Exploring NIST Cybersecurity Framework 2.0

The Institute of Internal Auditors

BDO

With You Today

JAMEY LOUPE
Assurance Market Leader
Risk Advisory Services
BDO USA

713-407-3935
jloupe@bdo.com

TIM SEIGLER
Assurance Principal
Third Party Attestation
BDO USA

770-560-9752
tseigler@bdo.com

Learning Objectives

1

NIST CSF 2.0 Overview and the changes from NIST 1.1 to NIST 2.0

2

Impact of Third-Party Service providers and cybersecurity to have “layers” of security to reduce risk

3

Internal Audit’s role in responding to business email compromises

Agenda for Today

- A History and Overview of NIST
- Need for NIST 2.0
- Differences between NIST 1.1 and NIST 2.0
- Detailed Insight into new NIST 2.0 Function
- Leveraging NIST 2.0 to Address Third Party Risk (Defense in Depth)

A Legacy of Excellence

NIST AND ITS CONTRIBUTION

- Established in 1901 by the U.S. Department of Commerce
- Focuses on scientific and technological research and standards development
- Plays a vital role in promoting cybersecurity best practices globally

NIST Cybersecurity Framework (CSF) 1.0

THE GENESIS

- Introduced NIST CSF v1.0 in 2014 following Executive Order 13636
- Provided a voluntary, risk-based approach to cybersecurity
- Offered a core framework with five functions: Identify, Protect, Detect, Respond, and Recover
- Geared towards critical infrastructure sectors initially

Evolution of the NIST Cybersecurity Framework (CSF)

UPDATES AND IMPROVEMENTS

- Engage with industry, academia, and government stakeholders for continuous improvement
- Increase and facilitate international adoption and integration with other Standards
- Released NIST CSF v1.1 in April 2018 with major addition addressing Cybersecurity Supply Chain Risk Management
- Improve usability and relevance through clarifications and enhancements across the framework

The Everchanging Landscape

THE NEED FOR NIST CSF 2.0

- Evolving cyber threats demanded a broader and more adaptable framework
- Increased focus on risk management for all organizations, regardless of size or sector
- Recognition of the growing importance of governance in cybersecurity strategy

Introducing NIST CSF 2.0

A CLOSER LOOK

- Expands the core framework to include a sixth function: Govern
- Offers comprehensive guidance with the use of implementation examples
- Continues to offer a voluntary, risk-based approach
- Provides a flexible framework that can be customized based on organizational needs
- Emphasizes the importance of continuous improvement
- Improves ease of use and accessibility (open source, material, different languages)

Framework Core Changes

NIST CSF V1.1 TO V2.0:

CSF v1.1	
5	Functions
23	Categories
108	Subcategories

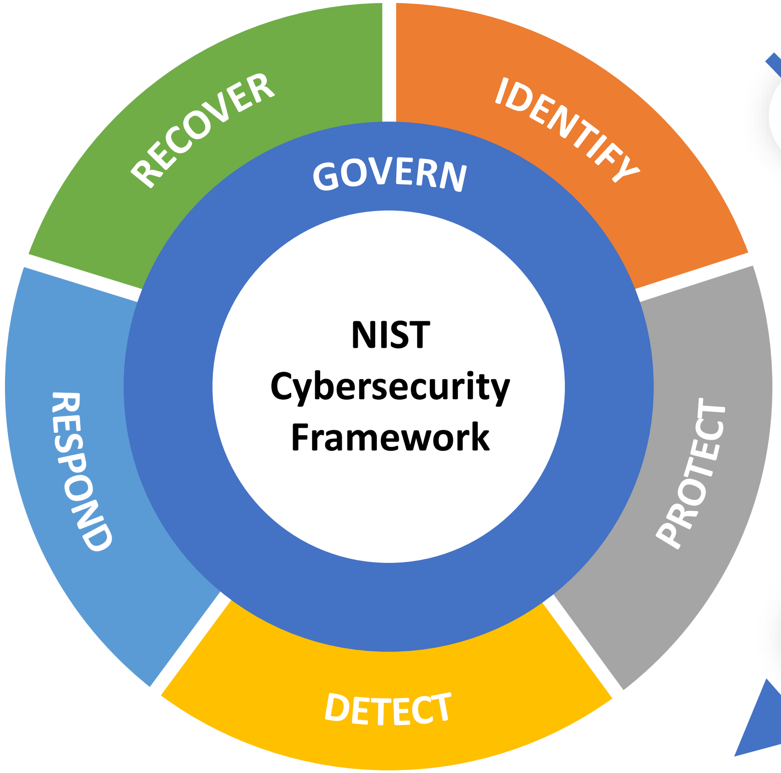
CSF v2.0	
6	Functions
22	Categories
106	Subcategories

Function	Category	ID
IDENTIFY	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
PROTECT	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AC
	Data Security	PR.DS
	Information Protection Processes and Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
DETECT	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
RESPOND	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
RECOVER	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Function	Category	ID
GOVERN (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
IDENTIFY (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
PROTECT (PR)	Identity Management, Authentication and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
DETECT (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
RESPOND (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
RECOVER (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Source: The NIST Cybersecurity Framework (CSF) 2.0 ▶

Applying NIST CSF to Mature your Cybersecurity Control Environment



1. Scope the Organization Profile
2. Gather needed information
3. Create the Organization Profile
4. Analyze gaps and create an action plan
5. Implement action plan and update profile

REPEAT …

Source: The NIST Cybersecurity Framework (CSF) 2.0 ▶

The Institute of Internal Auditors
Elevating Impact

Applying NIST CSF to Mature your Cybersecurity Control Environment

- **CSF Organizational Profile** describes organization's current or target cybersecurity posture in alignment with the CSF Core (Functions, Categories, and Subcategories)
  - **Current Profile** = Core outcomes currently achieved
  - **Target Profile** = Desired outcomes
- **Scope** defines facts and assumptions on which Organizational Profile(s) are based
  - Scope of Organizational Profile can cover entire organization or may be limited to division, business unit, program, system(s), etc.

- **Information gathered** to create profiles should be relevant to scope
  - **CSF Tiers** can be used to inform on Current and Target Profiles (i.e., rating) by NIST CSF Categories and Subcategories
- **Gaps** exist where differences between Current and Target Profiles are identified, and should be prioritized for resolution via formal action plans (e.g., POA&M)
- **Implement action plans** and update Organizational Profile as needed

Source: The NIST Cybersecurity Framework (CSF) 2.0 ▶

Applying NIST CSF

ADDITIONAL CONSIDERATIONS

▶ Organizations should leverage **NISTCSF 2.0 Resources** including:

- NIST CSF 2.0 Reference Tool - Allows download of NIST CSF 2.0 Core (Functions, Categories, Subcategories) with implementation examples
- Quick Start Guides - Organizational Profile templates and guidance on integrating CSF with ERM, applying CSF tiers to create Organizational Profiles, using CSF to improve C-SCRM processes, and specific considerations for small businesses

▶ Organizations may also integrate NIST CSF 2.0 with **other frameworks, models, and practices** including:

- CMMI (for alternative maturity scoring view)
- NIST SP 800-30 Guide for Conducting Risk Assessments
- NIST SP 800-37 Risk Management Framework (RMF)
- NIST Privacy Framework and Privacy Risk Assessment Methodology (PRAM)
- NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices

Source: The NIST Cybersecurity Framework (CSF) 2.0 ▶

Applying NIST CSF

ADDITIONAL CONSIDERATIONS

Scoring Methodology

- Determine scores (i.e., ratings) at the NIST CSF Subcategory level
- May aggregate scores at NIST CSF Category or Function level
- May customize scoring criteria by applying additional factors with weighting based on importance (e.g., process, policy, documentation, automation)
- Methodology should be applied **consistently**

Risk Considerations

- Risk may be used to inform determination of Target Profile
- Risk determination may be based on results of previous internal risk assessments or third-party assurance audits or assessments (using NIST or other frameworks)
- Risk should also be considered when prioritizing corrective actions to address gaps

Source: The NIST Cybersecurity Framework (CSF) 2.0 ▶

Applying NIST CSF Scorecard Example

NIST CSF Function	NIST CSF Tier	CMMI Level	NIST CSF Category	Current Profile	Target Profile	Risk Impact
GOVERN (GV)	Tier 2: Risk Informed	Level 2: Managed	Organizational Context (GV.OV)	2.5	3.0	Moderate
			Risk Management Strategy (GV.RM)	3.0	3.5	Low
			Roles, Responsibilities, and Authorities (GV.RR)	2.5	3.0	Moderate
			Policy (GV.PO)	3.0	3.5	Low
			Oversight (GV.OV)	3.0	4.0	Moderate
			Cybersecurity Supply Chain Risk Management (GV.SC)	2.0	3.5	High
IDENTIFY (ID)	Tier 2: Risk Informed	Level 2: Managed	Asset Management (ID.AM)	2.5	3.5	Moderate
			Risk Assessment (ID.RA)	2.5	3.0	Low
			Improvement (ID.IM)	2.0	4.0	High
PROTECT (PR)	Tier 2: Risk Informed	Level 2: Managed	Identity Management, Authentication, and Access Control (PR.AA)	2.2	3.0	Moderate
			Awareness and Training (PR.AT)	2.75	4.0	Moderate
			Data Security (PR.DS)	2.75	3.0	Low
			Platform Security (PR.PS)	1.9	3.0	Moderate
			Technology Infrastructure Resilience (PR.IR)	2.2	4.0	High
DETECT (DE)	Tier 2: Risk Informed	Level 2: Managed	Continuous Monitoring (DE.CM)	2.5	3.0	Low
			Adverse Event Analysis (DE.AE)	2.75	4.0	High
RESPOND (RS)	Tier 3: Repeatable	Level 3: Defined	Incident Management (RS.MA)	3.25	4.0	Moderate
			Incident Analysis (RS.AN)	2.75	3.0	Moderate
			Incident Response Reporting and Communication (RS.CO)	3.0	3.0	Low
			Incident Mitigation (RS.MI)	3.0	3.5	Moderate
RECOVER (RC)	Tier 2: Risk Informed	Level 2: Managed	Incident Recovery Plan Execution (RC.RP)	2.75	3.0	Low
			Incident Recovery Plan Communication (RC.CO)	2.25	3.0	Moderate

Cyber Assessment Methodology

Offering comprehensive cyber risk assessments, we help organizations understand the current state of its cyber program, identify potential gaps and risks, remediate those gaps and risks, and ultimately implement an effective cybersecurity framework.

PROJECT DEFINITION

- Identify scope of work with client
- Development of SOW and client negotiations

PROJECT PREPARATION

- Kick-off presentation
- Validate and customize questionnaire/ evidence request list
- Identify individual(s) that will complete self-assessment questionnaire
- Identify department(s)/ individual(s) to interview as part of data gathering

DATA GATHERING

- Self-assessment questionnaire collection
- Evidence request collection
- Key personnel interviews

DATA ANALYSIS

- Observe strengths and gaps based on data gathered
- Validation of control implementation through guided workshops
- Scoring subcategories and categories
- Risk analysis based on observations and relevant industry threats

RISK VALIDATION

- Current state report
- Combined state report
- Modification and updates based on client feedback
- Initial development of remediation options

FINDINGS PRESENTATION

- Presentation of the findings within the assessments
- Identify risk level by categories

NIST 2.0 GOVERN Function Control Application

Category	Subcategory ID	Subcategory Description	Implementation Examples
GV.RM: Risk Management Strategy The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions	**GV.RM-04**	Strategic direction that describes appropriate risk response options is established and communicated	**1st:** 1st Party Risk **Ex1:** Specify criteria for accepting and avoiding cybersecurity risk for various classifications of data **Ex2:** Determine whether to purchase cybersecurity insurance **Ex3:** Document conditions under which shared responsibility models are acceptable (e.g., outsourcing certain cybersecurity functions, having a third party perform financial transactions on behalf of the organization, using public cloud-based services)
	GV.RM-05	Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	**1st:** 1st Party Risk **3rd:** 3rd Party Risk **Ex1:** Determine how to update senior executives, directors, and management on the organization's cybersecurity posture at agreed-upon intervals **Ex2:** Identify how all departments across the organization - such as management, operations, internal auditors, legal, acquisition, physical security, and HR - will communicate with each other about cybersecurity risks

NIST 2.0 GOVERN Function Control Application

Category	Subcategory ID	Subcategory Description	Implementation Examples
GV.RM: Risk Management Strategy The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions	GV.RM-06	A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	1st: 1st Party Risk Ex1: Establish criteria for using a quantitative approach to cybersecurity risk analysis, and specify probability and exposure formulas Ex2: Create and use templates (e.g., a risk register) to document cybersecurity risk information (e.g., risk description, exposure, treatment, and ownership) Ex3: Establish criteria for risk prioritization at the appropriate levels within the enterprise Ex4: Use a consistent list of risk categories to support integrating, aggregating, and comparing cybersecurity risks
	GV.RM-07	Strategic opportunities (i.e., positive risks) are identified and included in organizational cybersecurity risk discussions	1st: 1st Party Risk Ex1: Define and communicate guidance and methods for identifying opportunities and including them in risk discussions (e.g., strengths, weaknesses, opportunities, and threats [SWOT] analysis) Ex2: Identify stretch goals and document them Ex3: Calculate, document, and prioritize positive risks alongside negative risks

NIST 2.0 GOVERN Function Control Application

Category	Subcategory ID	Subcategory Description	Implementation Examples
GV.OV: Oversight Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy	GV.OV-01	Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction	1st: 1st Party Risk Ex1: Measure how well the risk management strategy and risk results have helped leaders make decisions and achieve organizational objectives Ex2: Examine whether cybersecurity risk strategies that impede operations or innovation should be adjusted
	GV.OV-02	The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	1st: 1st Party Risk Ex1: Review audit findings to confirm whether the existing cybersecurity strategy has ensured compliance with internal and external requirements Ex2: Review the performance oversight of those in cybersecurity-related roles to determine whether policy changes are necessary Ex3: Review strategy in light of cybersecurity incidents
	GV.OV-03	Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	1st: 1st Party Risk Ex1: Review key performance indicators (KPIs) to ensure that organization-wide policies and procedures achieve objectives Ex2: Review key risk indicators (KRIs) to identify risks the organization faces, including likelihood and potential impact Ex3: Collect and communicate metrics on cybersecurity risk management with senior leadership

The Institute of Internal Auditors
Elevating Impact

Cybersecurity to Have "Layers" of Security to Reduce Risk

IMPACT OF THIRD-PARTY SERVICE PROVIDERS

Impact of Third-Party Service Providers on Cybersecurity

Increased Attack Surface

- Dependency on Third Parties
- Supply Chain Attacks

Data Privacy and Compliance

- Data Handling
- Compliance Risks

Security Practices and Policies

- Varying Security Standards
- Due Diligence

Incident Response and Recovery

- Coordination
- Responsibility and Accountability

Importance of Having "Layers" of Security (Defense in Depth)

Multiple Barriers

- Redundancy
- Complexity for Attackers

Comprehensive Protection

- Diverse Threats
- Holistic Approach

Examples of Security Layers

- Physical Security
- Network Security
- Endpoint Security
- Application Security
- Data Security
- User Security

Resilience and Recovery

- Incident Containment
- Business Continuity

The Institute of Internal Auditors
Elevating Impact

Responding to Business Email Compromises

Understanding Business Email Compromise (BEC)

BEC is a type of cybercrime where attackers gain access to a business email account and use it to deceive the company or its employees.

HOW DO COMPROMISES OCCUR?

- Phishing Attacks
- Malware
- Email Spoofing
- Social Engineering

IMPACT ON THE ORGANIZATION

- Financial Loss
- Reputational Damage
- Operational Disruption
- Legal Consequences

TIME TO IDENTIFY COMPROMISE

- **Average Time:** It typically takes organizations **77 days** to identify a BEC attack
- **Detection Challenges:** Difficulty in recognizing fraudulent emails and the sophisticated nature of attacks contribute to delayed detection

Understanding Business Email Compromise (BEC)

INTERNAL AUDIT'S ROLE IN THE GOVERN AND IDENTIFY FUNCTION

- **Asset Management:** Ensure all email systems and related assets are identified and documented
- **Business Environment:** Understand the organization's role in the supply chain and its exposure to BEC
- **Governance:** Evaluate policies, procedures, and governance structures related to email security
- **Risk Assessment:** Conduct regular risk assessments focusing on email systems and potential BEC threats

Understanding Business Email Compromise (BEC)

INTERNAL AUDIT'S ROLE IN THE DETECT AND PROTECT FUNCTION

- **Access Control:** Verify that access to email systems is restricted and monitored
- **Awareness and Training:** Ensure employees are trained on recognizing and responding to BEC attempts
- **Data Security:** Assess the implementation of encryption and other data protection measures
- **Maintenance:** Review the patch management process to ensure email systems are up-to-date
- **Anomalies and Events:** Monitor for unusual email activity that could indicate a BEC attempt
- **Continuous Monitoring:** Ensure continuous monitoring tools are in place and effective
- **Detection Processes:** Evaluate the effectiveness of detection processes and tools
- **Security Testing:** Conduct regular penetration testing and vulnerability assessments

Understanding Business Email Compromise (BEC)

INTERNAL AUDIT'S ROLE IN THE RESPOND AND RECOVER FUNCTIONS

- **Response Planning:** Ensure there is a clear, documented response plan for BEC incidents
- **Communications:** Verify that communication protocols are in place for notifying stakeholders
- **Analysis:** Review the incident analysis process to ensure root causes are identified
- **Mitigation:** Assess the effectiveness of actions taken to mitigate the impact of BEC incidents
- **Recovery Planning:** Ensure recovery plans are in place and regularly tested
- **Improvements:** Verify that lessons learned from BEC incidents are used to improve processes
- **Communications:** Ensure there are plans for communicating recovery efforts to stakeholders
- **Recovery Activities:** Review the effectiveness of recovery activities and their alignment with business continuity plans

Understanding Business Email Compromise (BEC)

SUMMARY

- **Proactive Role:** Internal Audit plays a critical role in identifying, protecting, detecting, responding to, and recovering from BEC incidents
- **Continuous Improvement:** Regular assessments and improvements are essential to stay ahead of evolving threats
- **Collaboration:** Effective response to BEC requires collaboration across the organization

Questions?