

NIST Cybersecurity Framework (CSF) 2.0

Implementation Step by Step

A Practical Guide



The Instructor

Instructor : Dr. Amar Massood

Over 34 years of industry experience

PhD in Computer Science, 70 certifications

PMI-RMP, ISO 31000 Lead Risk Manager, ISO 27001 Auditor, CEH, ECSA, CISSP, CISM, and CISA

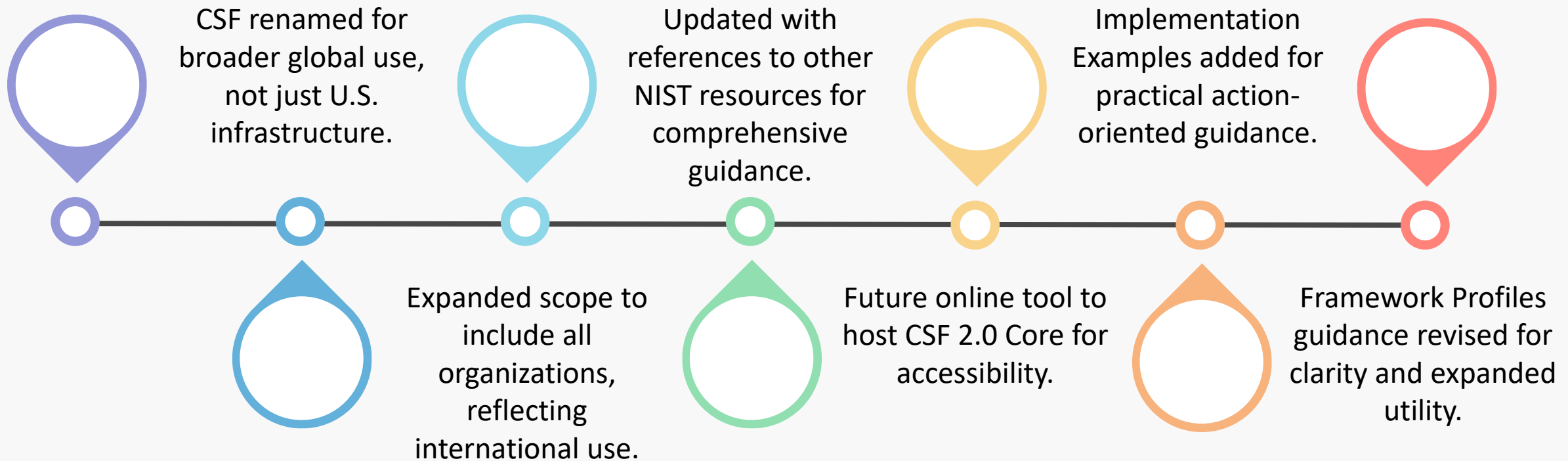
Step by step process with templates and tools

Easy implementation for small and medium-sized organizations

What is NIST CSF 2.0

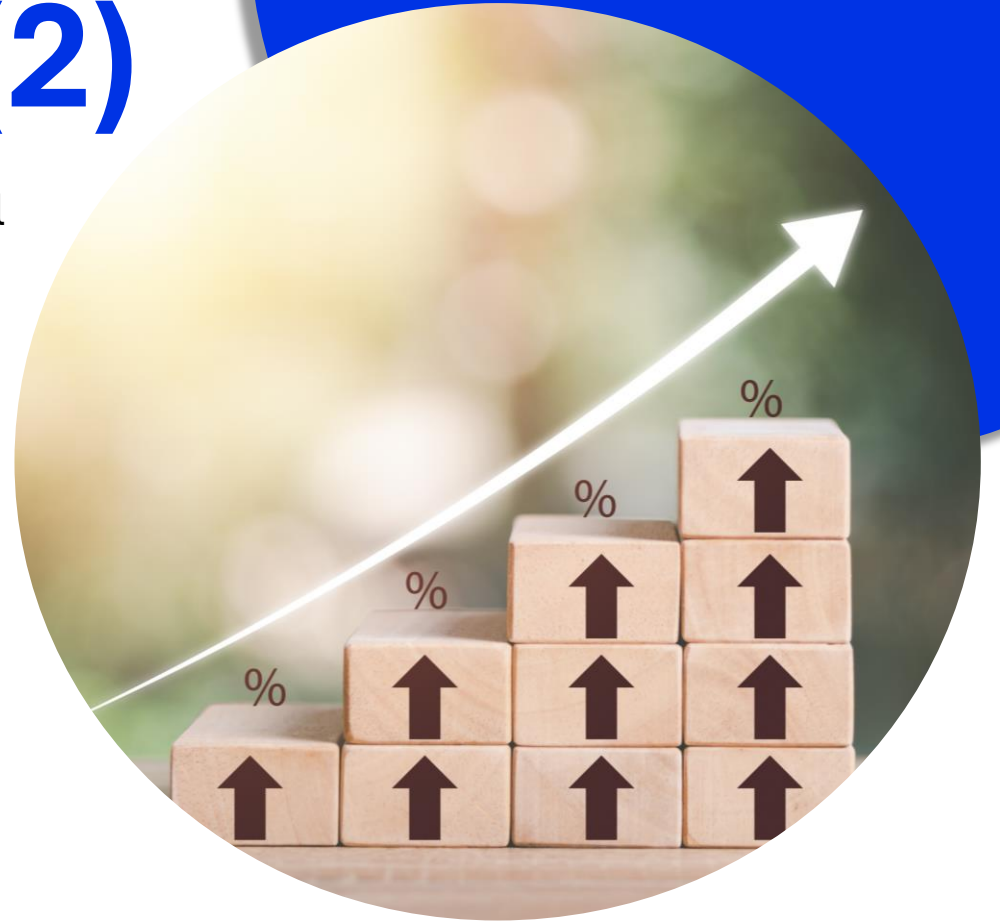
- CSF 2.0 aids all-size organizations in cybersecurity.
- Suitable for various sectors: industry, government, academia.
- Adaptable to different cybersecurity maturity levels.
- Not one-size-fits-all; tailored to unique risks.
- Addresses cybersecurity alongside other enterprise risks.
- Outcomes are sector-, country-, technology-neutral.
- Provides guidance, not prescriptions, for cybersecurity outcomes.
- Continuously updated to address evolving cybersecurity risks.

Change in CSF 2.0



Change in CSF 2.0 (2)

- New "Govern" Function added to emphasize organizational cybersecurity governance.
- Integration with NIST Privacy Framework and enterprise risk management highlighted.
- Cybersecurity supply chain risk management gets a dedicated Category.
- Latest NIST guidance incorporated for supply chain and software development.
- Cybersecurity assessment updated with references to NIST SP 800-55.
- Tiers redefined for better focus on governance, risk management, and third-party relationships.
- Continuous improvement stressed with new "Improvement" Category in "Identify" Function.



CSF Components

CSF Core

- Taxonomy of high-level cybersecurity outcomes
- Hierarchy: Functions, Categories, Subcategories

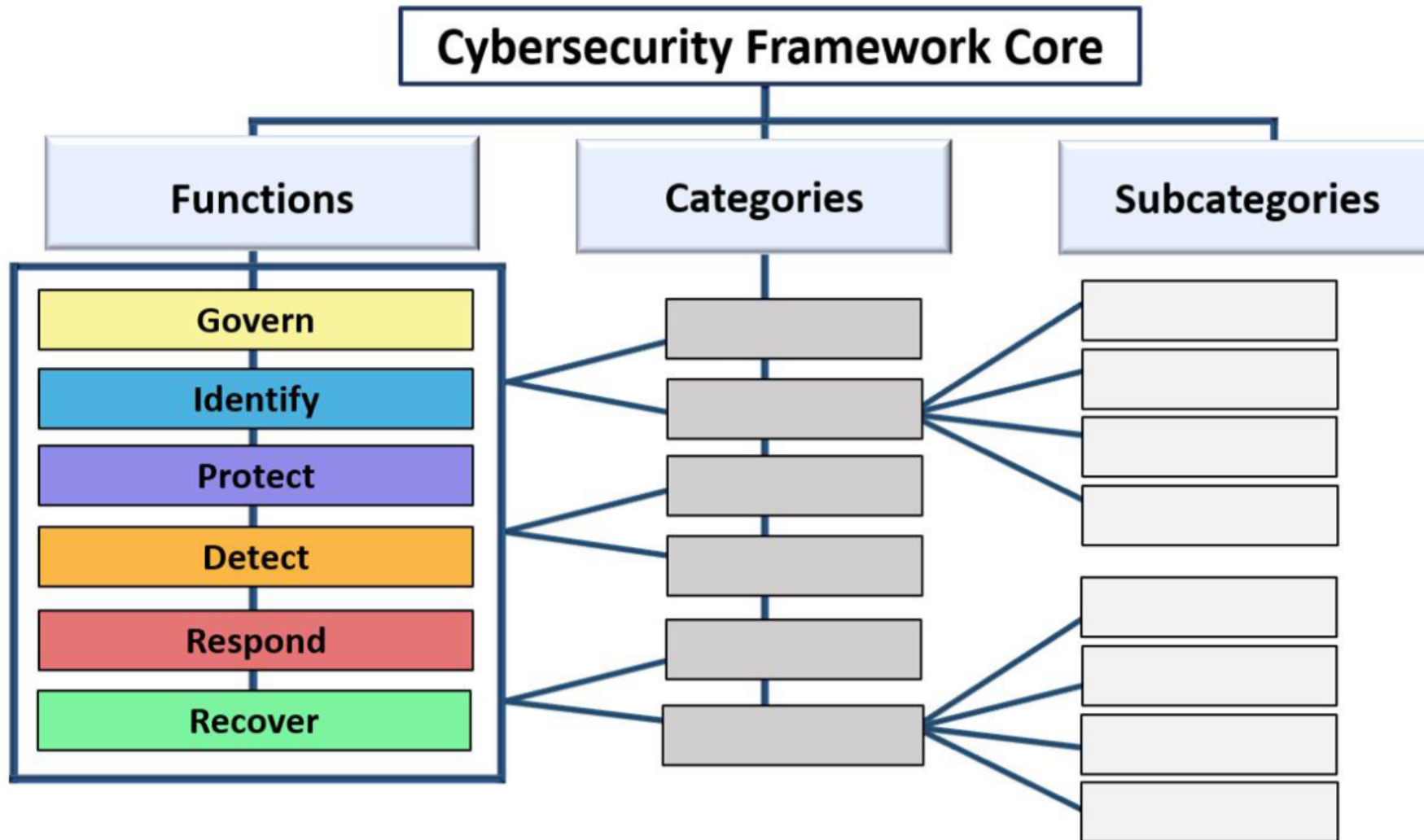
CSF Organizational Profiles

- Describe current/target cybersecurity posture
- Based on CSF Core outcomes

CSF Tiers

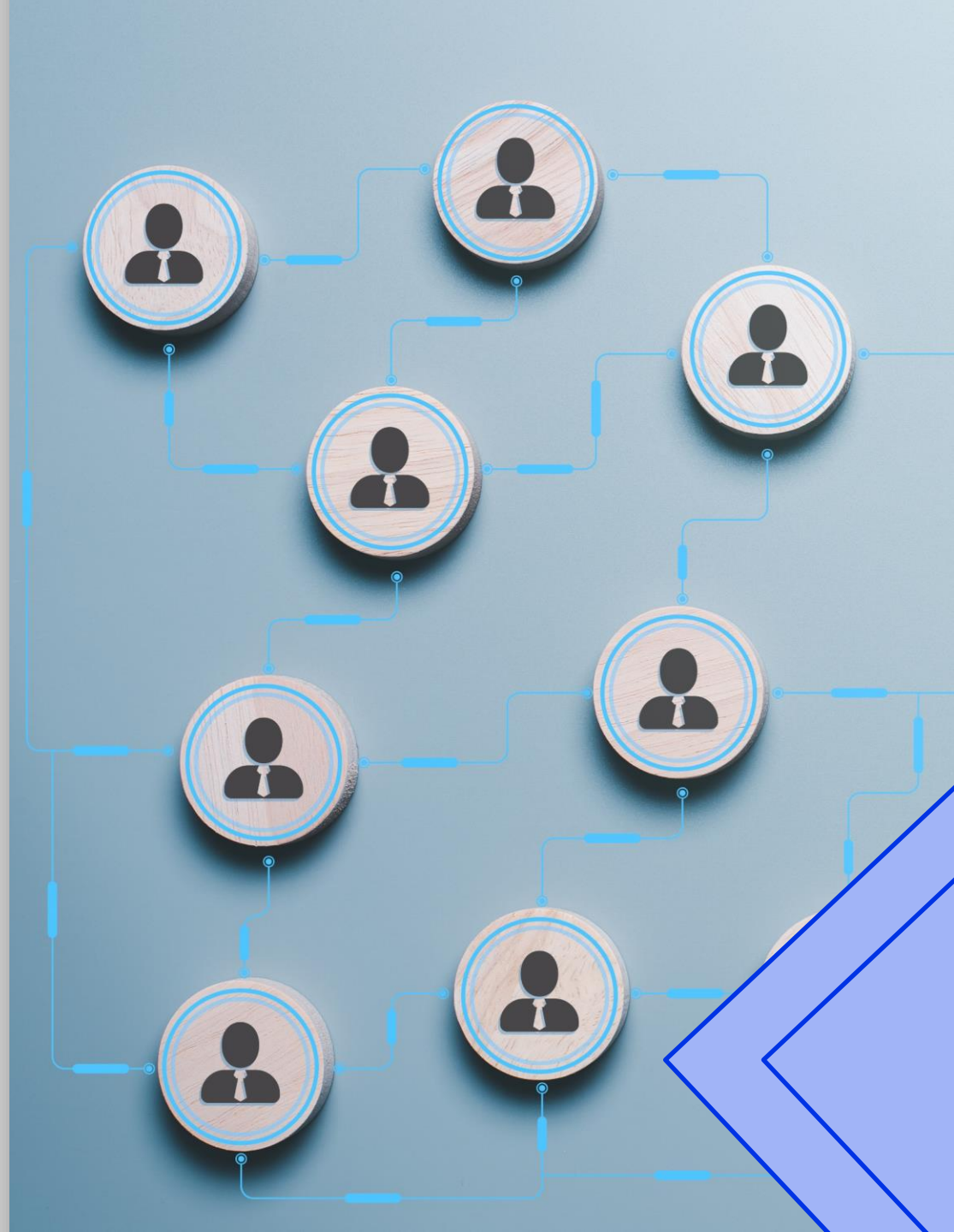
- Classify cybersecurity risk management rigor
- Provide context for risk views and processes

The CSF Core



GOVERN (GV)

- **GOVERN Function:** Sets cybersecurity risk management approach.
- **Strategy:** Establish, communicate, monitor cybersecurity policies.
- **Alignment:** Prioritize outcomes with mission, stakeholder expectations.
- **Integration:** Embed in enterprise risk management strategy.
- **Key Areas:** Organizational context, strategy, supply chain risks.
- **Roles:** Define responsibilities, authorities for cybersecurity.
- **Policies:** Develop and oversee cybersecurity policies.
- **Foundation:** Builds strong base for cybersecurity efforts.



IDENTIFY (ID)

IDENTIFY Function

Understand current cybersecurity risks.

Assess Assets

Identify data, hardware, software, and systems.

Evaluate Suppliers

Understand supplier-related cybersecurity risks.

Prioritize Efforts

Align with risk management strategy and mission.

Identify Improvements

Enhance policies, plans, and processes.

Inform All Functions

Guide efforts across the CSF framework.

PROTECT (PR)

- **PROTECT Function:** Implement safeguards for cybersecurity risks.
- **Manage Access:** Control identity, authentication, and access.
- **Train Employees:** Increase awareness and cybersecurity knowledge.
- **Secure Data:** Protect data confidentiality, integrity, and availability.
- **Platform Security:** Ensure hardware and software security.
- **Build Resilience:** Enhance technology infrastructure's ability to recover.





DETECT (DE)

- Timely Identification: Focuses on spotting potential cyber attacks.
- Crucial Role: Essential for overall cybersecurity strategy.
- Early Detection: Finds anomalies and indicators of compromise.
- Effective Mechanisms: Quickly identify suspicious activities.
- Minimizes Impact: Allows rapid response to incidents.
- Supports Response: Aids in incident recovery and mitigation.

RESPOND (RS)

- **Focus:** Actions after detecting a cybersecurity incident.
- **Goal:** Contain incident effects, minimize impact.
- **Key Outcomes:** Analysis, mitigation, reporting, communication.
- **Analysis:** Understand incident's nature, scope, root cause.
- **Mitigation:** Reduce severity, prevent further damage.
- **Reporting:** Document and communicate incident details.
- **Communication:** Clear, timely communication with stakeholders.

RECOVER (RC)

Focus: Restoration of assets, operations post-incident.

Goal: Timely return to normal, minimize long-term effects.

Key Activities: System restoration, prevention measures, communication.

System Restoration: Return affected assets to normal state.

Prevention Measures: Implement steps to avoid incident recurrence.

Communication: Transparent, trust-building recovery updates to stakeholders.

How Does The CSF Functions Work Together



Functions, Categories and SubCategories in Numbers

Level	Description	Number of Elements
Functions	High-level cybersecurity outcomes	6
Categories	More specific cybersecurity objectives within a Function	21
Subcategories	Granular details within a Category	112

Example of Function/Category/Subcategories



Function:

PROTECT (PR)



Category:

PR.AA: Identity Management, Authentication, and Access Control



Subcategory:

PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization



Function: PROTECT (PR)

PROTECT: Safeguards to Manage the Organization's Cybersecurity Risks

PR.AA: Identity Management, Authentication, and Access

PR.AT: Awareness and Training

PR.DS: Data Security

PR.PS: Platform Security

PR.IR: Technology Infrastructure
Resilience

Category: PR.AA:

Identity Management, Authentication, and Access Control

PR.AA focuses on access to assets by authorized users.

PR.AA-01: Identities and credentials are managed.

PR.AA-02: Identities are bound to credentials.

PR.AA-03: Authentication of users and hardware.

PR.AA-04: Identity assertions are protected.

PR.AA-05: Access permissions are defined and managed.

PR.AA-06: Physical access is controlled.

Subcategory: PR.AA-01:

Identities and credentials for authorized users, services, and hardware are managed by the organization

- PR.AA-01 focuses on managing identities and credentials.
- Ensures only authorized users and devices access sensitive information.
- Initiates requests for new or additional access.
- Tracks, reviews, and fulfills access requests with owner permission.
- Manages cryptographic certificates, keys, and other credentials.
- Selects unique identifiers for devices based on hardware characteristics.
- Physically labels authorized hardware for inventory and servicing.
- Critical for preventing unauthorized access and maintaining security.

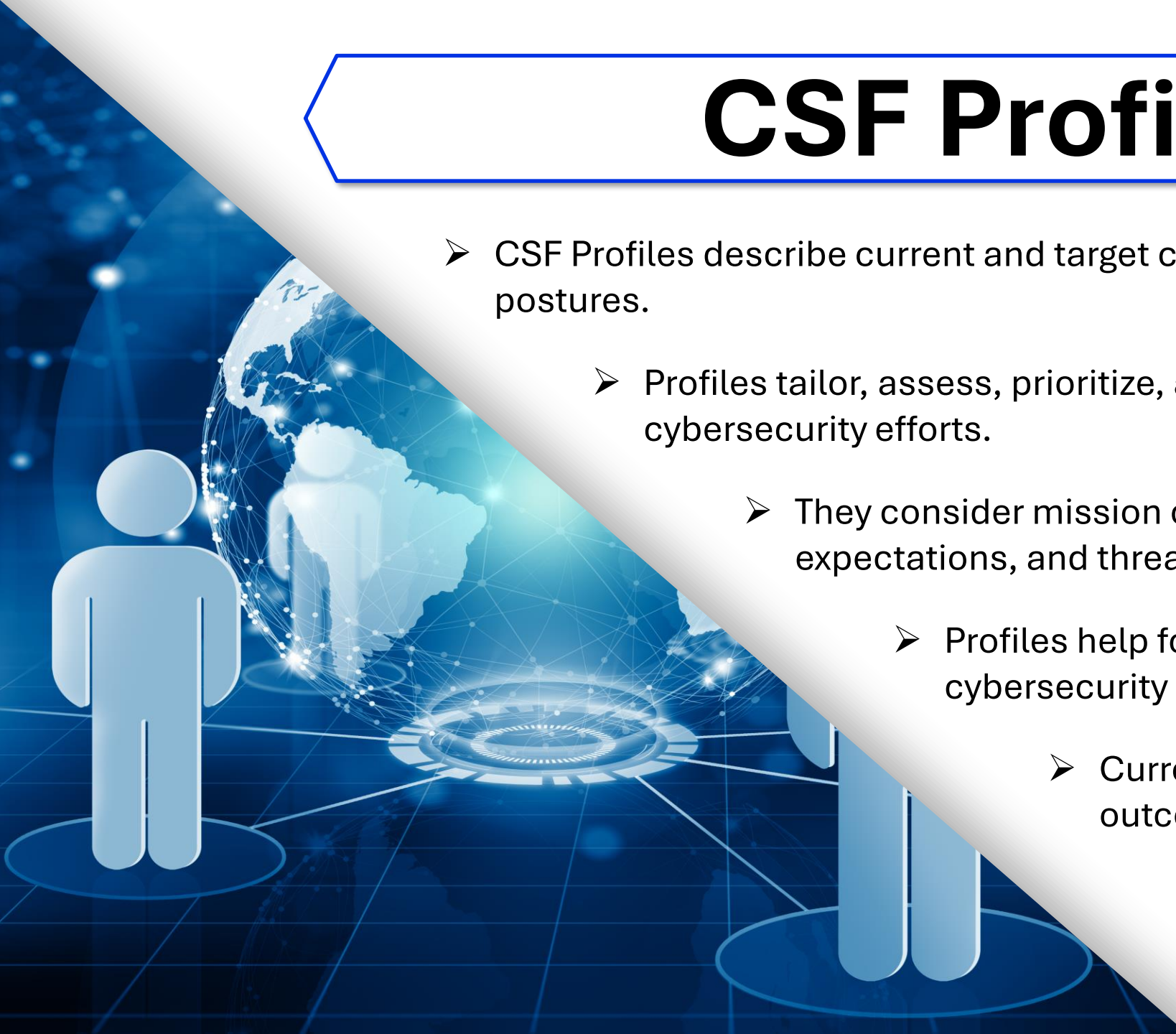
Our Course on CSF 2.0 Core

- This course focuses on CSF implementation steps.
- 6 Functions, 21 Categories, 112 Subcategories not covered here.
- Detailed course available for in-depth CSF exploration.
- Real-world examples illustrate each CSF component.
- **Aim:** Equip learners to strengthen cybersecurity posture.



CSF Profiles

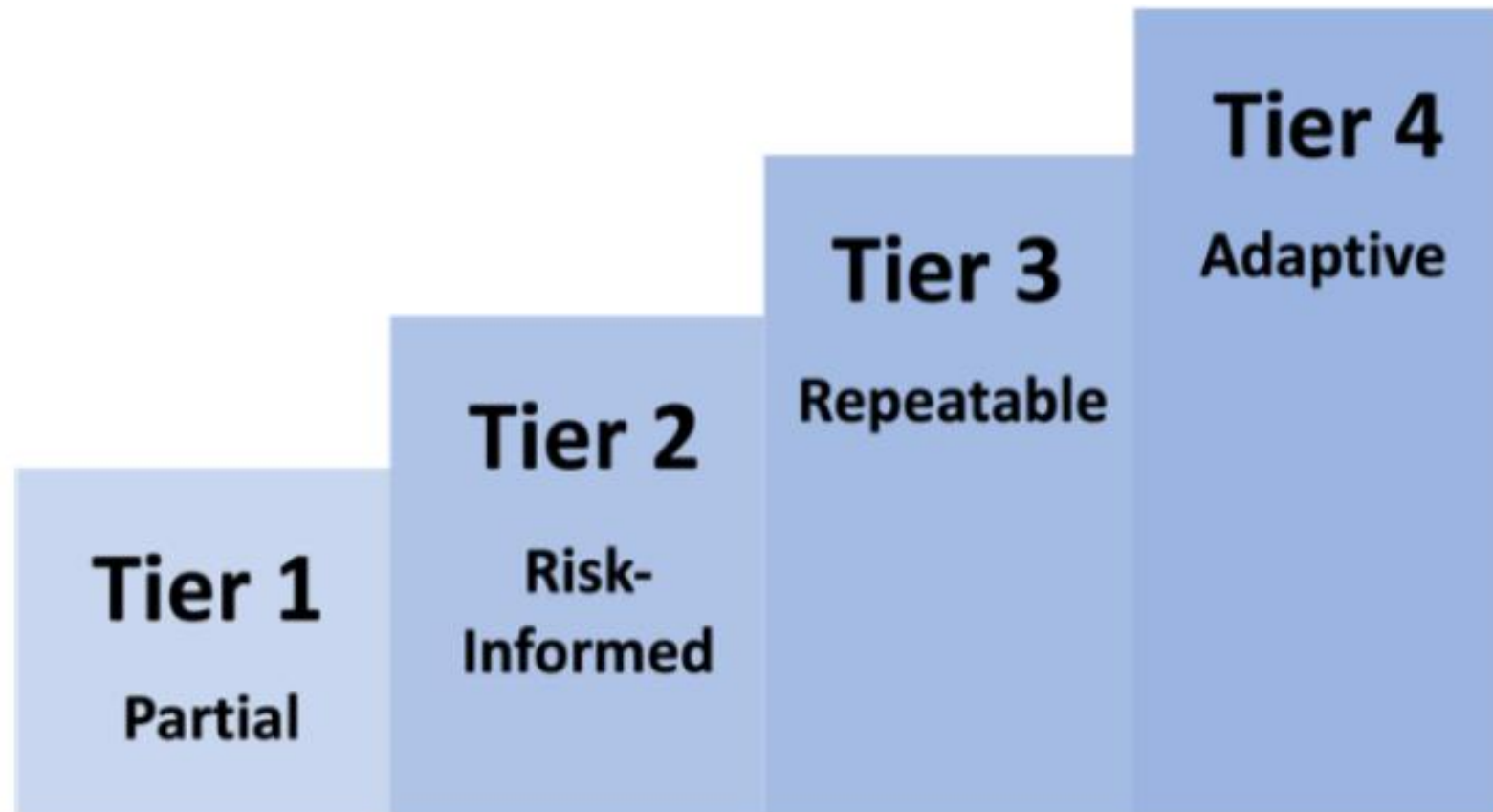
- CSF Profiles describe current and target cybersecurity postures.
- Profiles tailor, assess, prioritize, and communicate cybersecurity efforts.
- They consider mission objectives, stakeholder expectations, and threat landscape.
- Profiles help focus actions and communicate cybersecurity strategy.
- Current Profile outlines current cybersecurity outcomes and assessments.
- Target Profile defines desired outcomes and considers future changes.



How to Use CSF Profiles

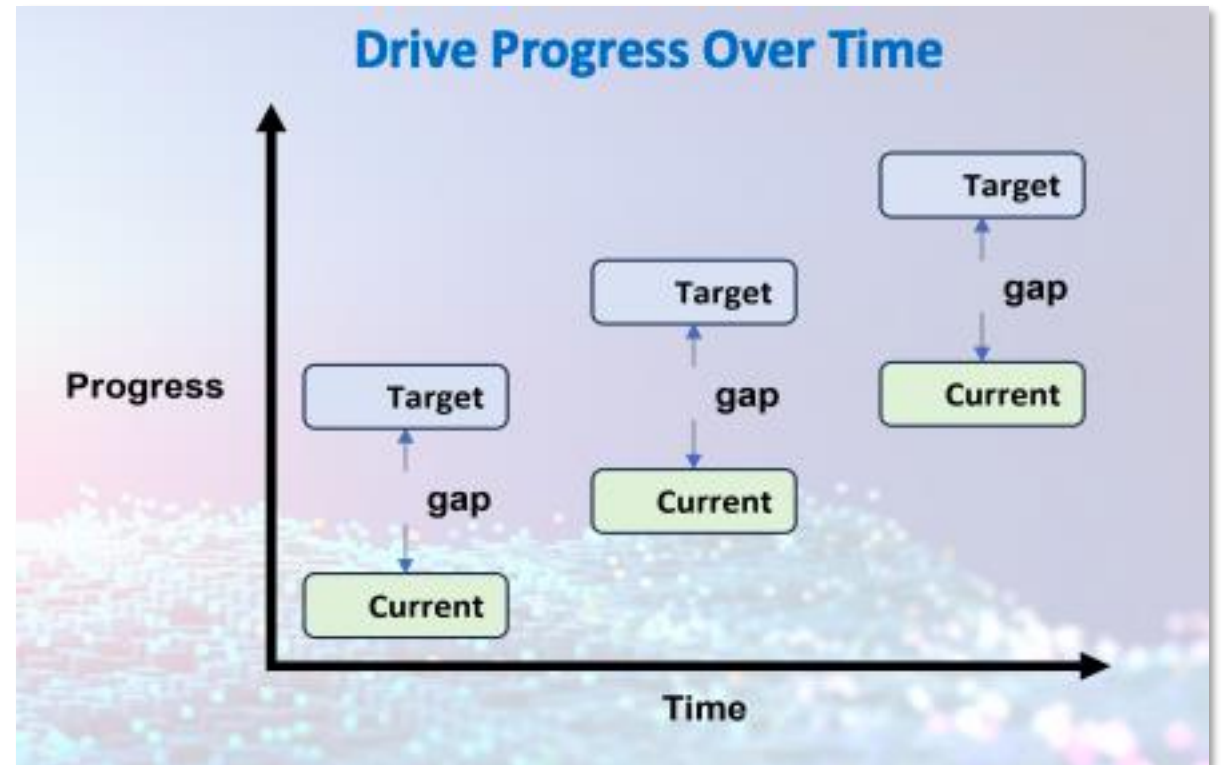


CSF Tiers



Drive Progress Over Time with Organizational Profiles

- Organizational Profiles manage cybersecurity posture.
- Current Profile outlines existing outcomes.
- Target Profile sets desired outcomes.
- Compare Profiles to assess progress.
- Profiles inform strategic decisions.
- Profiles prioritize cybersecurity efforts.
- Useful for communicating with stakeholders.



Our Use Case: GreenLeaf Retailers

GreenLeaf Retailers, a mid-sized retail company.

Operates physical stores and an online platform.

Committed to protecting customer data.

Applies NIST CSF 2.0 for cybersecurity.

Scopes Organizational Profile for security framework.

Gathers information for the Profile.

Creates Profile based on gathered data.

Implements action plan to address gaps.

CSF 2.0 Implementation Steps

1. Scope the Organizational Profile
2. Gather Information
3. Create the Organizational Profile
4. Analyze Gaps and Create an Action Plan
5. Implement the Action Plan and Update the Profile
6. Continual Improvement



Step 1:

Scope the Organizational Profile

NIST CSF implementation begins with Organizational Profile.

Profile lays foundation for framework's application.

Documents key facts and assumptions for scope.

Identifies critical functions, systems, and assets.

Allows for multiple profiles with different scopes.

Flexibility of NIST CSF enhances its effectiveness.

Profiles can focus on specific areas or systems.

Profiles can address specific threats like ransomware.

Essential Questions

- What is the purpose of creating the Organizational Profile?
- Will the Profile cover the entire organization or specific areas?
- What types of cybersecurity issues will the Profile address?
- Who is responsible for developing, reviewing, and operationalizing the Profile?
- Who will set and achieve the target outcomes?



GreenLeaf Answers

Question	Answer for GreenLeaf
What's the reason for creating the Organizational Profile?	To enhance cybersecurity posture and comply with industry standards
Will the Profile cover the entire organization?	Yes, it will cover the entire organization
Will the Profile address all types of cybersecurity threats, vulnerabilities, attacks, and defenses?	Yes, it will address all types
Which individuals or teams will be responsible for developing, reviewing, and operationalizing the Profile?	The cybersecurity team, IT department, and senior management
Who will be responsible for setting expectations for actions to achieve the target outcomes?	The Chief Information Security Officer (CISO) and the cybersec

Organization Profile Facts

Organizational Profile: Key CSF component.

Profiles can have distinct scopes.

Enables tailored cybersecurity efforts.

Scope based on technology, data, or users.

Example: Profiles for IT, OT, and PII.

Scope determines CSF outcome applicability.

Aligns efforts with specific risks and requirements.

Combine Profiles when scopes overlap.

Streamlines cybersecurity efforts with merged Profiles.

GreenLeaf Organizational Profile Facts

Profile Type	Scope	Data Types	Users
Information Technology (IT) Systems	All IT systems used in operations	Company data (financial records, employee information, business plans)	Employees and contractors accessing IT systems
Operational Technology (OT) Systems	OT systems in production and supply chain operations	Operational data (production metrics, equipment status, supply chain information)	Production staff and maintenance teams
Personally Identifiable Information (PII) Protection	Safeguarding PII of customers and employees	Data privacy (compliance with GDPR, CCPA)	Employees handling PII, third-party vendors

Step 2:

Gather Needed Information

- Gather necessary information for the Organizational Profile.
- Collect organizational policies, risk management priorities, and standards.
- Identify specific information based on use case and detail level.
- Use Community Profiles for shared interests and goals.
- Adapt Community Profiles for organization-specific needs.
- Download the NIST Organizational Profile Template for guidance.
- Fill in the template to create Current and Target Profiles.
- Use the template for side-by-side comparison and gap analysis.



Gathering Needed Information at GreenLeaf

Information Category	Examples for GreenLeaf
Organizational Policies	- Information Security Policy - Access Control Policy - Data Protection and Privacy Policy - Incident Response Policy
Risk Management Priorities	- Prioritization of assets critical to business operations - Emphasis on protecting customer data and intellectual property - Focus on mitigating risks associated with supply chain disruptions
Resources	- Budget allocation for cybersecurity initiatives - Availability of skilled cybersecurity personnel - Inventory of cybersecurity tools and technologies
Cybersecurity Requirements and Standards	- Compliance with GDPR for data privacy - Adherence to ISO/IEC 27001 for information security management - Following NIST SP 800-53 for security and privacy controls
Community Profiles	- Utilizing a sector-specific profile for the renewable energy industry - Adapting the profile to include GreenLeaf's unique operational needs
NIST Organizational Profile Template	- Filling in the template with GreenLeaf's current and target cybersecurity practices - Identifying gaps between current and target profiles for improvement

Prioritization

Prioritization is essential in Target Profile development.

Influenced by strategic objectives, laws, and risk management.

NIST SP 800-37 provides guidance on risk management.

NIST IR 8286B shows how CSF Core supports risk responses.

It assigns importance levels to various CSF outcomes.

Aligns cybersecurity efforts with overall goals and regulations.

It helps establish priorities based on risk appetite.

Enables informed decisions on responding to identified risks.

Step 3: Create the Organizational Profile

- a. Download and customize the latest CSF Organizational Profile template.
- b. Include relevant cybersecurity outcomes and document rationales.
- c. Document current cybersecurity practices in the Current Profile columns.
- d. Outline cybersecurity goals and plans in the Target Profile columns.
- e. Use the Priority field to note the importance of each goal.



a. Download CSF 2.0 Organizational Profile Template

CSF Outcomes		Current Profile			Target Profile	
Identifier	Description	Practices	Status	Rating	Priority	Goals
The identifiers and descriptions from the CSF Core – Functions, Categories, Subcategories. You can also add your own outcomes to address your organization’s unique risks and requirements.		Policies, processes, procedures and other activities related to an outcome. May include artifacts that contain evidence of achieving an outcome.	The current state or condition of an outcome, such as whether it is being achieved and to what degree.	An assessment or evaluation of current practices using scales such as: <ul style="list-style-type: none">• high/medium/low• 1-5• 0-100%,• red/yellow/green	The relative importance of an outcome using scales such as: <ul style="list-style-type: none">• Low/Medium/High• 1/2/3/4/5• rankings (1, 2, 3...)	Such as: <ul style="list-style-type: none">• Policies, Processes, and Procedures• Roles and Responsibilities Selected from: <ul style="list-style-type: none">• Informative References - standards, guidance, and best practices

b. Include Relevant Cybersecurity Outcomes and Document Rationales

- Identify applicable cybersecurity outcomes for your use case.
- Document rationales for including specific outcomes in the profile.

CSF Outcome (Function, Category, or Subcategory)	CSF Outcome Description	Included in Profile?	Rationale
PR.PT-01	Physical devices and systems are protected	Yes	Essential for securing physical assets
DE.CM-01	Network and system monitoring is implemented	Yes	Critical for early detection of threats
RS.CO-02	Internal and external stakeholders are notified of incidents	Yes	Important for transparency and compliance
RC.RP-05	The integrity of restored assets is verified	Yes	Ensures restored systems are secure and functional

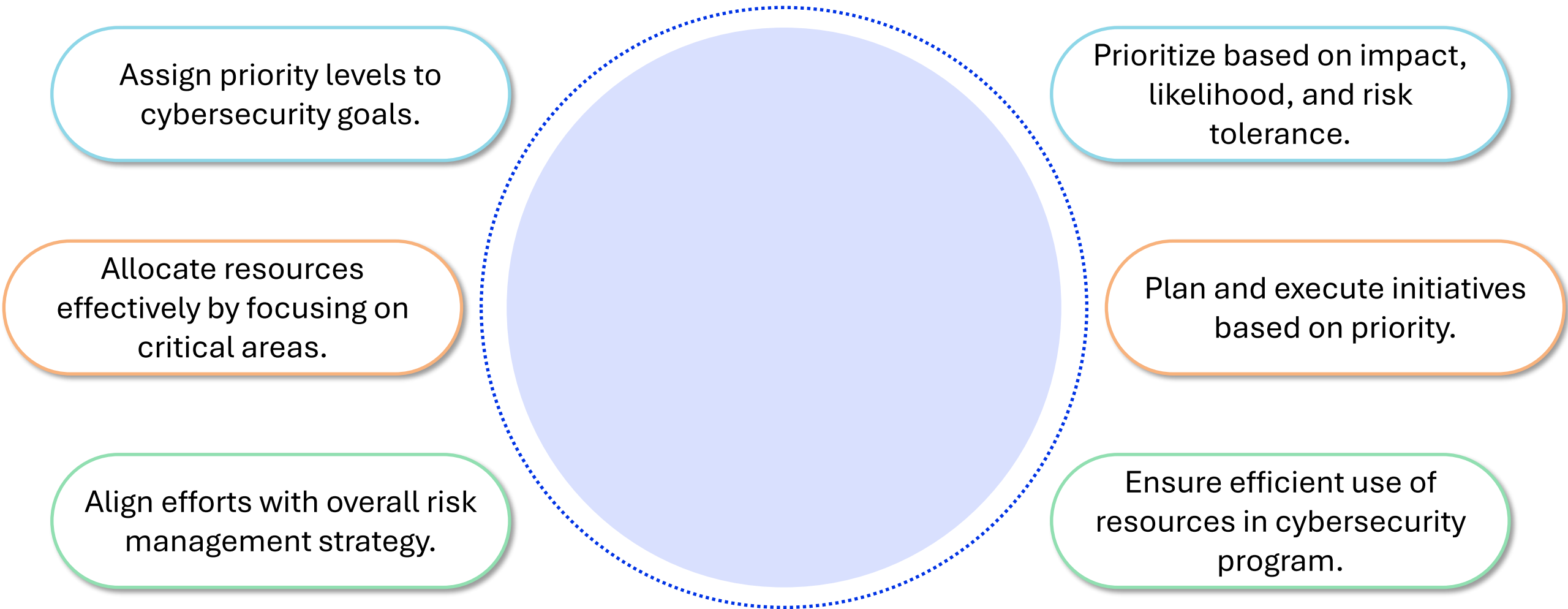
c. Document Current Cybersecurity Practices in the Current Profile columns

CSF Outcome (Function, Category, or Subcategory)	CSF Outcome Description	Included in Profile?	Rationale	Current Cybersecurity Practices
PR.PT-01	Physical devices and systems are protected	Yes	Essential for securing physical assets	Access controls, surveillance
DE.CM-01	Network and system monitoring is implemented	Yes	Critical for early detection of threats	Intrusion detection systems
RS.CO-02	Internal and external stakeholders are notified of incidents	Yes	Important for transparency and compliance	Incident response team
RC.RP-05	The integrity of restored assets is verified	Yes	Ensures restored systems are secure and functional	Restoration testing

d. Outline Cybersecurity Goals and Plans in the Target Profile Columns

CSF Outcome (Function, Category, or Subcategory)	CSF Outcome Description	Target Policies, Processes, and Procedures	Target Internal Practices	Target Roles and Responsibilities	Notes
PR.DS-01	Data-at-rest is protected	Update data storage policies to include advanced encryption	Implement advanced encryption techniques	IT security team responsible for encryption	Plan to complete encryption update by Q3 2024
RS.MI-05	Response plans incorporate lessons learned	Establish a formal process for updating response plans	Regular reviews of incident reports	Incident response team to update plans	Incorporate latest incident findings annually
DE.CM-09	Hardware and software are monitored	Implement comprehensive monitoring policies	Use monitoring tools for real-time analysis	IT team to oversee monitoring activities	Review and update monitoring tools biannually
ID.AM-01	Physical devices and systems are inventoried	Develop and maintain an asset inventory system	Regularly update asset inventory	Asset management team to maintain inventory	Ensure inventory accuracy monthly

e. Use the Priority Field to Note the Importance of Each Goal



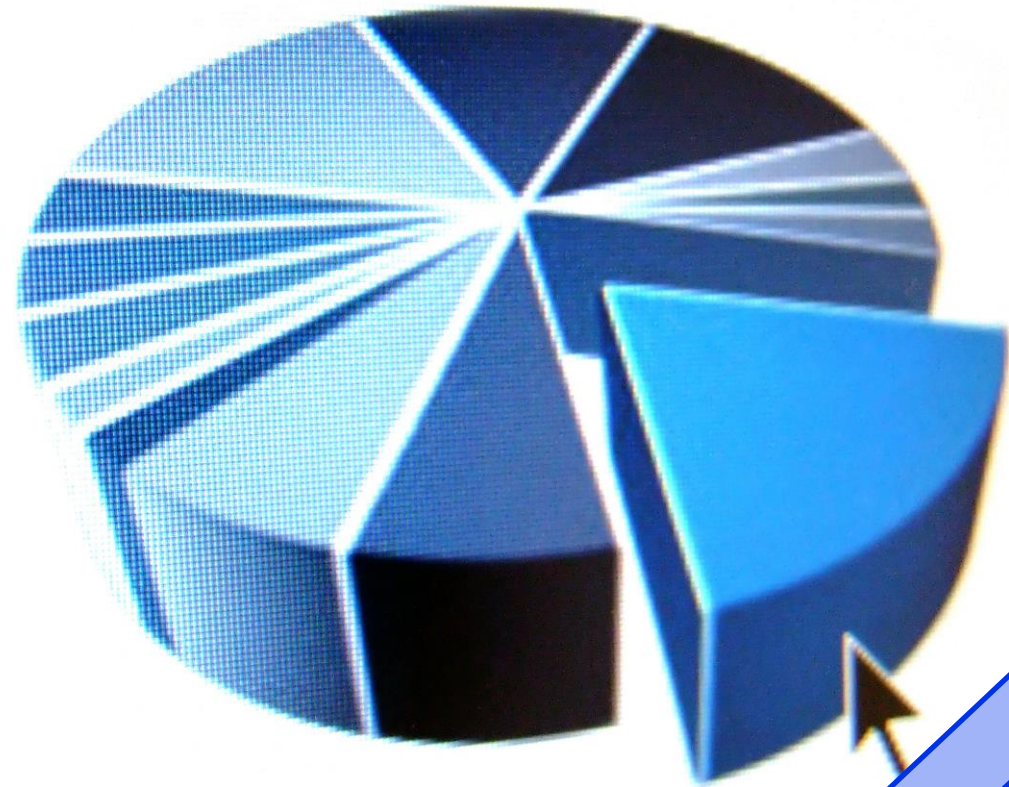
Priorities at GreenLeaf

CSF Outcome (Function, Category, or Subcategory)	CSF Outcome Description	Target Priority	Target Policies, Processes, and Procedures	Target Internal Practices	Target Roles and Responsibilities	Notes
PR.DS-01	Data-at-rest is protected	High	Update data storage policies to include advanced encryption	Implement advanced encryption techniques	IT security team responsible for encryption	Plan to complete encryption update by Q3 2024
RS.MI-05	Response plans incorporate lessons learned	Medium	Establish a formal process for updating response plans	Regular reviews of incident reports	Incident response team to update plans	Incorporate latest incident findings annually
DE.CM-09	Hardware and software are monitored	High	Implement comprehensive monitoring policies	Use monitoring tools for real- time analysis	IT team to oversee monitoring activities	Review and update monitoring tools biannually
ID.AM-01	Physical devices and systems are inventoried	Medium	Develop and maintain an asset inventory system	Regularly update asset inventory	Asset management team to maintain inventory	Ensure inventory accuracy monthly

Step 4:

Analyze Gaps and Create an Action Plan

- Identify differences between Current and Target Profiles.
- Analyze gaps to pinpoint cybersecurity weaknesses.
- Develop a prioritized action plan to address gaps.
- Allocate resources to critical gaps based on impact.
- Enhance cybersecurity posture in a cost-effective manner.



How to Analyse Gaps



Compare current practices to CSF best practices.



Focus on people, process, and technology differences.



Identify gaps with cybersecurity goals in mind.



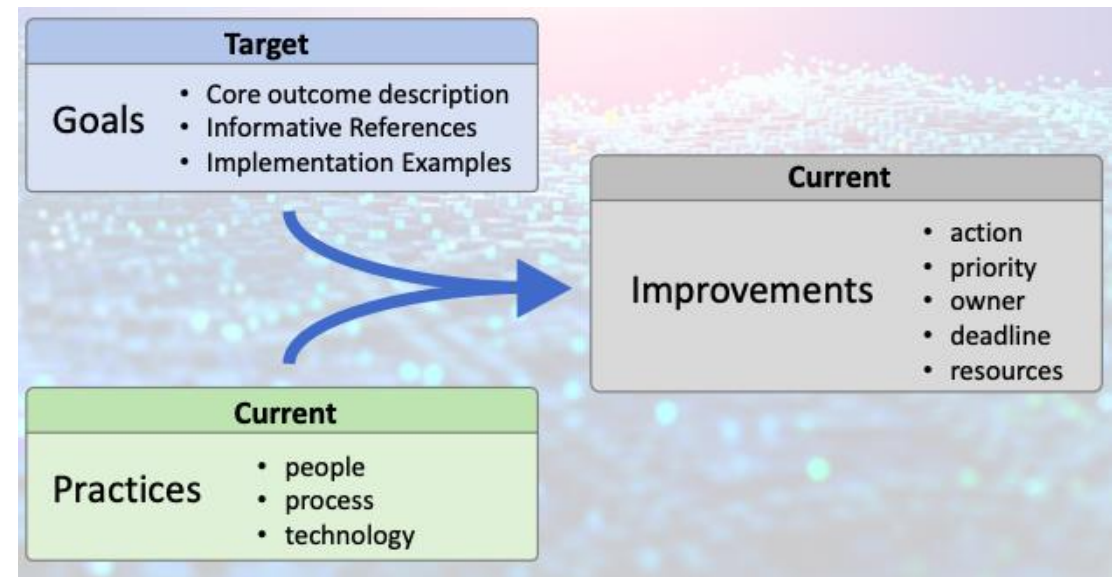
Document differences as candidate improvements for action.

Analysing Gaps at GreenLeaf

Current Practice	CSF Best Practice	Difference	Candidate Improvement
Basic encryption for data-at-rest	Advanced encryption techniques	Encryption level	Implement advanced encryption
Manual incident response plan updates	Formal process for updating response plans	Update process	Establish a formal update process
Periodic monitoring of hardware and software	Real-time analysis using monitoring tools	Monitoring frequency and technology	Implement comprehensive monitoring
Sporadic asset inventory updates	Regularly updated asset inventory system	Update frequency	Develop and maintain an updated system
Limited use of multi-factor authentication (MFA)	Widespread use of MFA	Authentication method	Expand the use of MFA across systems
Ad-hoc cybersecurity training for employees	Regular and structured cybersecurity training	Training frequency and structure	Implement regular training programs
Reactive approach to cybersecurity threats	Proactive threat hunting and analysis	Threat management approach	Develop a proactive threat management plan
Generic cybersecurity policies	Tailored cybersecurity policies for specific risks	Policy specificity	Customize policies to address specific risks

How to Create Action Plans

- Action plan lists pending cybersecurity improvements.
- Consider mission drivers, benefits, risks, and resources.
- Prioritize actions based on potential impact.
- Identify risks associated with each improvement.
- Detail resources required, including staffing and funding.
- Assign priority levels to allocate resources effectively.
- Provide a timeline for each action's implementation.
- Assign ownership for accountability and clear responsibility.
- Establish metrics to measure the success of actions.



Action Plan at GreenLeaf

Improvement Area	Priority	Risks	Required Resources	Timeline	Owner	Success Metrics
Update Encryption Policies	High	Potential downtime during implementation	IT security team, encryption software	Q3 2024	IT Security Manager	Successful implementation without downtime
Enhance Incident Response Plan	Medium	Inadequate training for new procedures	Incident response team, training materials	Q1 2025	Incident Response Coordinator	Reduction in response time to incidents
Implement Comprehensive Monitoring	High	Possible privacy concerns	IT team, monitoring tools	Q2 2025	IT Manager	Increased detection rate of security incidents
Maintain Asset Inventory	Medium	Inaccurate inventory data	Asset management team, inventory management system	Ongoing	Asset Manager	Monthly accuracy check with less than 5% discrepancies

What Best Practices to Use

- Informative References guide organizations in achieving cybersecurity outcomes.
- They connect the CSF Core to standards, guidelines, regulations, and resources.
- Provide insights on meeting CSF Core outcomes effectively.
- Align CSF outcomes with recognized cybersecurity documents for best practices.
- ISO/IEC 27001 specifies requirements for information security management systems.
- It helps organizations secure sensitive information systematically.
- NIST SP 800-53 offers a catalog of security and privacy controls.
- It provides measures to protect information systems from threats.
- Informative References assist in applying relevant security controls for specific challenges.



Best Practices at GreenLeaf

CSF Outcome (Function, Category, or Subcategory)	CSF Outcome Description	Informative Reference	Application at GreenLeaf
PR.AC-1	Access control policies and procedures are established	ISO/IEC 27001:2022 - A.5.15 Access Control, NIST SP 800-53 - AC Family	Access control policy in place; regular training for employees on access control protocols.
PR.IP-1	Data protection policies and procedures are established	ISO/IEC 27001:2022 - A.5.9 Asset Management, NIST SP 800-53 - MP Family	Data classification policy implemented; encryption used for sensitive data.
DE.AE-1	Anomalies and events are detected	NIST SP 800-53 - AU Family, ISO/IEC 27001:2022 - A.8.20 Network Security	Use of SIEM tools for real-time anomaly detection; regular analysis of security logs.
RS.RP-1	Response plan is executed during or after an incident	NIST SP 800-53 - IR Family, ISO/IEC 27001:2013 - A.5.24 Information Security Incident Management	Incident response plan in place; regular drills conducted to test response effectiveness.
RC.IM-1	Recovery plan is developed and implemented	NIST SP 800-53 - CP Family, ISO/IEC 27001:2013 - A.5.30 Information Security Aspects of Business Continuity Management	Recovery plan established for IT systems; regular backup and restoration tests conducted.

How to Implement Best Practices

- Use NIST CSF 2.0 Implementation Examples
- Examples offer notional fulfillment methods
- Not comprehensive or required actions
- Ideas for concrete cybersecurity steps
- Covers various cybersecurity aspects
- Reference Tool for exploration and download
- Customizable to organizational needs

Example of an Implementation Example

An Excerpt from the NIST CSF 2.0 Reference Tool

Subcategory

PR.PS-01: Configuration management practices are applied (formerly PR.IP-01, PR.IP-03, PR.PT-02, PR.PT-03)

Implementation Examples

Ex1: Establish, test, deploy, and maintain hardened baselines that enforce the organization's cybersecurity policies and provide only essential capabilities (i.e., principle of least functionality)

Ex2: Review all default configuration settings that may potentially impact cybersecurity when installing or upgrading software

Step 5:

Implement Action Plan and Update Profile

Step 5a: Implement Action Plan

Implement action plans to enhance cybersecurity.

Use management, programmatic, and technical controls.

Track progress with the Organizational Profile.

Monitor controls and risks with KPIs and KRIs.

Conduct risk assessments for risks beyond tolerance.

Update action plan and profile for high risks.

Create POA&M for gaps with longer timelines.

Use KPIs, KRIs, and POA&Ms for informed decisions.

KPIs/KRIs at GreenLeaf

KPI/KRI	Description	Application at GreenLeaf
KPI: Percentage of Patched Systems	Measures the proportion of systems updated with the latest security patches.	Aim for 95% of systems patched within 7 days.
KRI: Number of Unresolved Incidents	Tracks the count of security incidents that remain open or unresolved.	Keep unresolved incidents under 5 at any time.
KPI: Time to Detect Incidents	The average time taken to detect a security incident from its occurrence.	Reduce detection time to less than 4 hours.
KRI: Frequency of Phishing Attacks	The number of phishing attacks detected per month.	Monitor for any increase in phishing attempts.
KPI: Employee Cybersecurity Training	The percentage of employees who have completed mandatory cybersecurity training.	Ensure 100% employee training completion yearly.
KRI: Data Breach Impact	Measures the extent of data compromised in a breach, such as the number of records or the severity of impact.	Minimize data exposure in breaches.

Risk Assessment at GreenLeaf

Risk Category	Risk Description	Risk Tolerance Level	Assessment Method	Mitigation Plan	Responsible Team
Data Breach	Unauthorized access to sensitive customer data	Low	Regular security audits	Enhance encryption, implement stricter access controls	IT Security Team
Supply Chain Attack	Compromise of third-party vendor leading to system infiltration	Medium	Vendor security evaluations	Strengthen vendor security requirements, conduct audits	Supply Chain Team
Insider Threat	Potential malicious activity from within the organization	Low	Employee monitoring	Implement user behavior analytics, conduct training	Human Resources
Natural Disasters	Damage to physical infrastructure due to natural events	High	Business impact analysis	Develop and test disaster recovery and business continuity plans	Business Continuity Team
Cyber Espionage	Targeted attacks aiming to steal intellectual property	Low	Threat intelligence	Increase network monitoring, collaborate with law enforcement	IT Security Team
Regulatory Compliance	Non-compliance with industry regulations leading to legal penalties	Medium	Compliance audits	Regular review of compliance status, update policies as needed	Compliance Team

Updates to the Action Plan for Risks beyond Risk Tolerance at GreenLeaf

High Risk Area	Action Plan Update	Profile Update
Data Breaches	Implement advanced encryption techniques	Update data storage policies to include advanced encryption
Insider Threats	Enhance employee monitoring and conduct training	Strengthen access controls and user behavior analytics
Cyber Espionage	Increase network monitoring and collaborate with law enforcement	Enhance network security measures and intelligence sharing with law enforcement

Updates to the Organizational Profile for Risks beyond Risk Tolerance at GreenLeaf

CSF Outcome (Function, Category, or Subcategory)	CSF Outcome Description	Rationale	Current Priority	Current Status	Updated Priority	Updated Status	Notes
PR.AC-1	Access control policies and procedures	Risks from unauthorized access exceed tolerance	High	Partially Implemented	High	Fully Implemented	Strengthen access control measures
DE.CM-7	Security continuous monitoring capabilities	Inadequate monitoring capabilities for detecting advanced threats	Medium	Partially Implemented	High	Fully Implemented	Enhance monitoring tools and techniques
PR.IP-8	Data backup and recovery	Ineffective backup and recovery processes for critical data	Medium	Partially Implemented	High	Fully Implemented	Implement robust backup and recovery solutions
RS.CO-1	Response planning and coordination	Lack of coordination in incident response leading to delayed containment	Medium	Partially Implemented	High	Fully Implemented	Establish a centralized incident response coordination team



KPI

Updating your Profile

- Implement Action Plan activities for ongoing risk management.
- Leverage Risk Tolerance statements in Risk Assessments.
- Assess likelihood and impact to gauge Action Plan effectiveness.
- Use KPIs and KRIs for risk monitoring.
- Update Organizational Profile based on changes in risks.

Updating GreenLeaf Profile

GreenLeaf updates Organizational Profile regularly.

Action plan implemented focusing on high-risk areas.

Conducts risk assessments in line with SP 800-30.

Uses risk tolerance statements to evaluate risks.

Monitors control effectiveness with KPIs and KRIs.

Updates Profile based on changing risks and impacts.

Ensures cybersecurity efforts align with strategic objectives.

What we Learned

Organizational Profile:

CSF outcomes for a specific organization.

Community Profile:

CSF outcomes for multiple organizations.

Current Profile:

Outcomes an organization currently achieves.

Target Profile:

Desired cybersecurity outcomes for an organization.

Gap Analysis:

Identifies differences between Current and Target Profiles.

Informative References:

Best practices for implementing CSF outcomes.

Implementation Examples:

Notional ways to achieve CSF Subcategories.

Action Plan:

Addresses gaps, moves toward Target Profile.

What's Next

- Familiarize with NIST CSF Organizational Profile template.
- Explore relevant NIST Community Profiles.
- Determine needed number of Organizational Profiles.
- Inventory cybersecurity requirements.
- Prioritize CSF outcomes in Profiles.
- Assess Current Profile.
- Learn about Informative References.
- Continuously improve cybersecurity program.

Conclusion

- Completed NIST CSF 2.0 course.
- Tailored CSF to organizational needs.
- Prioritized cybersecurity outcomes.
- Developed actionable plans.
- Emphasized continuous assessment.
- Updated cybersecurity program.
- Fostered cybersecurity resilience.
- Applied NIST CSF principles.

