CREATe Compliance

Managing Cyber Risk Through Measuring and Improving Cybersecurity Capabilities

Pamela Passman
President and CEO
CREATe Compliance

March 2018

CREATe Compliance

CREATe Compliance enables enterprises to assess, build and strengthen compliance and risk programs via the CREATe Leading Practices services:

- **CREATe Leading Practices for Cybersecurity** – *Aligned to the NIST Cybersecurity Framework*
- **CREATe Leading Practices for Intellectual Property Protection**
- **CREATe Leading Practices for Trade Secret Protection**
- **CREATe Leading Practices for Anti-Corruption** – *Aligned to leading international guidance and the ISO 37001 Anti-Bribery Management Systems Standard*

This consistent ‘measure and improve’ approach across key risk areas enables benchmarking internally and sharing across the global supply chain.

Today we will discuss…

- Top Threats Today
- How Companies Can Better Manage Cyber Risk
- Leading Approaches, Frameworks and Standards
- CREATe Leading Practices

CREATE Compliance

Top Threats Today

Headlines Focus on Personal Data …

Cybersecurity INSIDERS

Porsche admits cyber attack and data breach of 29K Japan customers

February 23, 2018

Posted By **Naveen Goud**

47

---

the japan times

June 1, 2015

NATIONAL / CRIME & LEGAL

1.25 million affected by Japan Pension Service hack

BY TOMOKO OTAKE

STAFF WRITER

CREATE Compliance

… Yet Cyber Risks Go to the Core of Business

Bloomberg

Japan Wakes Up to Global 'Ransomware' Cyberattack

THE ASSOCIATED PRESS (YURI KAGEYAMA)
May 14, 2017, 11:40 PM EDT *Updated on* May 15, 2017, 2:31 AM EDT

Honda halts production at Japan plant after cyber attacks

AFP News 21 June 2017

CSO FROM IDG

FEB 15, 2018 8:32 AM PT

NEWS ANALYSIS

Cyber espionage: China wants Japanese firms' intellectual property

Cyber groups within China are targeting Japanese companies involved in heavy industry and national infrastructure as part of a multifaceted effort to create the Chinese strategic playbook.

Cyber Risk Threat Landscape

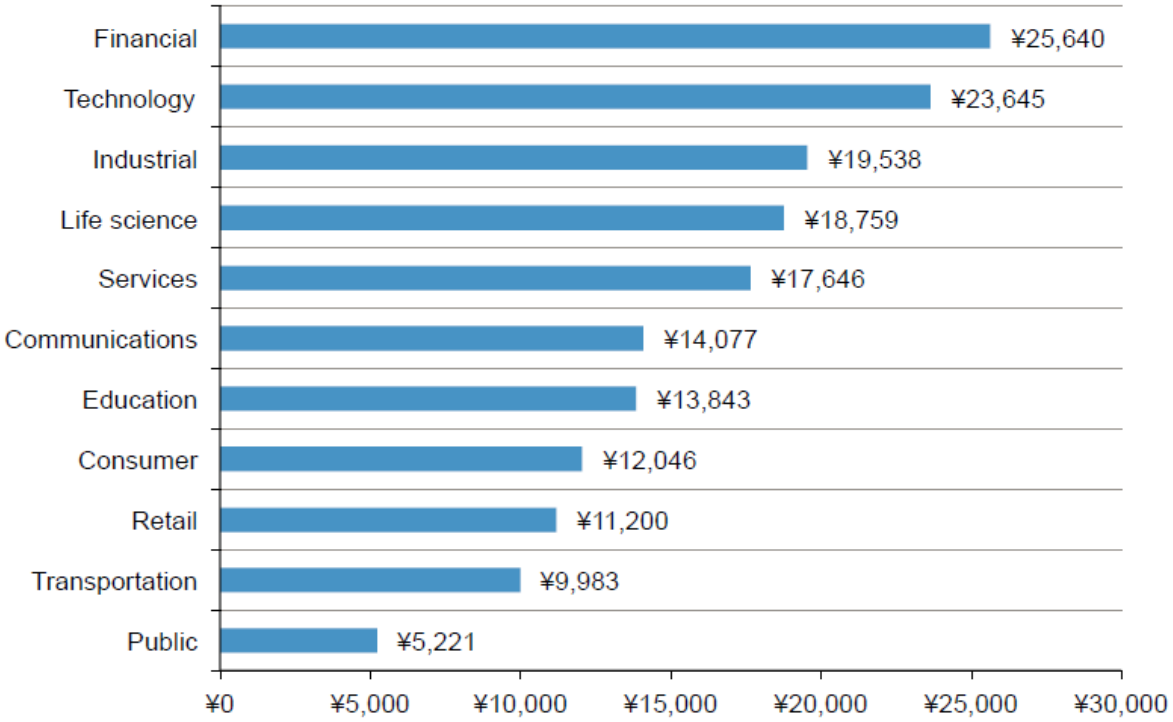
Threat Actor	Objectives	Methods	Vulnerabilities
Malicious Insiders	Competitive advantage, financial gain, national goals	Blunt force hacking Social Engineering Trojan Horse Spear phishing Watering Hole Exploits Malware Co-opted Credentials Physical/Non-technical	People Processes Technology
Nation States	Military technology, help national companies		
Competitors	Competitive advantage		
Transnati'l Organized Crime	Financial gain		
Hacktivists	Political/social goals		

CREATe Compliance

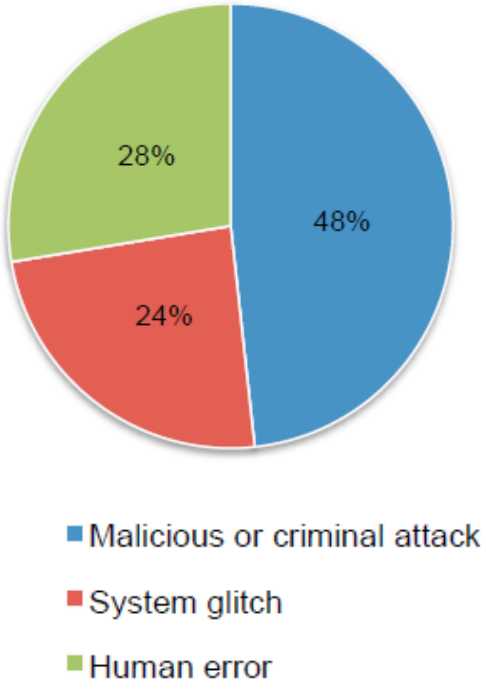
Source: CREATe.org – PwC Report: Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential thefts, February 2014

Data Breaches - Japan

Per capital cost by industry



Root cause of the data breach (of the benchmark sample)

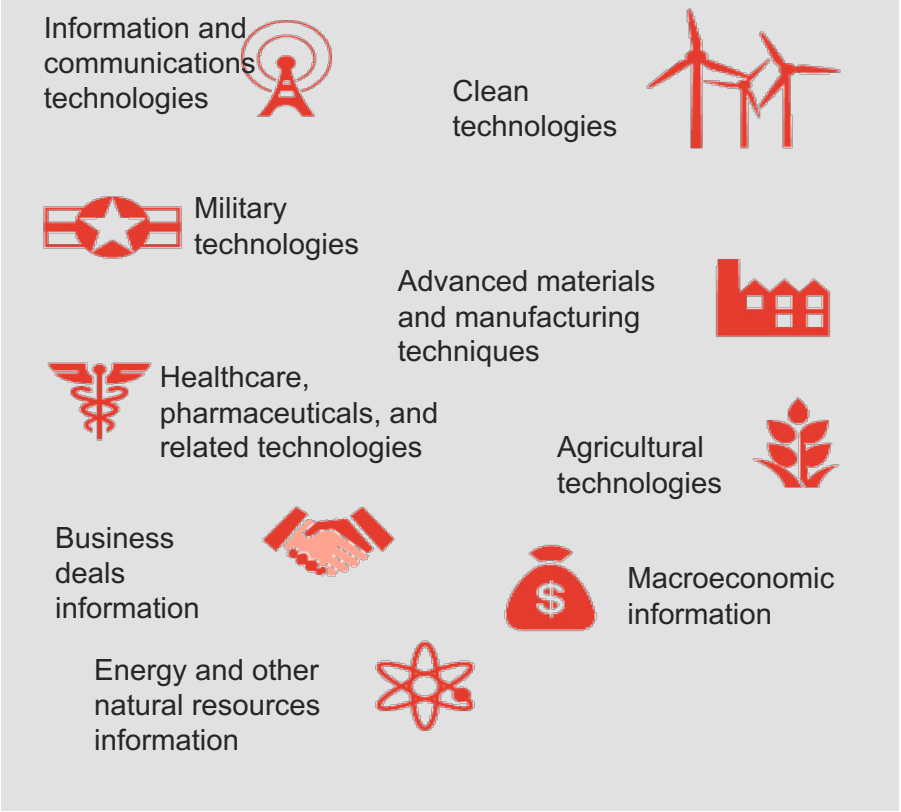


2017 Cost of Data Breach Study: Japan
Ponemon Institute, June 2017

CREATe Compliance

What's Most at Risk?

What information matters most to your business, and what matters most to your adversaries? They may not be the same thing.



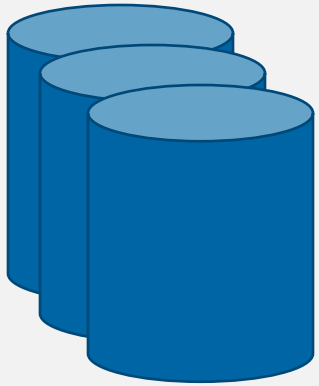
- Know what your company's most valuable and sensitive information assets are and where they are located in the business ecosystem
- Prioritize and allocate resources to effectively protect the "crown jewels" today and into the future
- Know that your company may be targets as the "means to an end" – gaining information about or access to the systems of others

Source: Office of the National Counterintelligence Executive, *Report to Congress on the Foreign Economic Collection and Industrial Espionage, 2009-2011, October 2011.*

CREATE Compliance

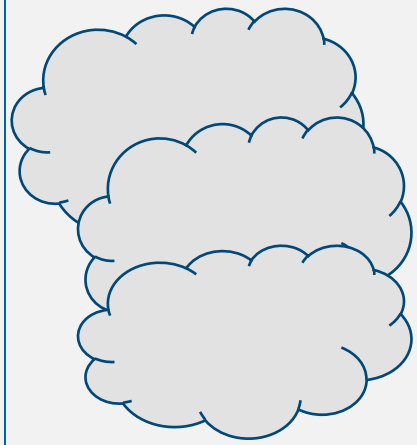
“Domains” of Cyber Vulnerability

“On Premises” Information Systems



1

“Off Premises” Cloud



2

Supply Chain

3

Web

4

CREATE Compliance

CREATE Compliance

How Companies Can Better Manage Cyber Risk

Implement a Risk and Information Security Management System

Reasons for implementing an information security management system:

- As part of an **enterprise risk management (ERM)** strategy - reviewed by senior management and/or the Board of Directors
- To meet customer **contractual requirements** related to cybersecurity and the protection of specific data, especially if the company provides any cloud-based or SAAS service, or comes in contact with the customer's network or confidential or sensitive information or data
- As required by **government procurement regulations** for providers of products/services, and in some cases for supply chain partners
- As required by **"critical infrastructure" laws** and regulations
- As required by a **cybersecurity insurance policy**

Base System on a Recognized and Flexible Framework

Goal: Demonstrate that a company has a risk and information security management system in place

Two leading approaches:

- ISO 27001 (certification)
- NIST Cybersecurity Framework (voluntary approach)

NIST Cybersecurity Framework enables you to:

- Measure the maturity of an information security system against the standards referenced and processes identified in the framework
- Choose a Target Profile – a level of maturity aligned to an organization's risk profile
- Determine gaps between system maturity and its Target Profile for each control in the Framework, creating an actionable plan for maturing its practices
- Mature practices using a cycle of continuous improvement

NIST Framework versus ISO 27001

Methodologies for Implementing Cybersecurity in an Organization

NIST FRAMEWORK:

- Voluntary, no limitations to parties that can provide verification
- U.S. developed for critical infrastructure organizations, but now widely used by all sectors and government
- Umbrella for other standards and guidance (references to ISO 27001, NIST 800-53, etc.)
- Profile Targets enable user to decide how deeply the implementation of cybersecurity should go and can be used for setting minimum requirements

ISO 27001:

- ISO Standard subject to ISO license fees and certification process
- Globally recognized process
- Mandatory requirements for documentation
- An organization either meets certification requirements or does not

CREATE Compliance

CREATE Compliance

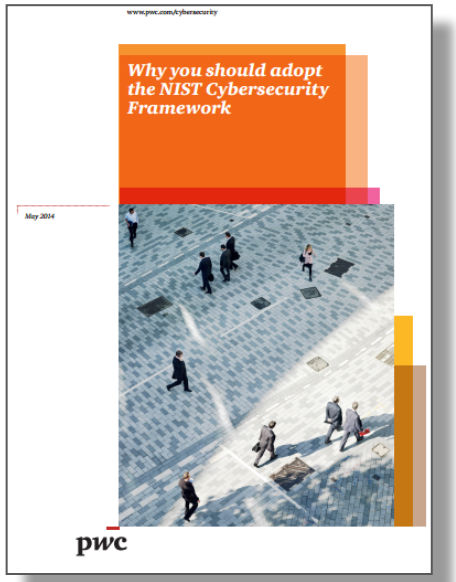
Leading Approaches, Frameworks and Standards

The NIST Cybersecurity Framework

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

"By 2020, more than 50% of organizations will use the NIST Cybersecurity Framework, up from 30% in 2015."

Gartner: Best Practices in Implementing the NIST Cybersecurity Framework
January, 21, 2016

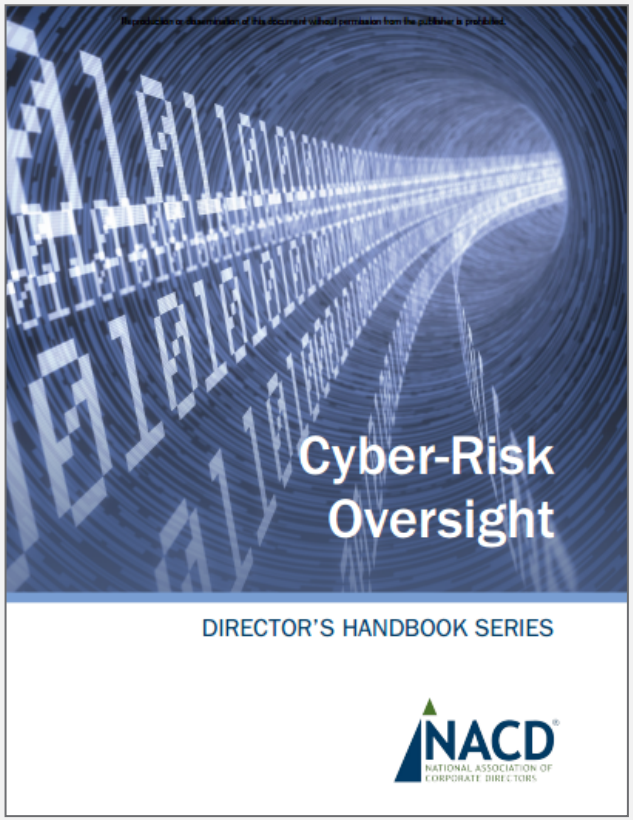


"The Framework creates a common language for the discussion of cybersecurity issues that can facilitate internal and external collaboration."

"Organizations that adopt the Framework at the highest possible risk-tolerance level may be better positioned to comply with future cybersecurity and privacy regulations."

CREATE Compliance

Questions from Board of Directors of Publicly Traded U.S. Companies



How would you answer these questions?

- Do we have appropriately differentiated strategies for general cybersecurity and for protecting our mission-critical assets?
- What are the company's cybersecurity risks?
- How is the company managing these risks?
- Who are our likely adversaries?
- How will we know if we have been breached? How will we find out?
- Do we have a systematic framework, such as the NIST Cybersecurity Framework, in place to address cybersecurity and assure adequate cybersecurity hygiene?

CREATE Compliance

Download the report at: https://www.nacdonline.org/cyber

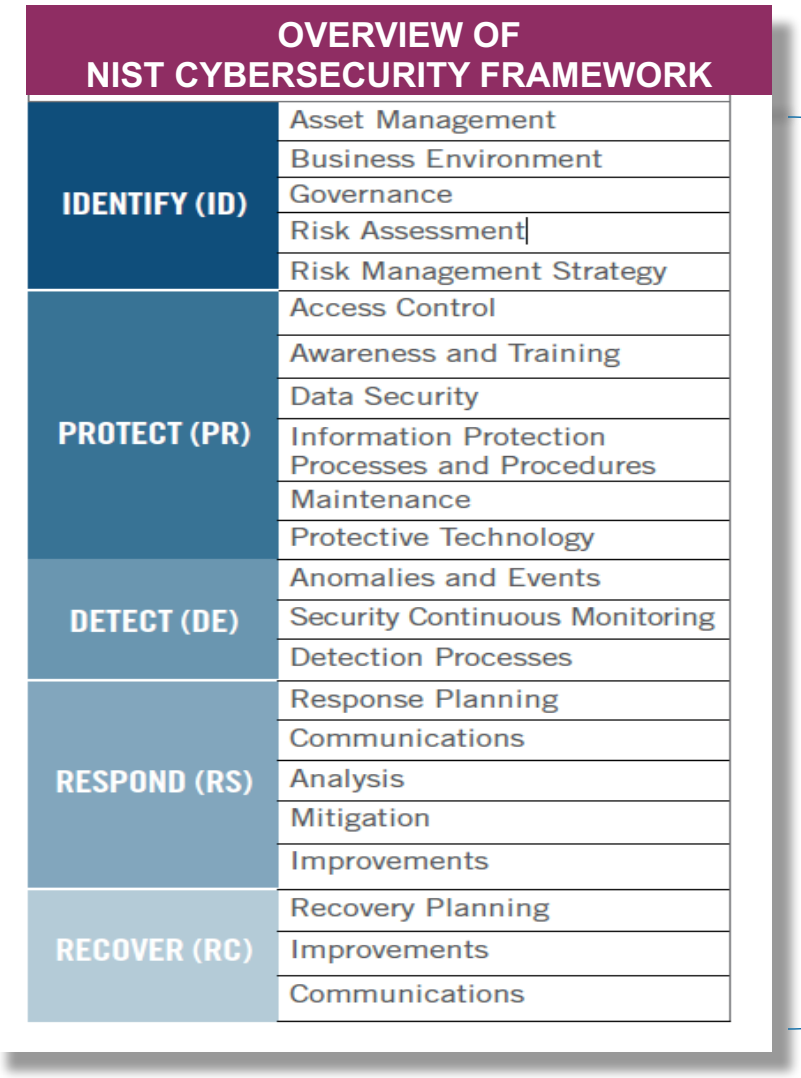
Popularity of NIST Cybersecurity Framework

Voluntary guidance, based on existing standards, guidelines, and practices

- Uses easy-to-understand language and creates a common taxonomy accessible to C-Suite, Board members and technical leaders
- Fosters risk and cybersecurity management communications among internal and external organizational stakeholders
- Provides flexibility for different sized organizations, with different risk profiles in any sector
- Recognizes that cyber risk is an organizational risk, not strictly information security or compliance
- Embodies a continual process – not a one time event
- Integrates into operational and business practices
- Integrates into enterprise risk management (ERM) process

Elements of the NIST Framework

Five main Functions



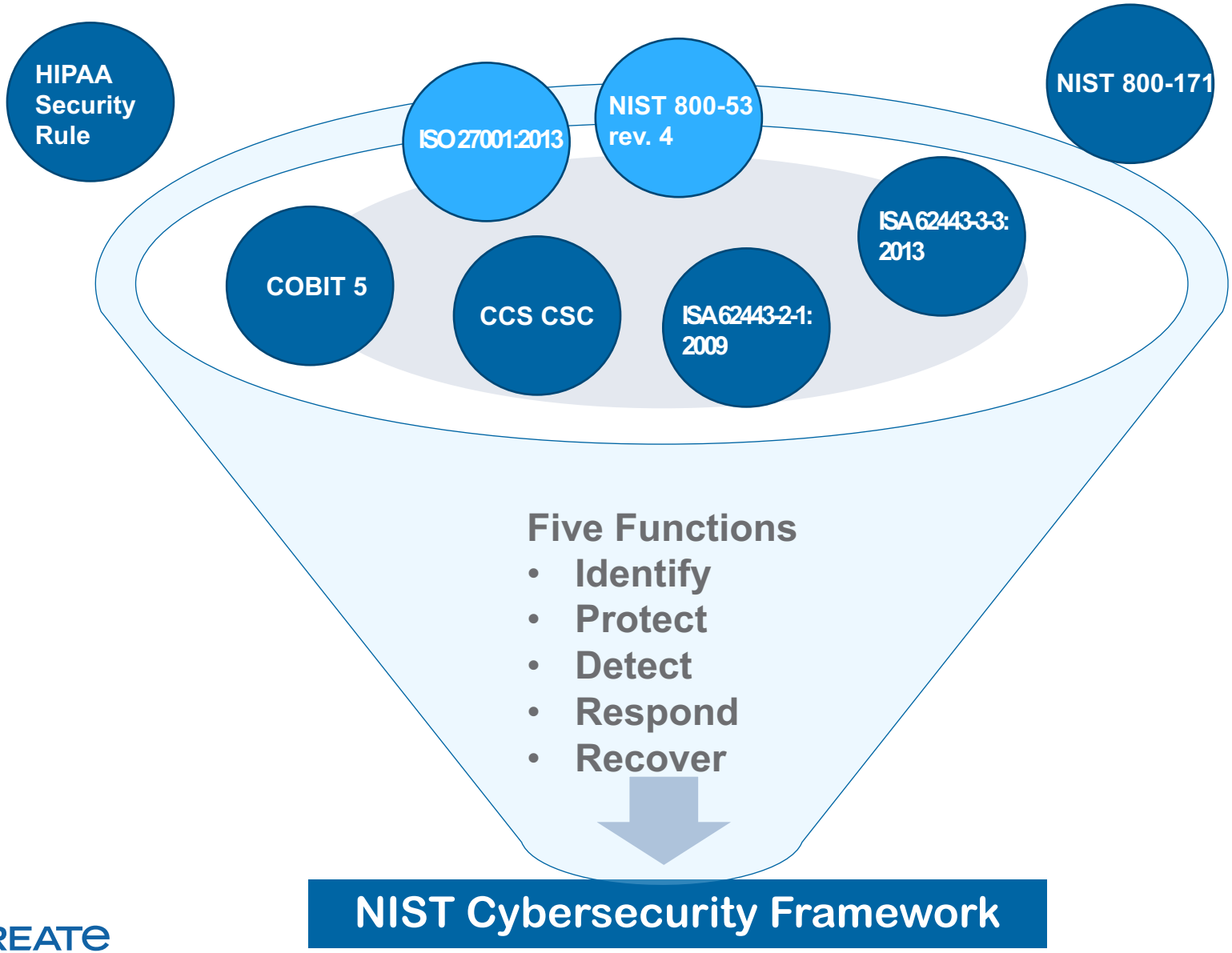
OVERVIEW OF NIST CYBERSECURITY FRAMEWORK	
IDENTIFY (ID)	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
PROTECT (PR)	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
DETECT (DE)	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
RESPOND (RS)	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
RECOVER (RC)	Recovery Planning
	Improvements
	Communications

22 Categories & 98 Subcategories of Controls

Providing an analysis of technical and management capabilities

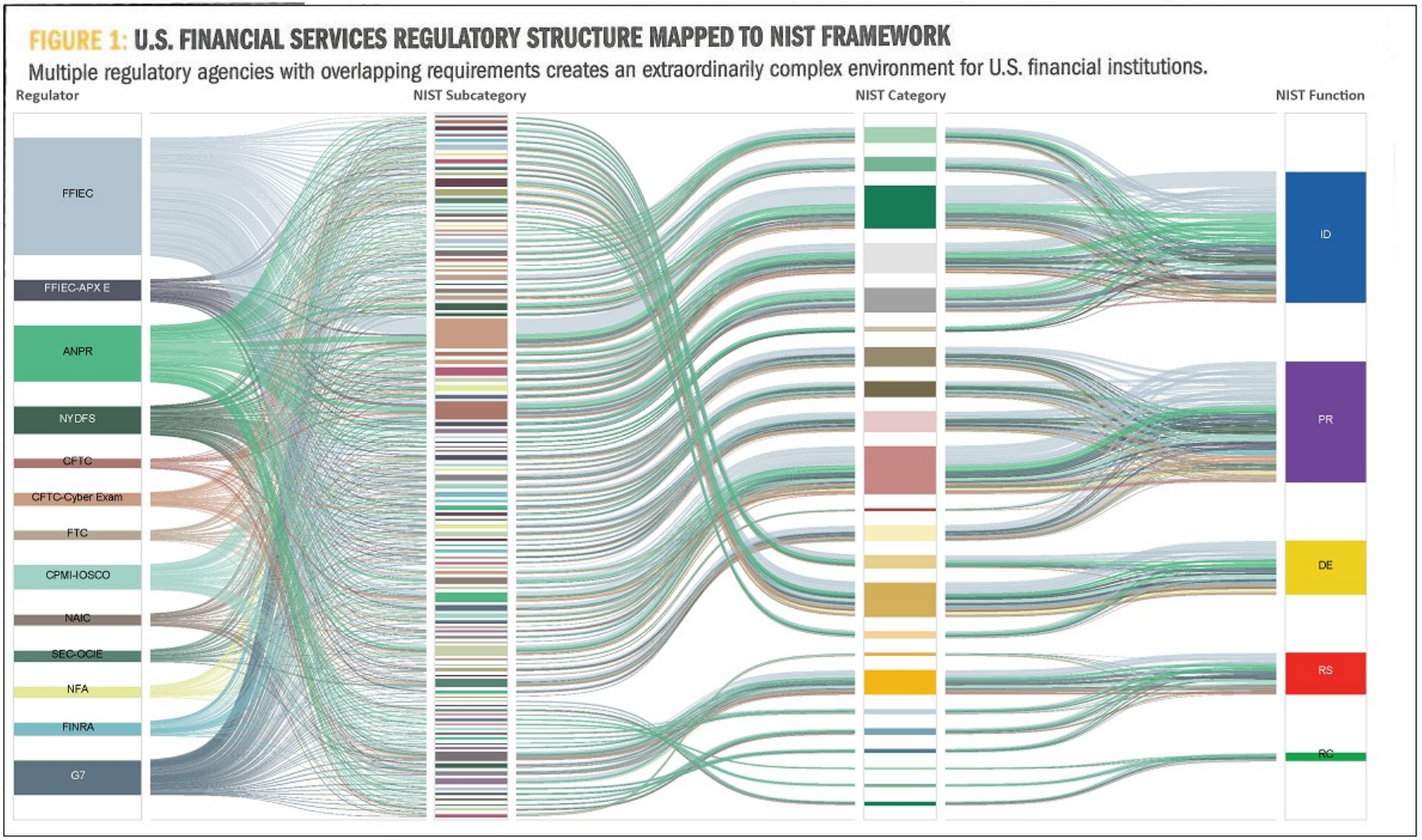
CREATE Compliance

NIST Cybersecurity Framework References



CREATE Compliance

Financial Services Sector Cybersecurity Requirements Map to NIST Framework



Federal Contractor Cybersecurity Requirements Map to NIST Framework and NIST Standards

NIST SPECIAL PUBLICATION (SP) 800-171 *("Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations")*

- **Applies to:** Companies contracting with the US Department of Defense, and their subcontractors.
- **Covers:** Technical data and computer software with military or space application that is subject to government restrictions on access, use or disclosure.
- **Requires:** Self-certification of compliance with SP 800-171 organizational and technical security requirements for protecting such data.
- **Organizational and Technical Controls:** SP 800-171 contains 110 controls in 14 categories. These include risk assessment, technical protections, 72-hour reporting of cyber incidents, and training and other organizational controls. SP 800-171 also incorporates and cross-references requirements from the NIST 800-53 standard (including general non-federal organization controls).
- **Consequences of non-compliance:** Possible loss of the government contract, civil damages for negligence/contract breach, criminal liability for fraud.
- **Effective date:** December 31, 2017. At a minimum, a System Security Plan and Plan of Action should have been in place by then.
- **Synergies with NIST Cybersecurity Framework**: Most SP 800-171 controls map to one or more NIST Framework requirements.

Cybersecurity Integrated into Business

Board Oversight

Executive Level Decision-Making

Incident Response Team

- Legal
- Risk
- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Chief Compliance Officer (CCO)
- Finance
- Communications/PR
- Physical Security
- Supply Chain
- Customer Support
- Human Resources

Stakeholders

- Employees
- Customers
- Vendors/Suppliers
- Partners
- Lenders
- Shareholders
- Regulatory agencies
- Law enforcement
- Media (formal and informal)

CREATE Compliance

Questions and Discussion

CREATE Compliance

CREATE
Compliance

Thank You