CYBERGLASS CYBER FRAMEWORK KIT (CSF 2.0)

CSF 2.0 Implementation Guide

Start here: how [Company Name] uses the NIST Cybersecurity Framework 2.0 to understand, assess, prioritize and communicate cybersecurity risk.

Organization	[Company Name]
Document ID	CSF-01
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- Read this guide first. It explains the framework, the order in which to use the other documents, and how the workbook supports each step.
- You do not need to achieve all 106 outcomes at once. Start with the High-priority outcomes in the workbook and set targets that match your risks.
- The CSF is voluntary and outcome-based. It says what to achieve, not which products to buy or how to configure them.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

How this document connects

Document or register	How records and decisions flow
CSF-02 Organizational Profile	Records current and target scores using section 6
CSF-03 Gap Analysis	Turns gaps into initiatives A-NN
CSF-04 Leadership Report	Reports progress
CSF Workbook	106 outcomes, scores, policy map and action plan
IT kit policies	Policy map links each outcome to the IT document that addresses it

Record flow example: Outcome PR.AA-03 scored 1 (current) vs 3 (target) → gap appears in the workbook → initiative A-01 'MFA everywhere' in CSF-03 → reported in CSF-04 until re-scored.

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS CYBER FRAMEWORK KIT (CSF 2.0)

CSF 2.0 Organizational Profile

[Company Name]'s Current and Target Profiles: scope, context, method, results and the reasons behind the targets.

Organization	[Company Name]
Document ID	CSF-02
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- Complete sections 2 to 4 before scoring; the scope and context decide which outcomes and evidence matter.
- Copy the results from the workbook's Summary and Tiers sheets into sections 6 and 7 after scoring.
- Keep this document short (6–10 pages). The detail lives in the workbook.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS CYBER FRAMEWORK KIT (CSF 2.0)

CSF 2.0 Gap Analysis and Action Plan

How [Company Name] prioritizes the gaps between its Current and Target Profiles and turns them into a funded, tracked plan.

Organization	[Company Name]
Document ID	CSF-03
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- Use the workbook's Profile and Action Plan sheets as the working lists; this document explains the method and records the decisions.
- Group related gaps into a small number of initiatives. Leadership approves initiatives, not dozens of line items.
- Replace the worked example in section 4 with your own top gaps once scoring is complete.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS CYBER FRAMEWORK KIT (CSF 2.0)

CSF 2.0 Leadership Report

A quarterly one-to-two-page cybersecurity report for [Company Name]'s owners, executives or board, structured by the six CSF functions.

Organization	[Company Name]
Document ID	CSF-04
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- Keep it to two pages. Leaders want direction and decisions, not detail.
- Use the same structure every quarter so trends are easy to see.
- Copy the function results and chart from the workbook's Summary sheet into section 2.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

Source: National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper (CSWP) 29, Gaithersburg, MD. https://doi.org/10.6028/NIST.CSWP.29. Republished courtesy of the National Institute of Standards and Technology. The CSF is a US government publication, not subject to copyright in the United States. Explanations, priorities, examples and templates are CyberGlass's own. NIST does not endorse CyberGlass or this template. Using this kit does not mean an organization conforms to, or is certified against, any standard.

1. Summary for Leadership

> **GUIDANCE** *(delete before publishing)*
> Write this box last. Leaders often read only this section, so make every line count.

Reporting period	[Q_ YYYY]
Overall status	[On track / at risk / off track], in one sentence
Biggest improvement	[e.g. MFA now enforced for 100% of accounts]
Biggest concern	[e.g. backups for the finance system not yet restore-tested]
Decisions needed	[e.g. approve budget for a managed detection service]

2. Progress by Function

Function	Last quarter	This quarter	Target	Highlights
Govern	[ ]	[ ]	[ ]	[ ]
Identify	[ ]	[ ]	[ ]	[ ]
Protect	[ ]	[ ]	[ ]	[ ]
Detect	[ ]	[ ]	[ ]	[ ]
Respond	[ ]	[ ]	[ ]	[ ]
Recover	[ ]	[ ]	[ ]	[ ]

[Insert the current vs target chart from the workbook.]

3. Tiers

Area	Current	Target	Target date
Risk governance	[ ]	[ ]	[ ]
Risk management	[ ]	[ ]	[ ]

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop