DS	Risk Manager 26 Nov 2026	Data Security Policy · Cryptographic Controls Policy
PR.IR-01	Network protection	PR.IR	HR Manager	Network Security Standard
DE.AE-03	Correlating information	DE.AE	Operations Manager 12 Nov 2026	Event Correlation and Log Review Standard
RS.MA-02	Triage and validation	RS.MA	Risk Manager 10 Dec 2026	Incident Triage and Categorisation Procedure
RS.AN-03	Analysis to determine what happened	RS.AN	Risk Manager	Incident Analysis Record
RS.AN-06	Investigation record	RS.AN	IT Manager 29 Oct 2026	Forensic Investigation and Evidence Handling Procedure
RS.AN-07	Incident data and metadata	RS.AN	To assign	Evidence and Chain of Custody Register
RS.MI-01	Containment	RS.MI	To assign	Incident Containment Procedure
RC.CO-03	Recovery communication to stakeholders	RC.CO	Compliance Lead 29 Oct 2026	Recovery Communication Procedure

MEDIUM

Partially implemented · 22

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

Ref	Requirement	Area	Owner · target	Closes it
GV.OC-05	Dependencies	GV.OC	To assign	Dependencies and Critical Services Analysis
GV.RM-03	Cybersecurity in enterprise risk management	GV.RM	IT Manager	Enterprise Risk Integration Procedure
GV.RM-04	Risk response strategy	GV.RM	Risk Manager	Risk Response Strategy and Options
GV.PO-02	Policy review	GV.PO	IT Manager	Policy Review and Maintenance Procedure
GV.SC-02	Supply chain roles	GV.SC	HR Manager 21 Jan 2027	Supplier Roles and Responsibilities Statement
GV.SC-03	Integration with enterprise risk	GV.SC	HR Manager	C-SCRM Integration into Enterprise Risk Procedure
GV.SC-07	Ongoing supplier risk	GV.SC	To assign	Critical Supplier Assessment Procedure
ID.AM-02	Software inventory	ID.AM	Operations Manager	Software Services and Systems Inventory
ID.AM-07	Data and metadata inventory	ID.AM	To assign	Data Inventory and Classification Register
ID.RA-03	Threats identified	ID.RA	Operations Manager 29 Oct 2026	Threat Register
ID.RA-06	Risk responses	ID.RA	To assign	Risk Response Plan
ID.IM-04	Response and recovery plans	ID.IM	Compliance Lead 12 Nov 2026	Incident Response Plan · Cybersecurity Improvement Plan

PR.AA-01	Identities and credentials	PR.AA	To assign	Identity and Access Management Policy
PR.AT-01	General awareness and training	PR.AT	Risk Manager	Security Awareness and Training Policy
PR.DS-02	Data in transit	PR.DS	Operations Manager 26 Nov 2026	Data Security Policy · Cryptographic Controls Policy
PR.PS-03	Hardware maintenance	PR.PS	To assign	Hardware and Software Lifecycle Register
DE.CM-02	Physical environment monitoring	DE.CM	Compliance Lead	Physical Environment Monitoring Procedure
DE.CM-03	Personnel activity monitoring	DE.CM	HR Manager 7 Jan 2027	Personnel Activity and Technology Usage Monitoring Procedure
DE.AE-06	Information provided to stakeholders	DE.AE	HR Manager 12 Nov 2026	Event and Alert Register
RS.AN-08	Incident magnitude	RS.AN	Risk Manager	Incident Magnitude Estimation Procedure
RS.CO-03	Information sharing	RS.CO	To assign	External Incident Notification and Regulatory Reporting Procedure
RC.RP-03	Backup integrity verification	RC.RP	Compliance Lead	Backup Integrity Verification Procedure

LOW Implemented, not evidenced · 28

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
GV.OC-04	Critical objectives and services	GV.OC	To assign	Critical Objectives and Services Register
GV.RM-01	Risk management objectives	GV.RM	To assign	Cybersecurity Risk Management Strategy
GV.RM-02	Risk appetite and tolerance	GV.RM	To assign	Risk Appetite and Risk Tolerance Statement
GV.RM-06	Standardised risk method	GV.RM	To assign	Cybersecurity Risk Assessment Methodology
GV.RR-04	Cybersecurity in human resources	GV.RR	To assign	Human Resources Cybersecurity Practices Procedure
GV.OV-01	Strategy outcome review	GV.OV	To assign	Programme Coverage and Adjustment Review
GV.OV-03	Performance measurement	GV.OV	To assign	Risk Management Strategy Performance Review Report
GV.SC-04	Supplier criticality	GV.SC	To assign	Supplier Identification and Prioritisation Procedure
GV.SC-05	Supply chain requirements in contracts	GV.SC	To assign	Supplier Contract Cybersecurity Requirements
GV.SC-06	Pre-award due diligence	GV.SC	To assign	Supplier Due Diligence Procedure

GV.SC-10	Post-relationship activities	GV.SC	To assign	Supplier Termination and Exit Procedure
ID.RA-09	Authenticity and integrity of acquisitions	ID.RA	To assign	Third-Party Hardware and Software Integrity Procedure
ID.IM-02	Improvement from tests and exercises	ID.IM	To assign	Security Test and Exercise Programme
ID.IM-03	Improvement from operations	ID.IM	To assign	Improvement Register
PR.AA-03	Authentication	PR.AA	To assign	Authentication and Credential Management Procedure
PR.AA-06	Physical access	PR.AA	To assign	Physical Access Control Policy
PR.DS-11	Backups	PR.DS	To assign	Backup and Restoration Procedure · Backup Test Register
PR.PS-01	Configuration management	PR.PS	To assign	Configuration Management Procedure
PR.PS-04	Log generation	PR.PS	To assign	Log Management and Retention Procedure
PR.PS-06	Secure development	PR.PS	To assign	Secure Software Development Policy
PR.IR-02	Environmental protection	PR.IR	To assign	Physical and Environmental Protection Procedure
DE.CM-01	Network monitoring	DE.CM	To assign	Network Monitoring Procedure
DE.CM-06	External service provider monitoring	DE.CM	To assign	External Service Provider Monitoring Procedure
DE.AE-08	Incident declaration	DE.AE	To assign	Incident Triage and Categorisation Procedure
RS.MA-01	Response plan execution	RS.MA	To assign	Incident Response Plan
RS.MA-03	Categorisation and prioritisation	RS.MA	To assign	Incident Triage and Categorisation Procedure
RS.MI-02	Eradication	RS.MI	To assign	Incident Eradication Procedure
RC.RP-06	End of incident declared	RC.RP	To assign	Incident Closure Procedure

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