



You make **possible**



# Cyber Best Practices

Introduction to the  
NIST Cybersecurity Framework

Steve Caimi, Cisco Security  
BRKSEC-1021

**Cisco** *live!*  
June 9-13, 2019 • San Diego, CA

#CLUS



# Abstract

## How can we efficiently and effectively manage cyber risk?

That's the fundamental question in cybersecurity today. It's so hard to answer because every organization has different levels of cyber awareness, risk tolerance, available budget, internal capability, and overall maturity. But it's also so critical: Every cyber investment your organization makes in people, process, and technology should be laser-focused on mitigating your risk where it matters the most.

The next question is obvious: What resources and best practices are available to help us along the path to efficient and effective cyber risk management? Well, we have great news. Join us in this highly engaging session where we'll discuss the Cybersecurity Framework (CSF) from the National Institute of Standards and Technology (NIST). First we'll give the big picture, and then we'll drill down into the just right level of detail so that you can learn and apply the NIST CSF right away. Next we'll introduce the Baldrige Cybersecurity Excellence Builder (CEB) that works together with the NIST CSF to help you have the right conversations in your organization.

Make the most of your cyber investments by registering for our session today.

# Cisco Webex Teams

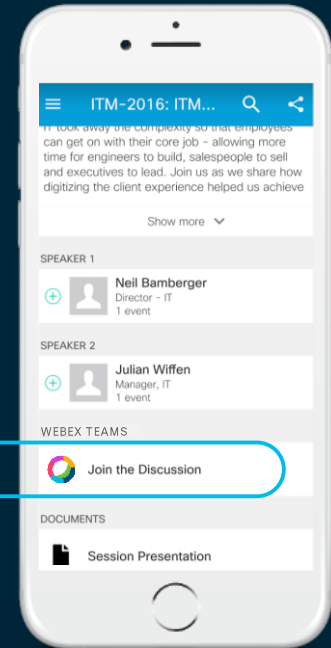
## Questions?

Use Cisco Webex Teams to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install Webex Teams or go directly to the team space
- 4 Enter messages/questions in the team space

Webex Teams will be moderated by the speaker until June 16, 2019.



[cs.co/ciscolivebot#BRKSEC-1021](https://cs.co/ciscolivebot#BRKSEC-1021)

# Agenda

- The importance of a cyber risk management mindset
- Why the NIST Cybersecurity Framework (CSF) matters to you
- A close look at the NIST CSF and how it works
- Use the Baldrige Cybersecurity Excellence Builder
- Get the most from best practices in your organization
- Conclusion

# Complete your online session evaluation



## It's important





**National Institute of  
Standards and Technology**  
U.S. Department of Commerce

- Non-regulatory agency of the US Department of Commerce
- Develops and promotes measurement, standards and technology to enhance productivity, facilitate trade, and improve the quality of life

## Primary Research Areas

- ☒ IT and Cybersecurity
- ☐ Advanced Manufacturing
- ☐ Healthcare
- ☐ Forensic Science
- ☐ Disaster Resilience
- ☐ Cyber-Physical Systems
- ☐ Advanced Communications

# The importance of a risk management mindset





# Gym Locker Security

**What do you think  
of this approach?**

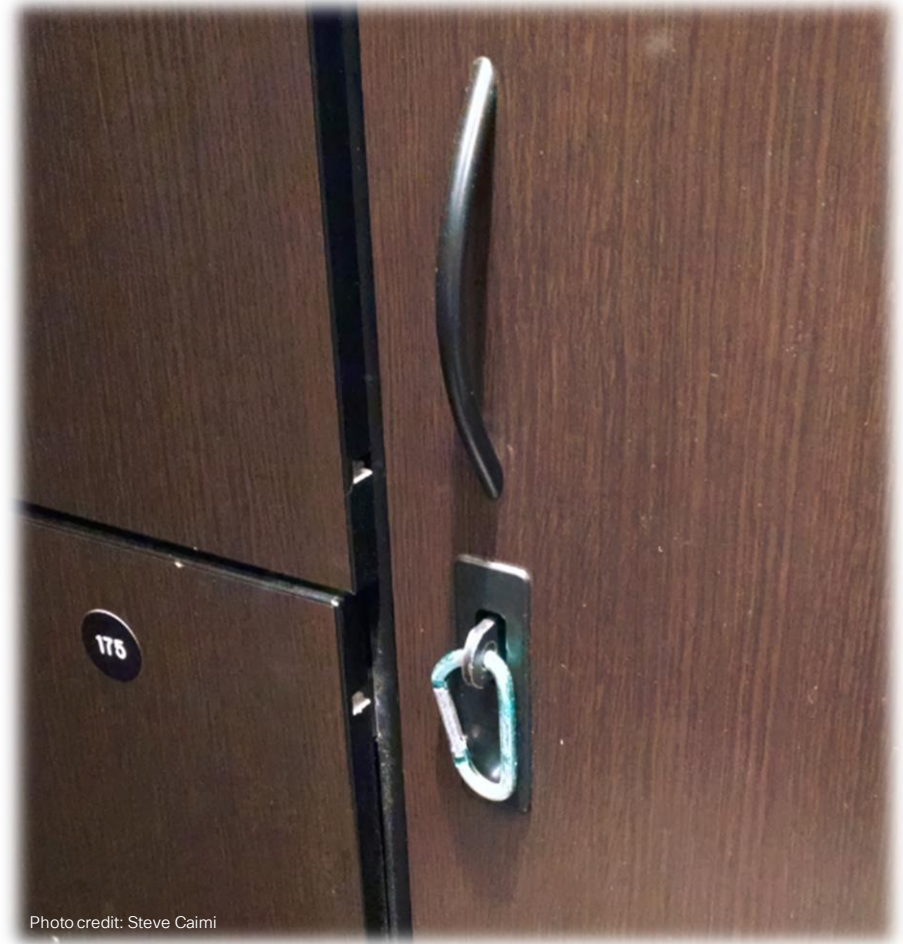


Photo credit: Steve Caimi

# Risk Management Process

## Frame

Establish a Risk Context

1

## Assess

Threats, Vulnerabilities,  
Harm, Likelihood

2

## Monitor

Things Change!

4

## Respond

Accept, Avoid, Mitigate,  
Transfer, or Share

3

Source: NIST SP 800-39, "Managing Information Security Risk"

# Which insurance plan do you choose?



## 2014 Honda Accord

Book Value: \$10,000

Plan	Coverage Option	Premium
1	Liability Only	\$300
2	Liability + Comprehensive	\$400
3	Liability + Comprehensive + Collision	\$700

# Investment Strategies



Source: NIST SP 800-39, "Managing Information Security Risk"

- Significant role in organizational risk management efforts
- Recognize that there is a **finite amount of resources** available to invest in effectively managing risk

# Really bad technology jokes

Ones you may never have heard. And may never want to hear again.

What do you call the revised dress code at the high-tech law office?

A firmware update

Why the NIST CSF  
matters to you



# Cybersecurity Goals

**C**

**Confidentiality**

**I**

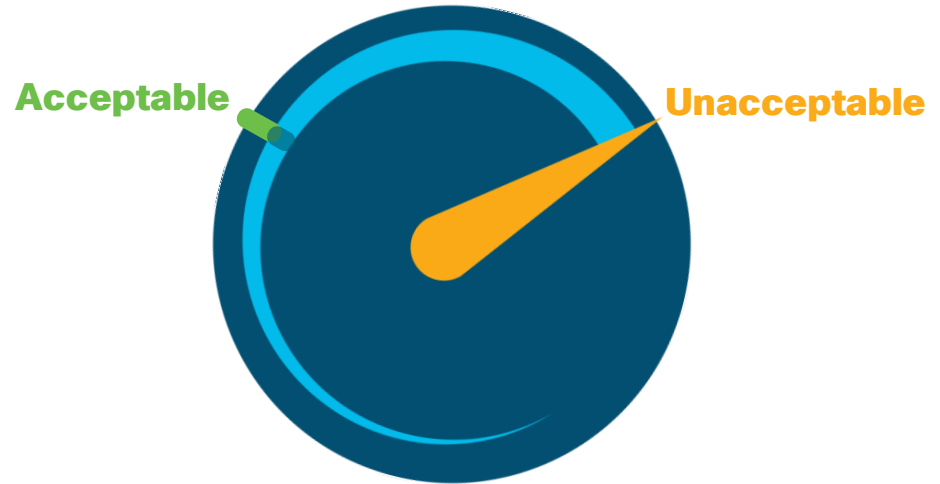
**Integrity**

**A**

**Availability**

How can we  
**efficiently** and **effectively**  
manage our cyber risk?

## The Cyber Question





# Cyber Answer(s)



## National Institute of Standards and Technology (NIST)

NIST Cybersecurity Framework, NIST Risk Management Framework  
[www.nist.gov](http://www.nist.gov)



## Center for Internet Security (CIS)

CIS Controls  
[www.cisecurity.org](http://www.cisecurity.org)



## International Organization for Standardization (ISO)

ISO/IEC 27000 family  
[www.iso.org](http://www.iso.org)



## ISACA

COBIT 5 Framework  
[cobitonline.isaca.org](http://cobitonline.isaca.org)

**NIST**

Information Technology Laboratory

**COMPUTER SECURITY RESOURCE CENTER****CSRC**

Projects

Publications +

Topics +

News &amp; Updates

Events

Glossary

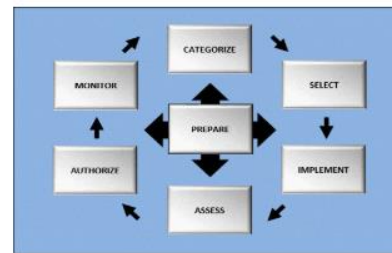
About CSRC +



NIST UPDATES ITS COMBINATORIAL  
COVERAGE MEASUREMENT TOOL



USABLE CYBERSECURITY RESEARCH AT NIST

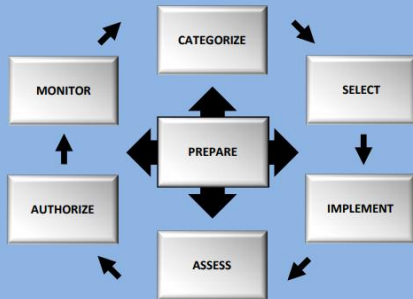


NIST UPDATES THE RISK MANAGEMENT  
FRAMEWORK (SP 800-37 REV. 2)

For 20 years, the **Computer Security Resource Center (CSRC)** has provided access to NIST's cybersecurity- and information security-related **projects, publications, news** and **events**. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

# NIST Frameworks

## Risk Management Framework (RMF)



NIST SP 800-37

## Cybersecurity Framework (CSF)



## NICE Cybersecurity Workforce Framework (NCWF)



NIST SP 800-181

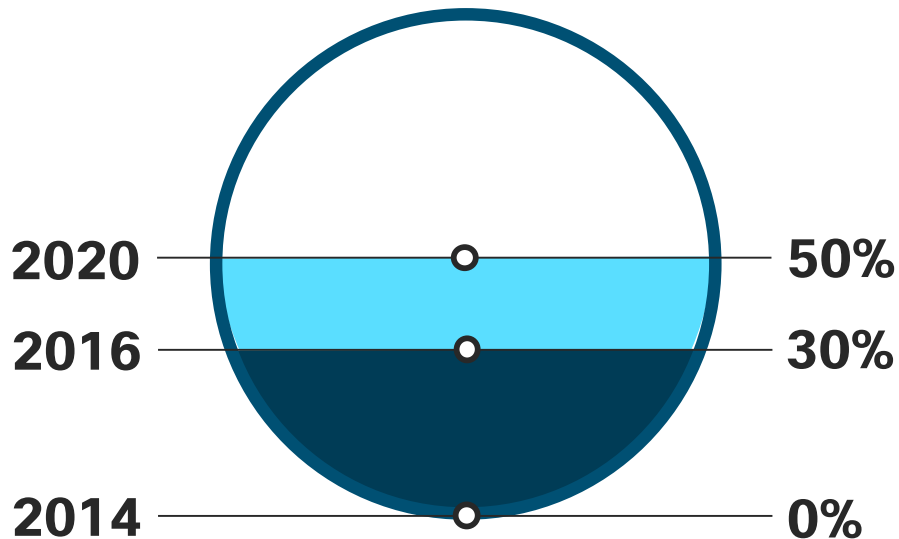
# Not just about technology



# Not just for the US government

## Gartner®

Source: Cybersecurity "Rosetta Stone" Celebrates Two Years of Success  
<https://www.nist.gov/news-events/news/2016/02/cybersecurity-rosetta-stone-celebrates-two-years-success>



# Not just for the US

Japanese translation by  
Information-technology  
Promotion Agency



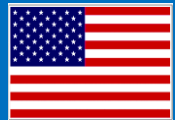
Bermuda uses it within  
government and  
recommends it to industry

Italian translation and  
adaptation within Italy's  
National Framework for  
Cybersecurity



Focus of ISO/IEC

Hebrew translation and  
adaptation by  
Government of Israel



Required\* in the US  
federal government

Executive Order 13800 (May 2017)

# Why the NIST CSF matters to you

- **You can** skip the scare tactics and FUD
- **You can** make the most of what you have
- **You can** focus on the things that really matter
- **You can** make the case for more funding
- **You can** protect your reputation
- **You can** demonstrate due diligence



# How about a million more reasons?



## A FRAMEWORK FOR CYBERSECURITY

By **Scott Schlimmer**, Contributor, CSO | APRIL 19, 2018 11:36 AM PT

Opinions expressed by ICN authors are their own.

Source: CSO Online

<https://www.csoonline.com/article/3268937/implementing-the-nist-cybersecurity-framework-could-be-worth-at-least-1-4m-to-your-business.html>

### OPINION

## Implementing the NIST cybersecurity framework could be worth at least \$1.4m to your business

While there are many other frameworks available, the NIST CSF provides a nationally recognized guideline as you scale your business and cybersecurity program.



# Really bad technology jokes

Ones you may never have heard. And may never want to hear again.

Where do you dispose of old Linux servers that reach End of Life?

The core dump

# A close look at the NIST CSF and how it works



# NIST CSF Origins



## Improving Critical Infrastructure Cybersecurity

### Executive Order 13636

February 2013

“It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a **cyber environment** that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.”

# NIST CSF Origins

v**1.1**

**Apr 2018**

v**1.0**

**Feb 2014**

**EO**

13636

**Feb 2013**

Cisco *live!*

## Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018



# NIST CSF Highlights



- Common cybersecurity language
- Leverages existing best practices
- Simple, flexible, and global
- Not a compliance mandate!
- Freely available to everyone
- Risk-based investment decisions



Framework  
Core



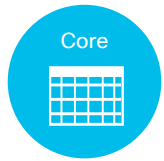
Framework  
Tiers



Framework  
Profiles

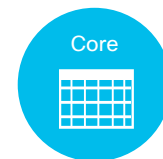
**NIST**  
**CSF Components**

# Framework Core



Functions	Categories	Subcategories	Informative References

# Functions

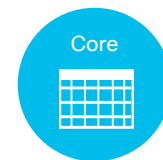


## ● Functions

ID	● <b>Identify</b>	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities
PR	● <b>Protect</b>	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services
DE	● <b>Detect</b>	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event
RS	● <b>Respond</b>	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event
RC	● <b>Recover</b>	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event

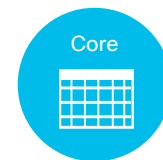


# Categories



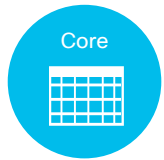
Function	● Categories		
Identify	ID.AM	<b>Asset Management (ID.AM-1)</b>	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
	ID.BE	<b>Business Environment</b>	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
	ID.GV	<b>Governance</b>	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cyber risk.
	ID.RA	<b>Risk Assessment</b>	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals).
	ID.RM	<b>Risk Management Strategy</b>	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

# Subcategories



Function	Category	● Subcategories	
Identify	Asset Management	ID.AM-1	Physical devices and systems within the organization are inventoried
		ID.AM-2	Software platforms and applications within the organization are inventoried
		ID.AM-3	Organizational communication and data flows are mapped
		ID.AM-4	External information systems are catalogued
		ID.AM-5	Resources (hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value
		ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (suppliers, customers, partners) are established

# Informative References



Function	Category	Subcategory	● Informative References
Identify	Asset Management	Physical device inventories	<ul style="list-style-type: none"><li>• CIS CSC 1</li><li>• COBIT 5 BAI09.01, BAI09.02</li><li>• ISA 62443-2-1:2009 4.2.3.4</li><li>• ISA 62443-3-3:2013 SR 7.8</li><li>• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2</li><li>• NIST SP 800-53 Rev. 4 CM-8, PM-5</li></ul>

## International Standards References

- Center for Internet Security (CIS)
- Control Objectives for Information and Related Technology (COBIT)
- International Society of Automation (ISA)
- International Organization for Standardization (ISO)
- NIST Special Publication 800-53



Framework  
Core



Framework  
Tiers



Framework  
Profiles

**NIST**  
**CSF Components**

# Framework Tiers



4

## **Adaptive**

Practices fully established and continuously improved

3

## **Repeatable**

Practices approved and established by organizational policy

2

## **Risk Informed**

Practices approved but not completely established by policy

1

## **Partial**

Informal, ad hoc, reactive responses



Framework  
Core



Framework  
Tiers



Framework  
Profiles

**NIST**  
**CSF Components**

# Framework Profiles



**The alignment of the Framework core with an organizations business requirements, risk tolerance, and resources**

- Describes the current state and desired future state
- Reveals gaps that can flow into action plan development
- Facilitates a roadmap for reducing cybersecurity risk



Framework  
Core



Framework  
Tiers



Framework  
Profiles

**NIST**  
**CSF Components**



Functions		Categories	
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management, Authentication and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

# High Level View



**All Categories**

Functions		Categories		People	Process	Technology
ID	Identify	ID.AM	Asset Management	✓	✓	✓
		ID.BE	Business Environment	✓	✓	X
		ID.GV	Governance	✓	✓	X
		ID.RA	Risk Assessment	✓	✓	✓
		ID.RM	Risk Management Strategy	✓	✓	X
		ID.SC	Supply Chain Risk Management	✓	✓	X
PR	Protect	PR.AC	Identity Management, Authentication and Access Control	✓	✓	✓
		PR.AT	Awareness and Training	✓	✓	X
		PR.DS	Data Security	✓	✓	✓
		PR.IP	Information Protection Processes and Procedures	✓	✓	✓
		PR.MA	Maintenance	✓	✓	✓
		PR.PT	Protective Technology	✓	✓	✓
DE	Detect	DE.AE	Anomalies and Events	✓	✓	✓
		DE.CM	Security Continuous Monitoring	✓	✓	✓
		DE.DP	Detection Processes	✓	✓	X
RS	Respond	RS.RP	Response Planning	✓	✓	X
		RS.CO	Communications	✓	✓	X
		RS.AN	Analysis	✓	✓	✓
		RS.MI	Mitigation	✓	✓	✓
		RS.IM	Improvements	✓	✓	X
RC	Recover	RC.RP	Recovery Planning	✓	✓	X
		RC.IM	Improvements	✓	✓	X
		RC.CO	Communications	✓	✓	X

Functions		Categories			People	Process	Technology
ID	Identify	ID.AM	Asset Management		✓	✓	✓
		ID.BE	Business Environment		✓	✓	X
		ID.GV	Governance		✓	✓	X
		ID.RA	Risk Assessment		✓	✓	✓
		ID.SM	Supply Chain Risk Management		✓	✓	X
		ID.SC	Supply Chain Risk Management		✓	✓	X
PR	Protect	PR.AC	Access Management, Authentication, Authorization, and Account Control		✓	✓	✓
		PR.AT	Awareness and Training		✓	✓	X
		PR.DS	Data Security		✓	✓	✓
		PR.PP	Physical Protection, Protection of Assets, and Protection of Information		✓	✓	✓
		PR.MA	Maintenance		✓	✓	✓
		PR.PT	Protective Technology		✓	✓	✓
DE	Detect	DE.EI	Events and Incidents		✓	✓	✓
		DE.CM	Security Continuous Monitoring		✓	✓	✓
		DE.DT	Detection		✓	✓	X
RS	Respond	RS.RP	Response Planning		✓	✓	X
		RS.CO	Communication		✓	✓	X
		RS.AN	Analysis		✓	✓	✓
		RS.MI	Mitigation		✓	✓	✓
		RS.IM	Improvements		✓	✓	X
		RS.CO	Communication		✓	✓	X
RC	Recover	RC.RP	Recovery Planning		✓	✓	X
		RC.IM	Improvements		✓	✓	X
		RC.CO	Communications		✓	✓	X

- Only about **half** of the Framework's controls are addressed by technology
- Highlights the importance of both **people** and **process** in cybersecurity

# Really bad technology jokes

Ones you may never have heard. And may never want to hear again.

How did the network engineer  
configure high availability for the  
office coffee machines?

Hot Standby Roasting Protocol (HSRP)

# How to use the NIST CSF



# How to Use the Framework

Basic Review of  
Cybersecurity Practices

**3.1**

**3.4**

Buying Decisions

**NEW**

Establishing  
or Improving a  
Cybersecurity Program

**3.2**

**3.5**

Identifying Opportunities  
for Updated  
Informative References

Communicating  
Cybersecurity Requirements  
with Stakeholders

**3.3**

**3.6**

Methodology to  
Protect Privacy and  
Civil Liberties

# Improving a Cybersecurity Program





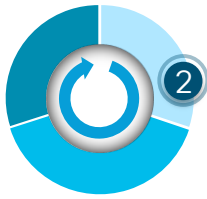
# Prioritize and Scope



## **Identify business/mission objectives and high-level organizational priorities**

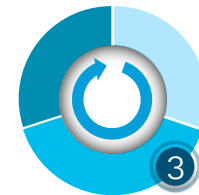
- Make strategic decisions on cybersecurity
- Determine scope of systems and assets that support the mission
- Assess risk tolerance





## **Identify related systems, regulatory requirements, and overall risk approach**

- Identify threats to systems and assets
- Identify vulnerabilities associated with systems and assets



# Create Current Profile

Function	Category	Subcategory		Current Profile
Identify	Asset Management	Physical device inventories	Tier 1	Manual, spreadsheet-based system is insufficient and lacks network visibility.
		Software inventories	Tier 1	Asset management system cannot detect new software applications being deployed.
		Communication / data flow maps	Tier 2	Flow maps are documented and approved but needs to be formalized by policy.
		External system catalogs	Unused	Current business model does not require external system catalogs.
		Resource prioritization	Tier 4	Prioritization system is working well for our needs today.
		Roles/responsibilities clarification	Tier 3	New cybersecurity responsibilities need to be formalized by policy.



# Conduct Risk Assessment

Fxn.	Cat.	Sub.	Current Profile	Risk Assessment	
ID	ID.AM	ID.AM-1	Tier 1	✗	Unacceptably high risks
		ID.AM-2	Tier 1	✗	
		ID.AM-3	Tier 2	✓	Acceptable risks at this time
		ID.AM-4	Unused	✓	
		ID.AM-5	Tier 4	✓	
		ID.AM-6	Tier 3	✓	



# Create Target Profile



This is where we want to be

- Physical device and software inventories at Tier 4, “Adaptive”
- Practices fully established, continuously improved, and built into our overall risk management program



Fxn	Cat	Sub	Target Profile
ID	ID.AM	ID.AM-1	Tier 4
		ID.AM-2	Tier 4
		ID.AM-3	Tier 2
		ID.AM-4	Unused
		ID.AM-5	Tier 4
		ID.AM-6	Tier 3

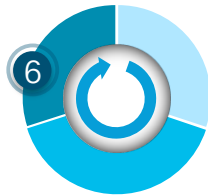
# Gap Analysis

Fxn	Cat	Sub	Current Profile
ID	ID.AM	ID.AM-1	Tier 1
		ID.AM-2	Tier 1
		ID.AM-3	Tier 2
		ID.AM-4	Unused
		ID.AM-5	Tier 4
		ID.AM-6	Tier 3



Enables a  
**prioritized**  
action plan

Fxn	Cat	Sub	Target Profile
ID	ID.AM	ID.AM-1	Tier 4
		ID.AM-2	Tier 4
		ID.AM-3	Tier 2
		ID.AM-4	Unused
		ID.AM-5	Tier 4
		ID.AM-6	Tier 3



# Gap Analysis

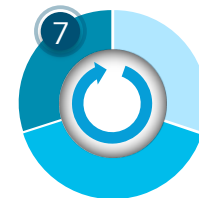
We need an accurate device inventory...



...but we don't even know what's on our network!



“The organization then determines resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.” – NIST CSF



# Implement Action Plan

Fxn	Cat	Sub	Informative Resources
ID	ID.AM	ID.AM-1	<ul style="list-style-type: none"><li>• CIS CSC 1</li><li>• COBIT 5 BAI09.01, BAI09.02</li><li>• ISA 62443-2-1:2009 4.2.3.4</li><li>• ISA 62443-3-3:2013 SR 7.8</li><li>• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2</li><li>• <b>NIST SP 800-53 Rev. 4 CM-8, PM-5</b></li></ul>
		ID.AM-2	<ul style="list-style-type: none"><li>• CIS CSC 2</li><li>• COBIT 5 BAI09.01, BAI09.02, BAI09.05</li><li>• ISA 62443-2-1:2009 4.2.3.4</li><li>• ISA 62443-3-3:2013 SR 7.8</li><li>• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2</li><li>• <b>NIST SP 800-53 Rev. 4 CM-8, PM-5</b></li></ul>

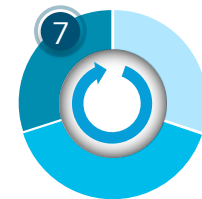
## NIST SP 800-53 Revision 4

### CM-8 / Information System Component Inventory

Control: The organization:

a. Develops and documents an inventory of information system components that:

1. Accurately reflects the current information system;
2. Includes all components within the authorization boundary of the information system;
3. Is at the level of granularity deemed necessary for tracking and reporting; and
4. Includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]



# Implement Action Plan

1

Build Software-Defined Access (SDA) requirements into our security policy, process, and training

Chief Information Security Officer



2

Invest in SDA technology that delivers network visibility, discovery, classification, and control

Network Engineering  
Security Engineering



3

Integrate SDA technology with our asset tracking software for real-time inventory management

Network Engineering  
IT Operations



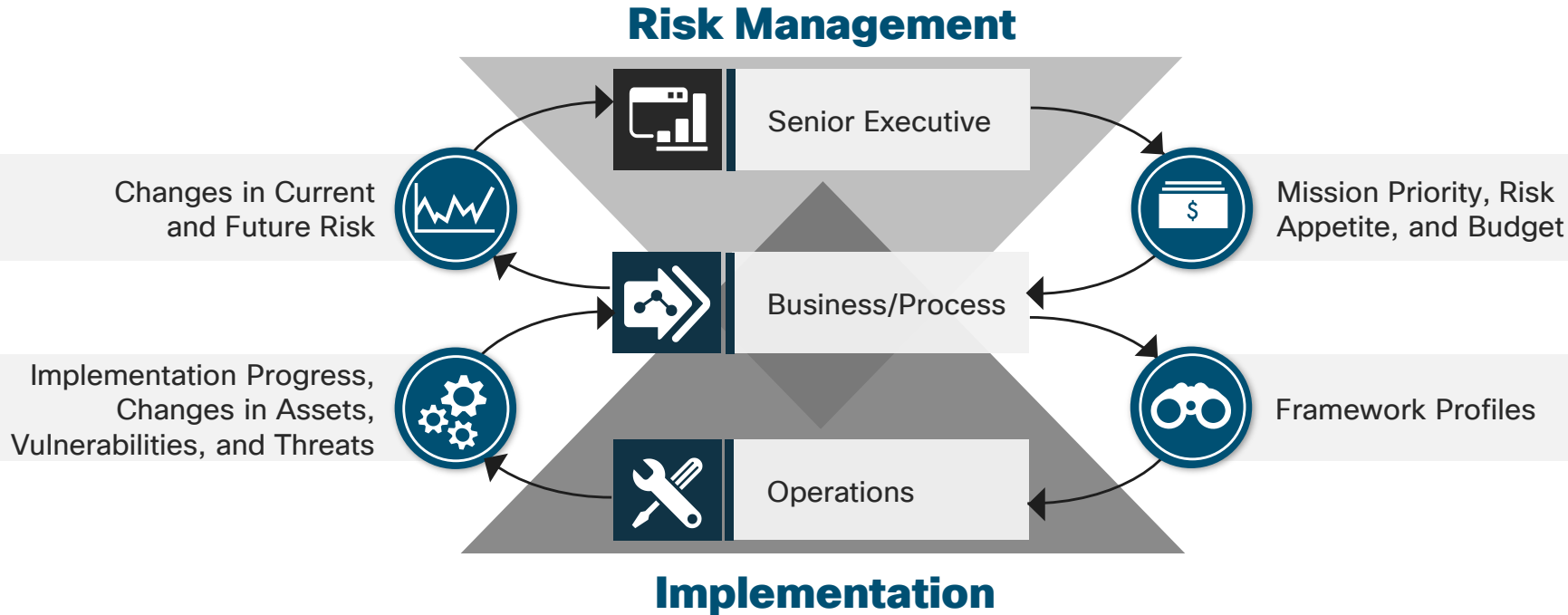


# Continuous Improvement: Not Once and Done!

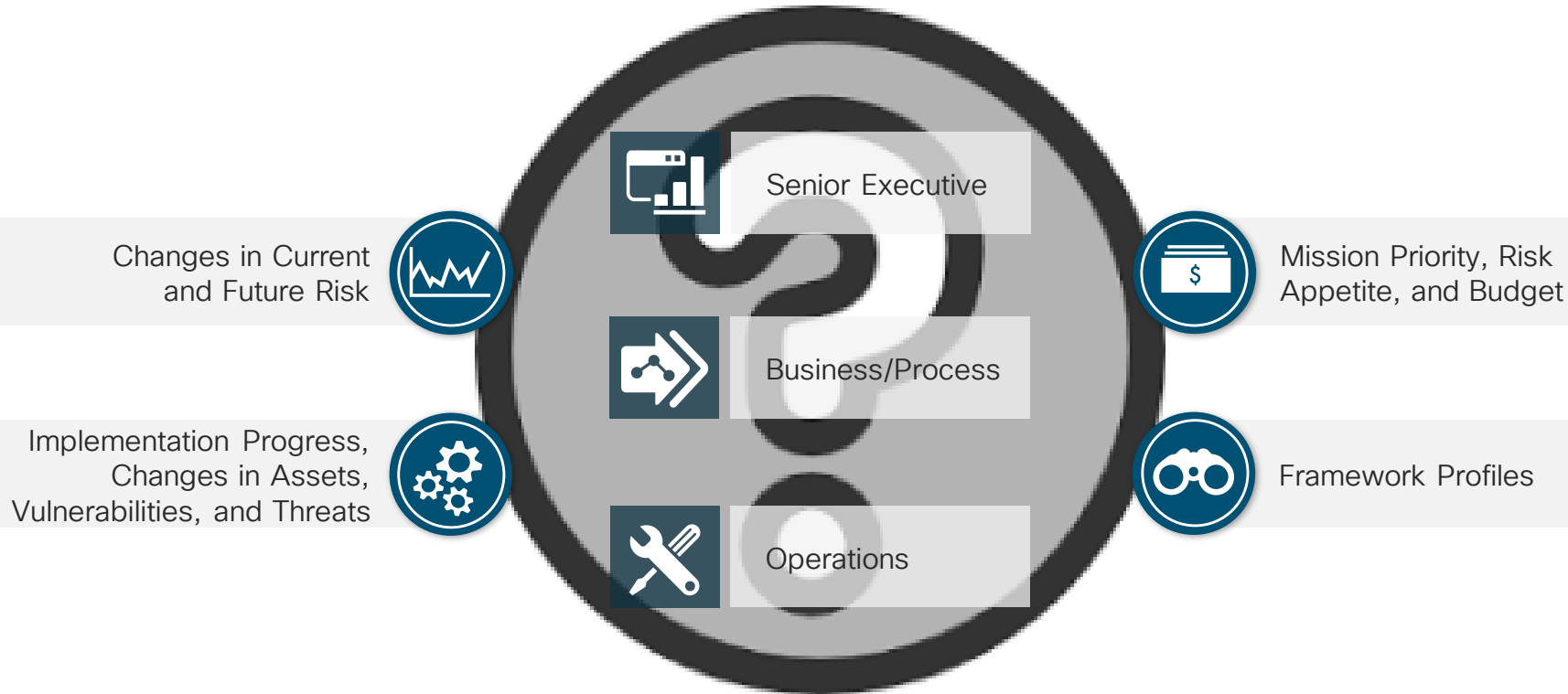


# Implementation Coordination

**Figure 2:**  
Notional Information and  
Decision Flows within an  
Organization



# But how do you have those conversations?



# Really bad technology jokes

Ones you may never have heard. And may never want to hear again.

Where did the Unix administrator  
go for professional help?

/etc/services

# Use the Baldrige Cybersecurity Excellence Builder





# Imagine if you had a way to..

- **Determine** the cyber activities that are essential to your strategy and service delivery
- **Prioritize** your investments in managing cybersecurity risk
- **Determine** how best to enable people to be risk conscious and security aware
- **Assess** the efficiency and effectiveness of your use of cyber standards and practices
- **Assess** the cybersecurity results you achieve
- **Identify** strengths to leverage and priorities for improvement

# Baldrige: Quality and Performance Excellence



Supports Performance Excellence  
in the US and around the world

Public-private partnership dedicated  
to Performance Excellence

Provides organization assessment  
tools to measure and evaluate



Government



Education

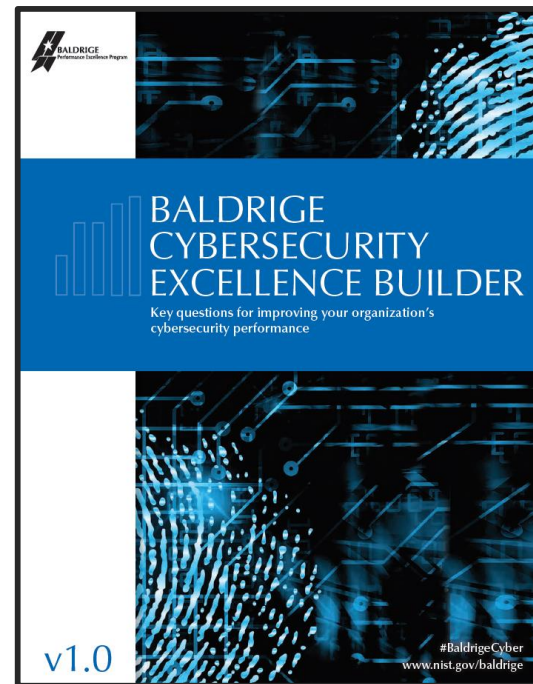


Healthcare

# Baldrige Cybersecurity Excellence Builder (CEB)

New self-assessment tool to improve your organization's cybersecurity performance

- Asks the key cybersecurity assessment questions to drive the excellence conversation in your organization
- Helps you identify areas for improvement in your cybersecurity risk management program
- Adapts and scales to your organization's needs, goals, capabilities, and environment



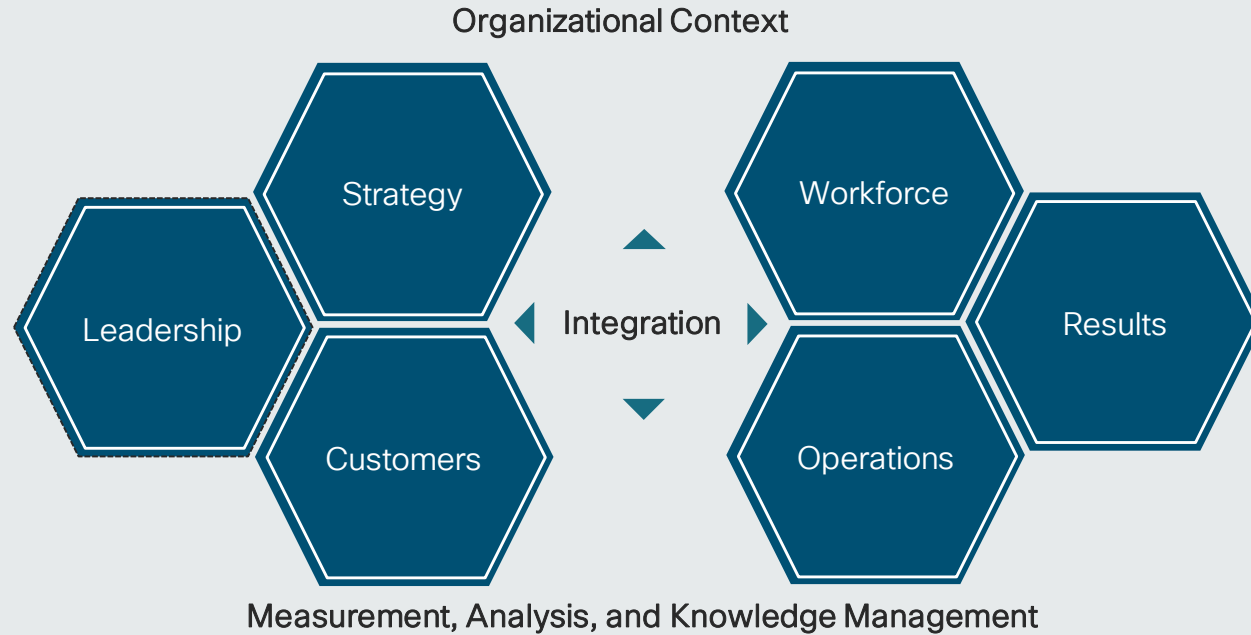
<https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative>



# Baldrige CEB and NIST CSF

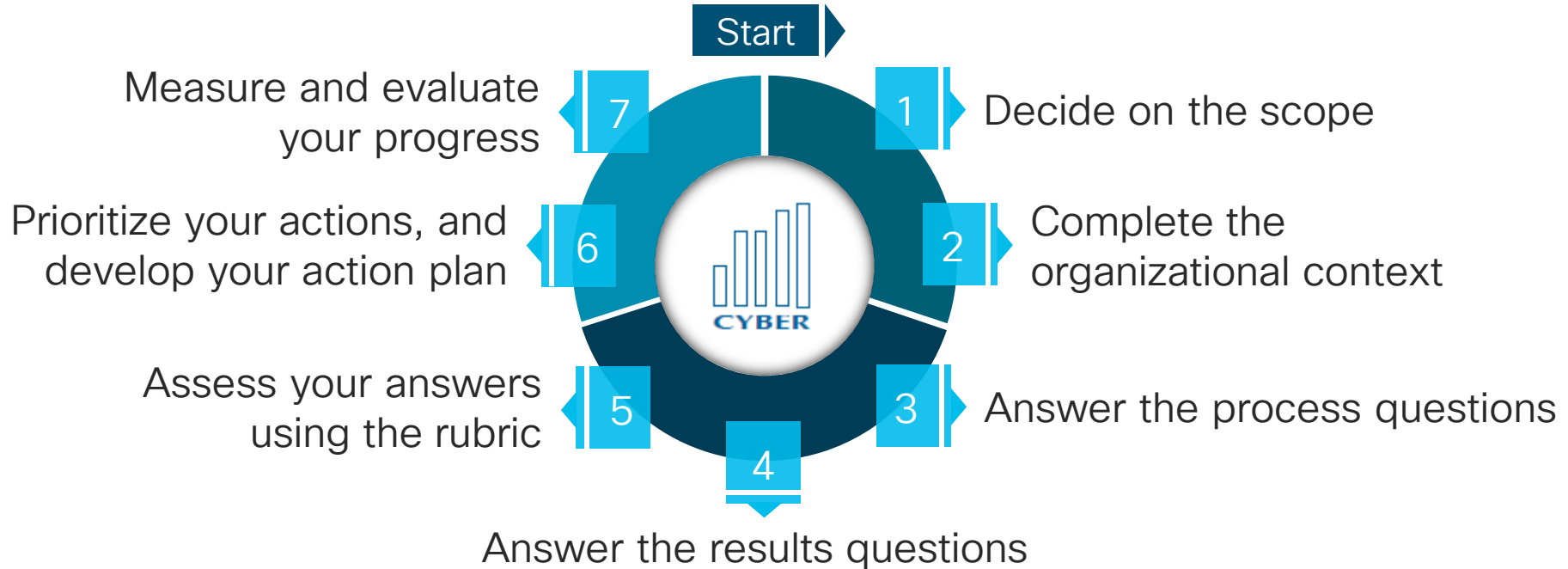


# Baldrige CEB



Helping you  
**understand and  
improve**  
what's critical to  
**your organization's**  
cybersecurity risk  
management  
program

# Improve Your Cyber Performance



# Organizational Context Questions



## Baldridge Cybersecurity Excellence Builder

### **C** Organizational Context

Having a clear understanding of your organization, why it exists, where your senior leaders want to take it in the future, who your key stakeholders are, what their expectations are, and what resources support critical functions will enable you to make and implement strategic decisions about cybersecurity risks, policies, and operations.

#### C.1 Organizational Description: What are your key organizational characteristics?

##### a. Organizational Environment

- (1) **Product Offerings** What are your organization's main product and service offerings? What is the relative importance of each to your success? What mechanisms do you use to deliver your products and services?
- (2) **MISSION, VISION, and VALUES** What are your stated MISSION, VISION, and VALUES? What are your organization's CORE COMPETENCIES, and what is their relationship to your MISSION?

# Sample Process and Results Questions

## Process Questions



### 5.1 Workforce Environment: How do you build an effective and supportive environment for your cybersecurity workforce?

- (1) HOW do you assess your CYBERSECURITY WORKFORCE CAPABILITY and CAPACITY needs?
- (2) HOW do you recruit, hire, place, and retain new CYBERSECURITY WORKFORCE members?
- (3) HOW do you organize and manage your CYBERSECURITY WORKFORCE to establish roles and responsibilities?
- (4) HOW do you prepare your CYBERSECURITY WORKFORCE for changing CAPABILITY and CAPACITY needs?

## Results Questions



### 7.2 Customer Results: What are your customer-focused cybersecurity performance results?

- (1) What are your RESULTS for your internal and external CUSTOMERS' satisfaction and dissatisfaction with your CYBERSECURITY policies and operations?
- (2) What are your RESULTS for the impact of your organization's CYBERSECURITY policies and operations on CUSTOMER ENGAGEMENT?
- (3) What are your RESULTS for your internal and external CUSTOMERS' understanding and fulfillment of their CYBERSECURITY roles and responsibilities?

# Assessment Rubric



## Maturity Levels (scoring guide)

	Maturity Level	Evaluation Factor			
		Approach	Deployment	Learning	Integration
<b>1</b> Reactive	Reactive	CYBERSECURITY-related policies/operations are characterized by activities created to fix problems rather than by PROCESSES.	CYBERSECURITY-related APPROACHES are NOT used consistently in appropriate organizational units or by CUSTOMERS, PARTNERS, and suppliers, as appropriate.	Improvement in CYBERSECURITY-related policies/operations is achieved mainly in reaction to immediate needs or problems.	There is no coordination among CYBERSECURITY-related policies/operations in different parts of your organization or between CYBERSECURITY-related policies/operations and those of the rest of the organization; individual areas or work units operate independently.
<b>2</b> Early	Early	CYBERSECURITY-related policies/operations are beginning to be carried out with well-ordered, repeatable APPROACHES.	KEY CYBERSECURITY-related APPROACHES are beginning to be used consistently in appropriate organizational units and by CUSTOMERS, PARTNERS, and suppliers, as appropriate.	CYBERSECURITY-related policies/operations are in the early stages of a transition from reacting to problems to a general improvement orientation.	CYBERSECURITY-related APPROACHES are ALIGNED with other areas or work units, and with organization-wide APPROACHES, largely through joint problem solving.
<b>3</b> Developing	Developing	Some elements of CYBERSECURITY-related policies/operations are characterized by EFFECTIVE, well-ordered, repeatable APPROACHES.	KEY CYBERSECURITY-related APPROACHES are used consistently in appropriate organizational units and by CUSTOMERS, PARTNERS, and suppliers, as appropriate, although some are in the early stages of use.	CYBERSECURITY-related policies/operations are beginning to be SYSTEMATICALLY evaluated and improved.	CYBERSECURITY-related APPROACHES are beginning to be ALIGNED among work units and with your organization's basic needs.
<b>4</b> Mature	Mature	Many elements of CYBERSECURITY-related policies/operations are characterized by EFFECTIVE, well-ordered, repeatable APPROACHES.	KEY CYBERSECURITY-related APPROACHES are used consistently in appropriate organizational units and by CUSTOMERS, PARTNERS, and suppliers, as appropriate, although use may vary in some areas or work units.	CYBERSECURITY-related policies/operations are SYSTEMATICALLY evaluated for improvement, and learnings are shared, with some INNOVATION.	CYBERSECURITY-related APPROACHES are ALIGNED among work units and with your organization's overall needs.
<b>5</b> Leading	Leading	Most elements of CYBERSECURITY-related policies/operations are characterized by EFFECTIVE, well-ordered, repeatable APPROACHES.	KEY CYBERSECURITY-related APPROACHES are used consistently in most appropriate organizational units by CUSTOMERS, PARTNERS, and suppliers, as appropriate, with no significant gaps.	CYBERSECURITY-related policies/operations seek and achieve efficiencies through analysis, INNOVATION, and the sharing of information and knowledge.	CYBERSECURITY-related policies/operations in different units work mainly in harmony with each other and with current and future organizational needs defined by your organization.
<b>6</b> Exemplary	Exemplary	All elements of CYBERSECURITY-related policies/operations are characterized by EFFECTIVE, well-ordered, repeatable APPROACHES.	KEY CYBERSECURITY-related APPROACHES are used consistently in all appropriate organizational units and by CUSTOMERS, PARTNERS, and suppliers, as appropriate.	Fact-based, SYSTEMATIC evaluation and improvement and organizational LEARNING through INNOVATION are KEY tools; CYBERSECURITY-related policies/operations are characterized by refinement and INNOVATION, backed by ANALYSIS and sharing.	CYBERSECURITY-related policies/operations in different units work in total harmony with each other and with current and future organizational needs defined by your organization.

# Assessment Rubric



## Assess your answers

Maturity Level	Evaluation Factor			
	Approach	Deployment	Learning	Integration
<b>Reactive</b>	CYBERSECURITY-related policies/operations are characterized by activities created to fix problems rather than by PROCESSES.	CYBERSECURITY-related APPROACHES are not used consistently in appropriate organizational units or by CUSTOMERS, PARTNERS, and suppliers, as appropriate.	Improvement in CYBERSECURITY-related policies/operations is achieved mainly in reaction to immediate needs or problems.	There is no coordination among CYBERSECURITY-related policies/operations in different parts of your organization or between CYBERSECURITY-related policies/operations and those of the rest of the organization; individual areas or work units operate independently.
<b>Early</b>	CYBERSECURITY-related policies/operations are beginning to be carried out with well-ordered, repeatable APPROACHES.	KEY CYBERSECURITY-related APPROACHES are beginning to be used consistently in appropriate organizational units and by CUSTOMERS, PARTNERS, and suppliers, as appropriate.	CYBERSECURITY-related policies/operations are in the early stages of a transition from reacting to problems to a general improvement orientation.	CYBERSECURITY-related APPROACHES are ALIGNED with other areas or work units, and with organization-wide APPROACHES, largely through joint problem solving.
<b>Developing</b>	Some elements of CYBERSECURITY-related policies/operations are characterized by EFFECTIVE, well-ordered,	KEY CYBERSECURITY-related APPROACHES are used consistently in appropriate organizational units and by CUSTOMERS, PARTNERS, and suppliers, as appropriate, although some are in the early stages of	CYBERSECURITY-related policies/operations are beginning to be SYSTEMATICALLY evaluated and improved.	CYBERSECURITY-related APPROACHES are beginning to be ALIGNED among work units and with your organization's basic needs.



Maturity Level	Evaluation Factor			
	Approach	Deployment	Learning	Integration
<b>Exemplary</b>	All elements of CYBERSECURITY-related policies/operations are characterized by EFFECTIVE, well-ordered, repeatable APPROACHES.	KEY CYBERSECURITY-related APPROACHES are used consistently in all appropriate organizational units and by CUSTOMERS, PARTNERS, and suppliers, as appropriate.	Fact-based, SYSTEMATIC evaluation and improvement and organizational LEARNING through INNOVATION are KEY tools; CYBERSECURITY-related policies/operations are characterized by refinement and INNOVATION, backed by ANALYSIS and sharing.	CYBERSECURITY-related policies/operations in different units work in total harmony with each other and with current and future organizational needs defined by your organization.
<b>Exemplary</b>	are characterized by EFFECTIVE, well-ordered, repeatable APPROACHES.	PARTNERS, and suppliers, as appropriate.	CYBERSECURITY-related policies/operations are characterized by refinement and INNOVATION, backed by ANALYSIS and sharing.	current and future organizational needs defined by your organization.

# Self-Analysis Worksheet

Process (Categories 1–6)	Reactive, Early, Developing, Mature, Leading, or Exemplary?				High, Medium, or Low?
	Approach	Deployment	Learning	Integration	Importance
<b>1 Leadership</b>					
1.1 Leading for Cybersecurity: How do your senior and cybersecurity leaders lead your cybersecurity policies and operations?					
1.2 Governance and Societal Responsibilities: How do you govern your cybersecurity policies and operations and fulfill your cybersecurity-related societal responsibilities?					



# Self-Analysis Worksheet (example)

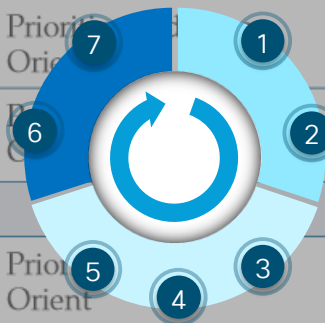
Process (Categories 1–6)	Reactive, Early, Developing, Mature, Leading, or Exemplary?				High, Medium, or Low?
	Approach	Deployment	Learning	Integration	Importance
<b>1 Leadership</b>					
1.1 Leading for Cybersecurity: How do your senior and cybersecurity leaders lead your cybersecurity policies and operations?	<b>6</b> Exemplary	<b>5</b> Leading	<b>3</b> Developing	<b>4</b> Mature	
1.2 Governance and Societal Responsibilities: How do you govern your cybersecurity policies and operations and fulfill your cybersecurity-related societal responsibilities?	<b>3</b> Developing	<b>2</b> Early	<b>2</b> Early	<b>1</b> Reactive	

# CEB/CSF Crosswalk

Cybersecurity Excellence Builder Categories and Items	Related Sections in the <i>Cybersecurity Framework</i>		
	2.4, Figure 2: Notional Information and Decision Flows	3.2, Establishing or Improving a Cybersecurity Program	Appendix A: Framework Core Functions and Categories <sup>1</sup>
<b>C Organizational Context</b>			
C.1 Organizational Description	Executive Level	Step 1: Prioritize and Scope; Step 2: Orient	ID-AM, ID-BE, ID-SC
C.2 Organizational Situation	Executive Level; Changes in Current and Future Risk	Step 1: Prioritize and Scope; Step 2: Orient	ID-BE, ID-RM
<b>1 Leadership</b>			
1.1 Leading for Cybersecurity	Executive Level	Step 1: Prioritize and Scope; Step 2: Orient	ID-BE, RC-CO
1.2 Governance and Societal Responsibilities	Executive Level	Step 2: Orient	ID-GV, RS-CO

# CEB/CSF Crosswalk

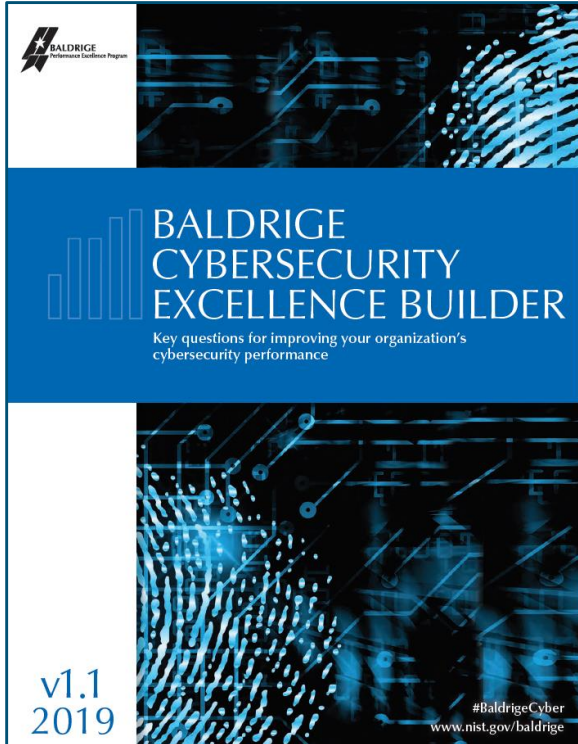
Cybersecurity Excellence Builder Categories and Items	Related Sections in the <i>Cybersecurity Framework</i>		
	2.4, Figure 2: Notional Information and Decision Flows	3.2, Establishing or Improving a Cybersecurity Program	Appendix A: Framework Core Functions and Categories <sup>1</sup>
<b>C Organizational Context</b>			
C.1 Organizational Description	Executive Level	Step 1: Prioritize Step 2: Orient	ID-AM, ID-BE, ID-SC
C.2 Organizational Situation	Executive Level; Changes in Current and Future Risk	Step 1: Prioritize Step 2: Orient	ID-BE, ID-RM
<b>1 Leadership</b>			
1.1 Leading for Cybersecurity	Executive Level	Step 1: Prioritize Step 2: Orient	ID-BE, RC-CO
1.2 Governance and Societal Responsibilities	Executive Level	Step 2: Orient	ID-GV, RS-CO



# Benefits by Organizational Roles

Role/Function	Benefit of/Reason for Using the <i>Baldrige Cybersecurity Excellence Builder</i>
<b>Board and Executive Management</b>	<ul style="list-style-type: none"><li>• Understand how internal and external cybersecurity should support organizational (business) objectives, including support for customers</li><li>• Understand current and planned workforce engagement processes and their success</li><li>• Understand opportunities to improve cybersecurity in alignment with organizational objectives</li><li>• Understand the potential exposure of the organization's assets to various risks</li><li>• Align cybersecurity policy and practices with the organization's mission, vision, and values</li></ul>
<b>Chief Information Officer (CIO)</b>	<ul style="list-style-type: none"><li>• Understand how cybersecurity affects organizational information management practices and culture</li><li>• Improve communication and engagement with organizational leaders and the cybersecurity workforce</li><li>• Understand how cybersecurity affects the organization's culture and environment</li></ul>
<b>Chief Information Security Officer (CISO)</b>	<ul style="list-style-type: none"><li>• Support the organization's commitment to legal and ethical behavior</li><li>• Create and apply cybersecurity policy and practices to support the organization's mission, vision, and values</li><li>• Respond to rapid or unexpected organizational or external changes</li><li>• Support continuous improvement through periodic use of the self-assessment tool</li><li>• Support organizational understanding of compliance with various contractual and/or regulatory requirements</li><li>• Understand the effectiveness of workforce communication, learning, and engagement, as well as operational considerations for cybersecurity</li></ul>

# CEB Summary



Voluntary self-assessment tool



Understand and improve the effectiveness of your cyber risk management efforts



Identify opportunities for improvement based on your cyber risks, needs, and objectives



Get the most from  
best practices in  
your organization



“To me, the most important thing is not which, but to pick one and align it to your own needs, threats and risk tolerance.”

**Steve Martino**  
SVP, Cisco S&TO



# Successful Adoption

Get started!

Engage leadership

Make it your own

Talk to us!





# Pitfalls to Avoid

Doing nothing or  
doing it alone



Adopting controls without a  
risk-based strategy

Thinking it's  
once-and-done

Applying a one-size-fits-all  
approach

“The voluntary NIST Cybersecurity Framework should be every company’s first line of defense. Adopting version 1.1 is a must do for all CEOs.”

**Wilbur Ross**

US Secretary of Commerce

# Conclusion



# Cybersecurity Best Practices



# Summary



## The Problem

Efficient and effective cyber risk management



## The Solution

Cybersecurity Best Practices



## Cisco Security

Our solutions and services enable best practices adoption

# Learn More

## **NIST Cybersecurity Framework**

[nist.gov/cyberframework](https://nist.gov/cyberframework)

## **Baldrige Cybersecurity Excellence Builder**

[nist.gov/baldrige](https://nist.gov/baldrige)

## **Cisco Security and Trust Organization**

[trust.cisco.com](https://trust.cisco.com)

## **Cisco Solutions aligned with NIST CSF**

[cisco.com/go/nist](https://cisco.com/go/nist)

# Complete your online session evaluation



- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live water bottle.
- All surveys can be taken in the Cisco Live Mobile App or by logging in to the Session Catalog on [ciscolive.cisco.com/us](https://ciscolive.cisco.com/us).

Cisco Live sessions will be available for viewing on demand after the event at [ciscolive.cisco.com](https://ciscolive.cisco.com).

# Continue your education



Demos in the  
Cisco campus



Walk-in  
self-paced labs



Meet the engineer  
1:1 meetings



Related sessions



# Really bad technology jokes

Ones you may never have heard. And here's the last one.

What happened to the DNS Server process that wanted to remain anonymous?

Sadly, it got “named”



Thank you





You make **possible**