Introduction to NIST Cybersecurity Framework

Tuan Phan

Trusted Integration, Inc.

525 Wythe St
Alexandria, VA 22314
703-299-9171 Ext 103
www.trustedintegration.com
Twitter: TrustedAgentGRC

August 2014

(ISC)$^{2®}$ Quantico Chapter

TrustedAgent GOVERNANCE, RISK AND COMPLIANCE

TRUSTED INTEGRATION

Introducing Trusted Integration, Inc.

- Alexandria-based small business, founded in 2001
- Core focus on creating adaptive, scalable, and cost-effective Governance, Risk & Compliance (GRC) Solutions.
- Privately-held
- Memberships: ISSA, ISACA, AFCEA, Shared Assessments
- Deep relationships with Security, Risk and Technology Communities:

tripwire

IBM PartnerWorld

QUALYS

SHARED ASSESSMENTS

JDBIGGS ASSOCIATES

BCT PARTNERS

ADI TECHNOLOGIES Full Service Federal Marketing Consultants

INFOSIGHT Bringing the future of IT into focus

Localweb.com Cloud Hosting Provider

SAINT®

ISACA® Serving IT Governance Professionals

GRC Innovator since 2003

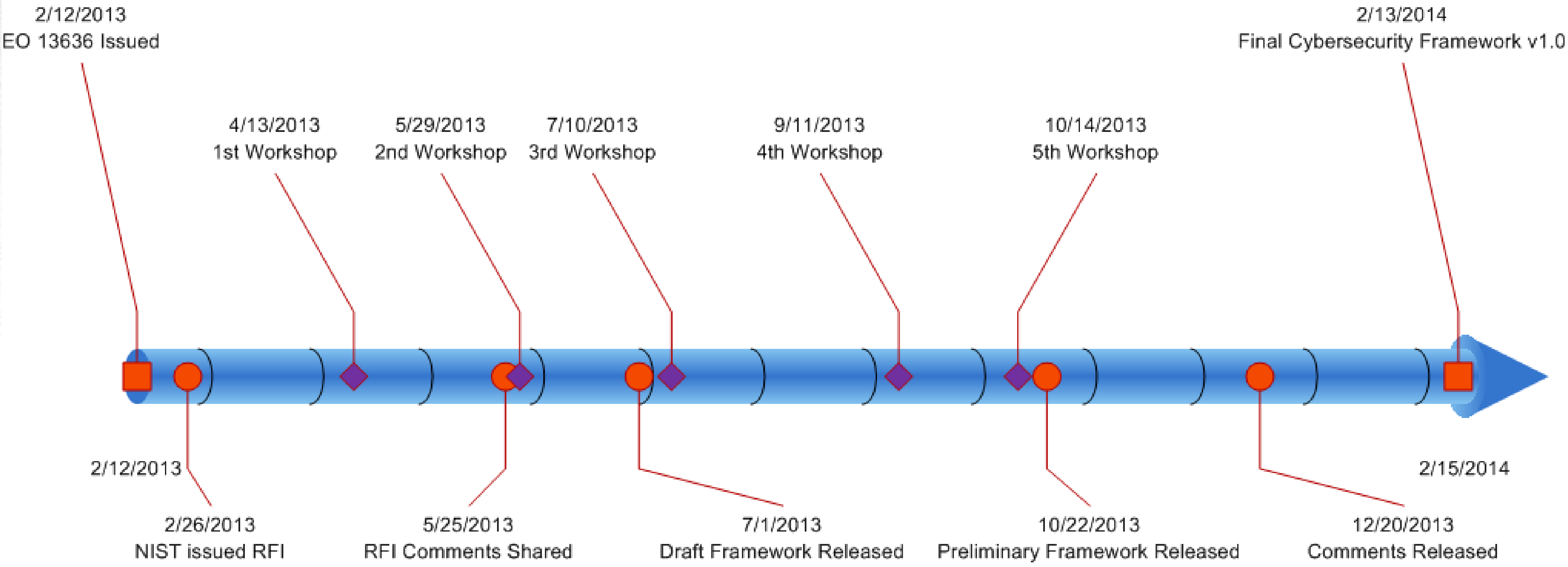
- 2014 SC Magazine Review for Risk & Policy Management
- 2013 Golden Bridge Technology Recipient for:
  - Gold Award for Government Compliance Solution
  - Silver Award for Governance, Risk and Compliance Solution
- Several Government Agencies and Commercial Enterprises depend on TrustedAgent GRC.

What is Cybersecurity Framework

- Voluntary risk-management approach
- Guidance to manage cybersecurity risk
- Encourage organizations to consider cybersecurity risk and their impact on the organization similar to:
  - Financial risk
  - Operational risk
  - Safety risk
- Does not displace or substitute for governing regulations applicable to the organizations:
  - HIPAA-HITECH
  - NERC CIP
  - PCI DSS
  - FFIEC

What is Cybersecurity Framework (cont'd)

- Collaborative in nature:
  - Incorporating over 2,700 comments since original RFI.
  - From EO 13636 until preliminary framework took over 8 months
  - Major road shows for NIST covering 5 major locations across US
  - When release, the final framework will have taken over a year to develop.

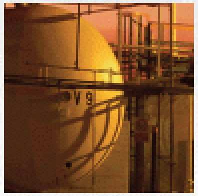


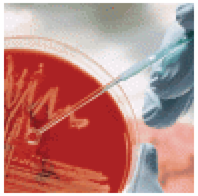
Goals of the Framework

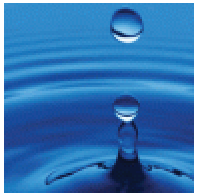
- Adaptable, flexible, and scalable
- Improve organization’s readiness for managing cybersecurity risk
- Flexible, repeatable and performance-based
- Cost-effective
- Leverage standards, methodologies and processes
- Promote technology innovation
- Actionable across the enterprise → Focus on outcomes

Applicability

- Critical infrastructure (CI) community
  - Owners
  - Operators
- Covers 16 critical infrastructure sectors:

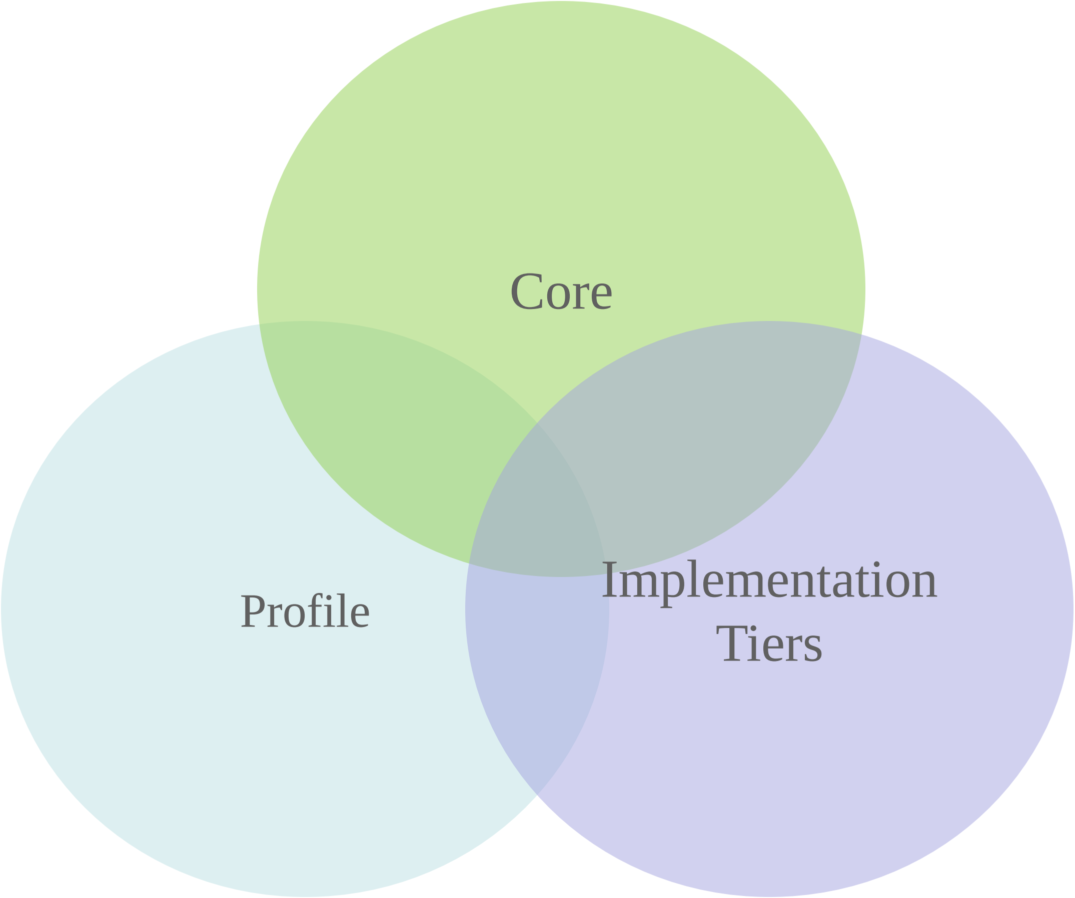






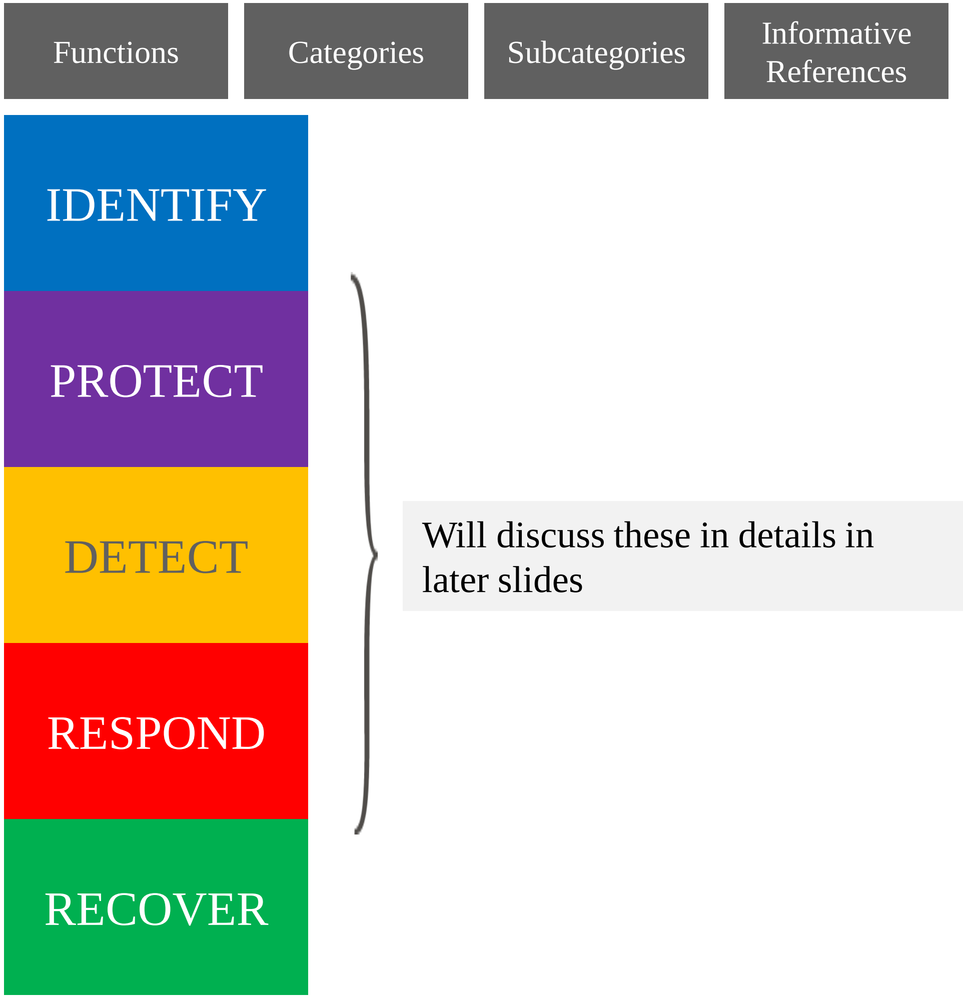
☝ Raise your hand if your sector is not listed

Key Parts of the Framework



Framework Core

- Details cybersecurity activities and key references.
- Not intended to be a checklist.
- Normalizes activities to commonly used standards and guidelines.
- Has four elements:
  - Functions: High-level cybersecurity activities to be developed, prioritized, and implemented.
  - Categories: Groups of cybersecurity outcomes
  - Subcategories: Decomposed the activities within the Categories
  - Information References: Illustrative standards, guidelines and practices



Functions

Categories

Subcategories

Informative References

IDENTIFY

PROTECT

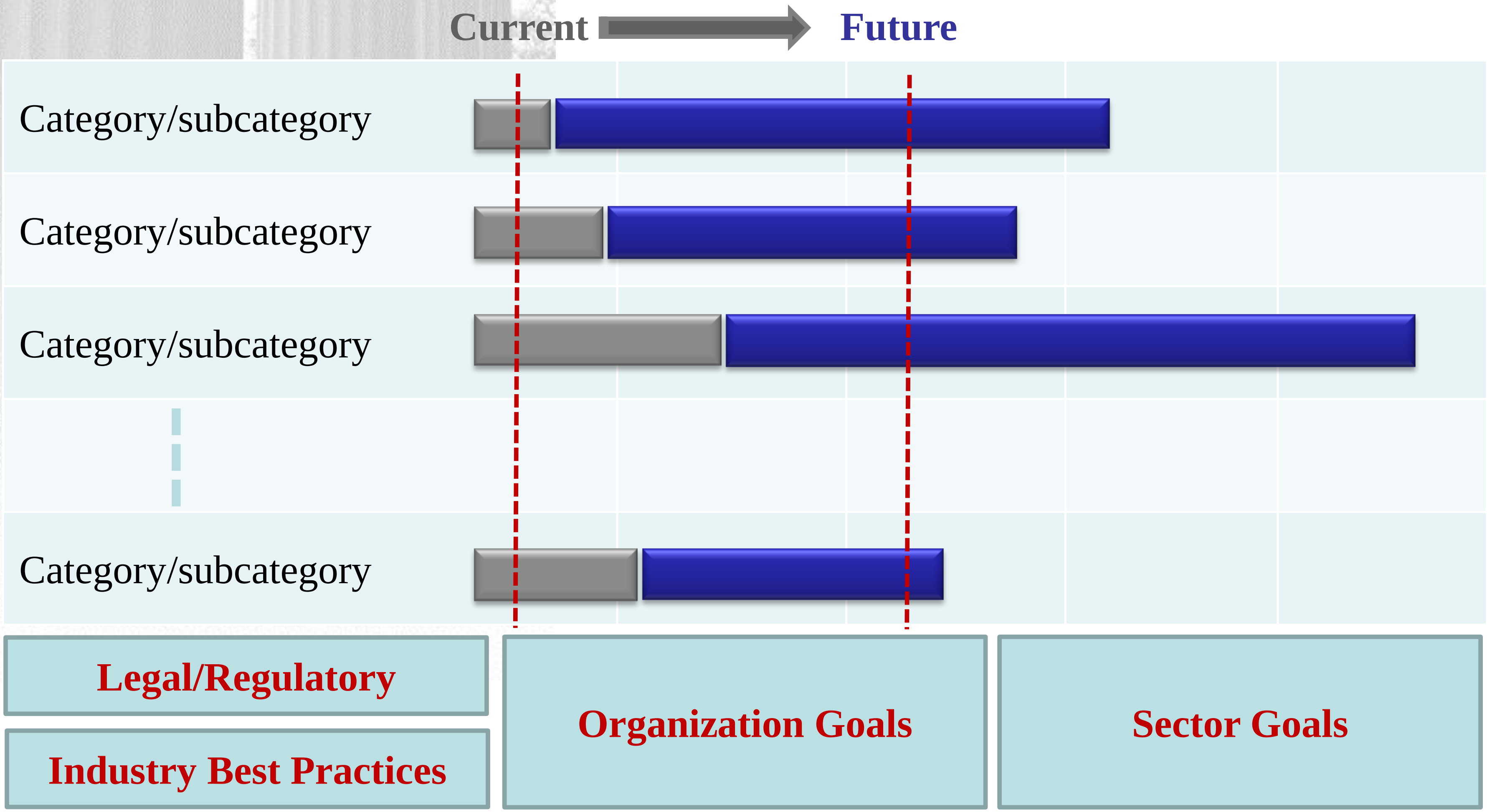
DETECT

RESPOND

RECOVER

Will discuss these in details in later slides

Framework Profile



Current → Future

Category/subcategory

Category/subcategory

Category/subcategory

Category/subcategory

Legal/Regulatory

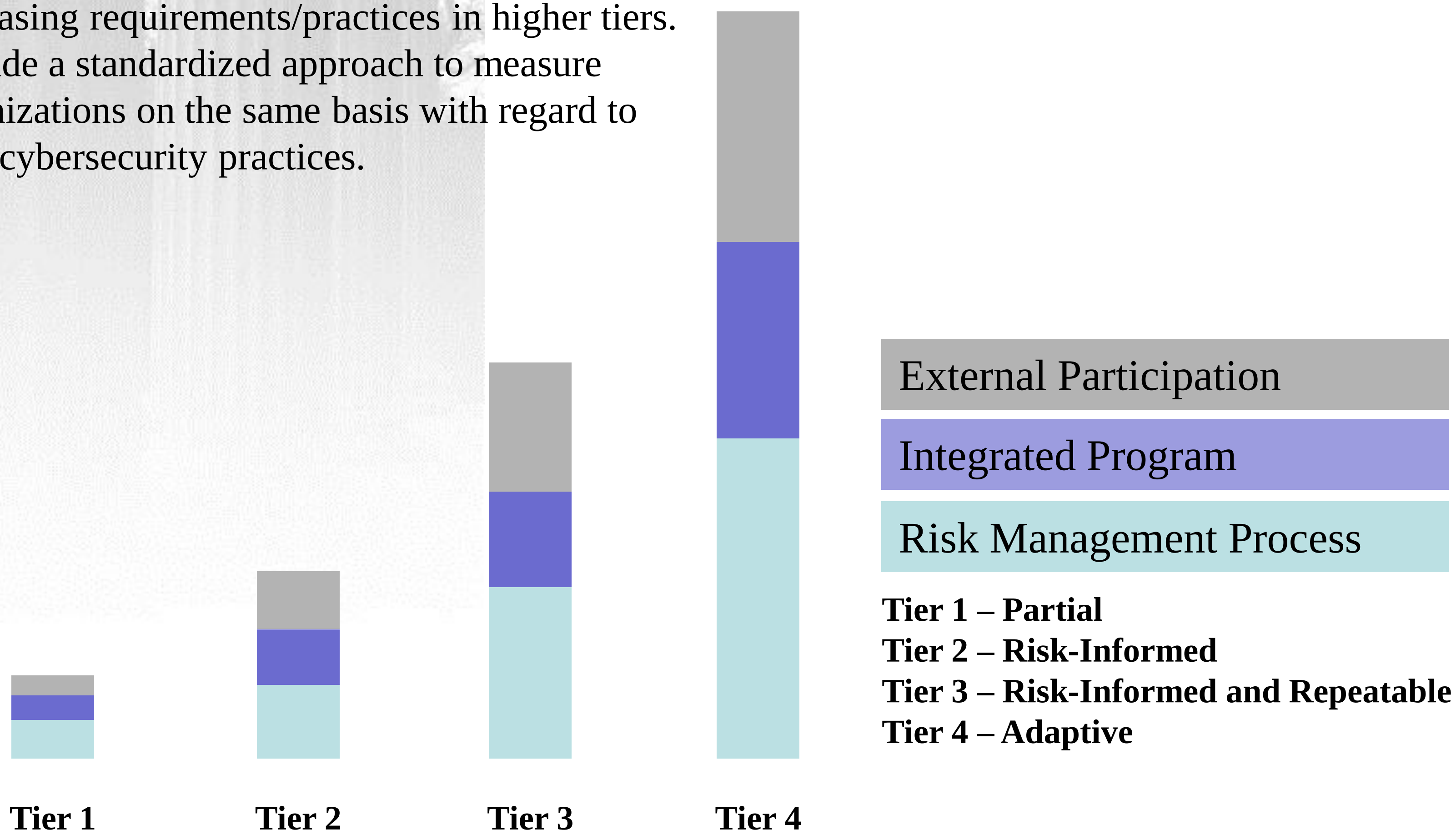
Industry Best Practices

Organization Goals

Sector Goals

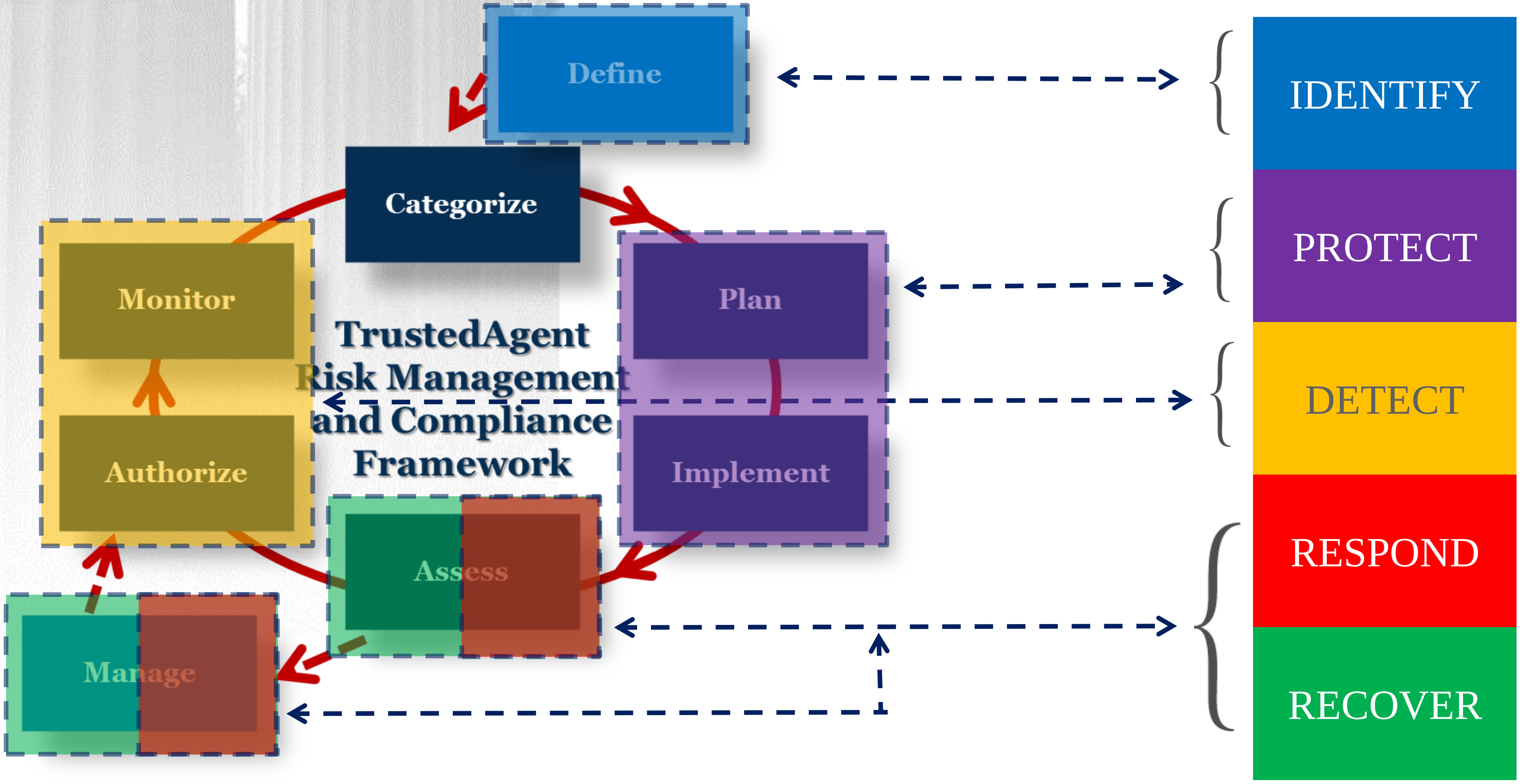
Framework Implementation Tiers

- Describe the maturity of the organization with regard to management of cybersecurity activities.
- Increasing requirements/practices in higher tiers.
- Provide a standardized approach to measure organizations on the same basis with regard to their cybersecurity practices.

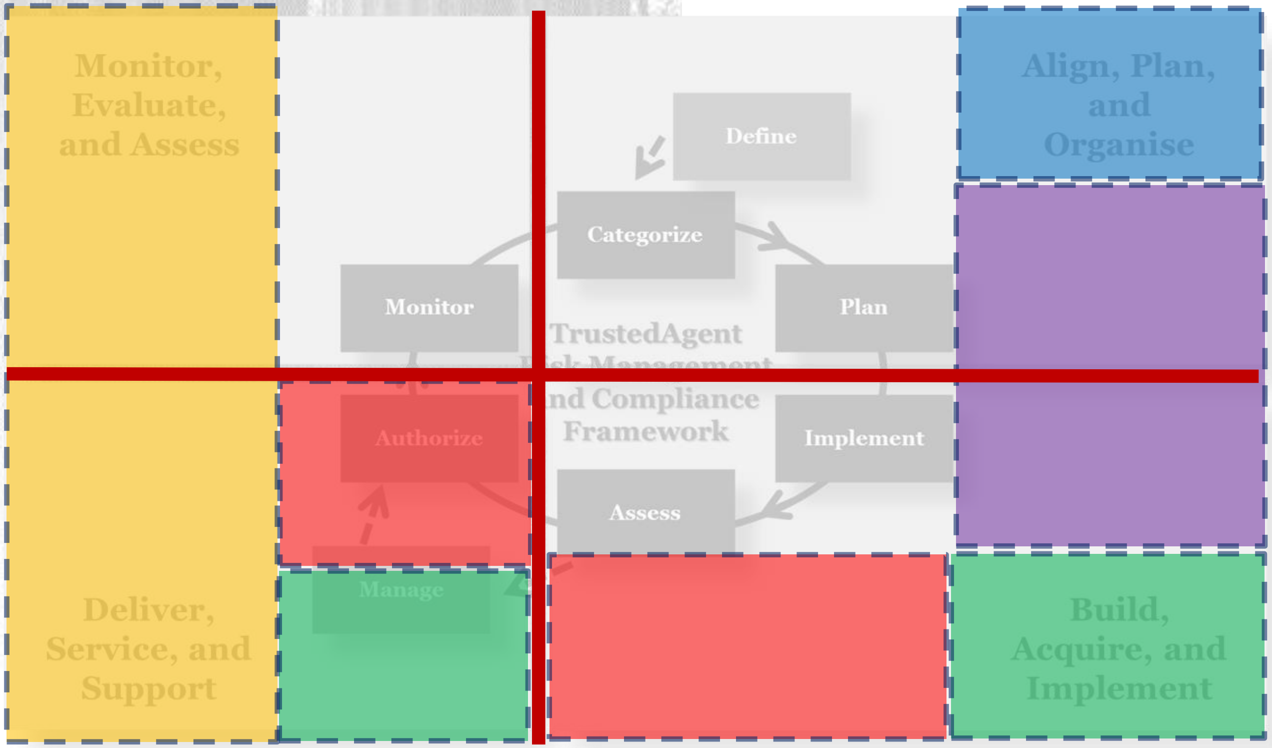


Tier 1 – Partial
Tier 2 – Risk-Informed
Tier 3 – Risk-Informed and Repeatable
Tier 4 – Adaptive

Mapping to Risk Management Framework



Mapping to COBIT/ISO 27001

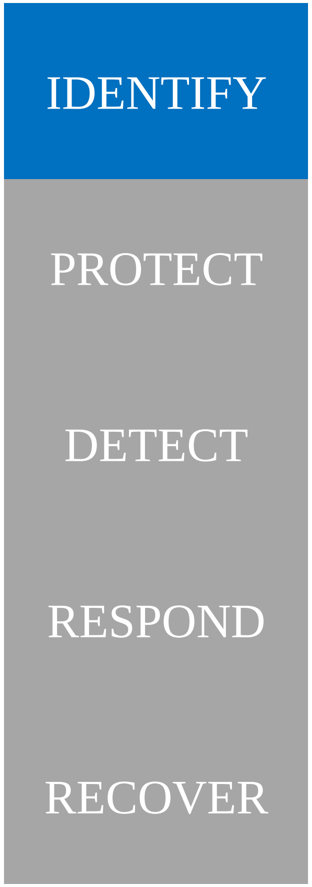

Monitor, Evaluate, and Assess
Align, Plan, and Organise
Define
Categorize
Monitor
Plan
TrustedAgent Risk Management and Compliance Framework
Authorize
Implement
Assess
Manage
Deliver, Service, and Support
Build, Acquire, and Implement

- 🟦 IDENTIFY
- 🟪 PROTECT
- 🟨 DETECT
- 🟥 RESPOND
- 🟩 RECOVER

High-Level Requirements → Categories

Develop the organizational understanding to manage cybersecurity risk to systems, programs, assets and capabilities.

- Asset Management (ID.AM)
- Business Environment (ID.BE)
- Governance (ID.GV)
- Risk Assessment (ID.RA)
- Risk Management (ID.RM)



IDENTIFY

PROTECT

DETECT

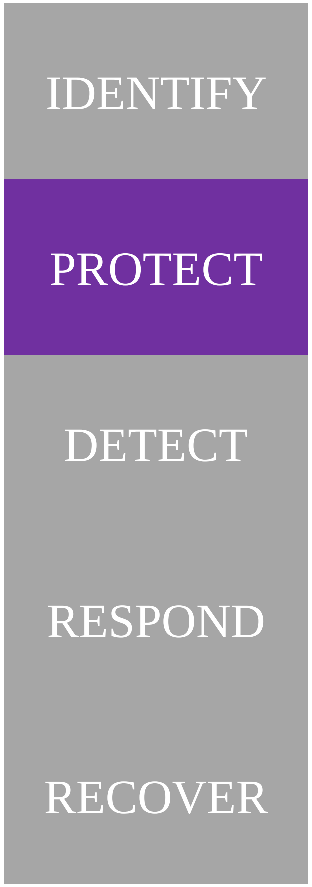
RESPOND

RECOVER

High-Level Requirements → Categories

Develop and implement the appropriate safeguards and controls to ensure delivery of critical infrastructure services..

- Access Control (PR.AC)
- Awareness and Training (PR.AT)
- Data Security (PR.DS)
- Information Protection Processes and Procedures (PR.IP)
- Maintenance (PR.MA)
- Protective Technology (PR.PT)


IDENTIFY

PROTECT

DETECT

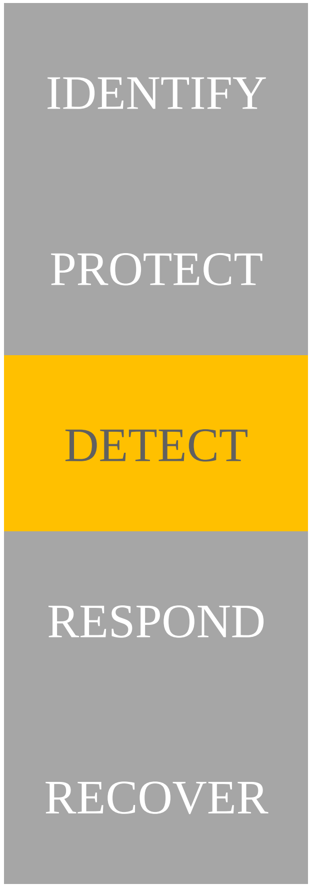
RESPOND

RECOVER

High-Level Requirements → Categories

Develop and implement the appropriate activities and controls to identify occurrence of a cybersecurity event..

- Anomalies and Events (DE.AE)
- Security Continuous Monitoring (DE.CM)
- Detection Processes (DE.DP)



IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

High-Level Requirements → Categories

Develop and implement the appropriate activities and controls to take action regarding a detected cybersecurity event.

- Response Planning (RS.PL)
- Communications (RS.CO)
- Analysis (RS.AN)
- Mitigation (RS.MI)
- Improvements (RS.IM)

IDENTIFY

PROTECT

DETECT

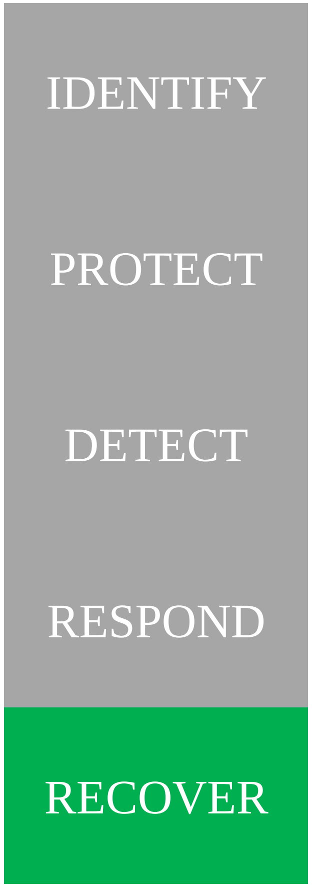
RESPOND

RECOVER

High-Level Requirements → Categories

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.

- Recovery Planning (RC.RP)
- Improvements (RC.IM)
- Communications (RC.CO)



Key Updates with CSF since Feb 2014

Privacy

- Design considerations for the privacy framework has been established.
- 2nd Privacy Engineering Workshop is scheduled for Sep 15-16, 2014

Security

- NIST released draft RFP to solicit experience from industries.
- NIST opens comment period for 45 days on Tuesday this week.
  - ***TI is looking to work with organizations and members of the chapter to support this RFI response.***

Law-making

- Increased activities on Capitol Hill to pass consensus pieces of cybersecurity legislation (data breach, information sharing, privacy protections, DHS role in cyber workforce)
- Industry-groups (Auto-ISAC, NEMA, NEI) and sector-specific regulators (SEC, DOT/NHTSA, FTC) ramp up standards and clarifications

Conclusion

- Foundational framework for cybersecurity management flexible to support any organization:
  - Applicable to many industries
  - Size or organization
  - Scalable
  - Maturity
- Offer choices of standards to assess, evaluate and monitor progress:
  - NIST
  - COBIT/ISO 27001
  - ISA
- Significant data to indicate that CSF is making good progress among industries.
- Adoption in SMBs may still need additional work.

Demo of TrustedAgent GRC using CSF

TRUSTED
INTEGRATION
SC MAGAZINE
THE GOLDEN BRIDGE AWARDS GOLD BEST 2013 BUSINESS WORLD
THE GOLDEN BRIDGE AWARDS SILVER BEST 2013 BUSINESS WORLD

Compliance Management

Audit Management

Vulnerability Management

Enterprise Risk Management

Incident Management

IT Governance

Continuous Monitoring

TrustedAgent GRC

Risk and Compliance

Policy Management

Vendor Risk Management

Governance

Thank You

Contact Information

Tuan Phan
Trusted Integration, Inc.
525 Wythe Street
Alexandria, VA 22314
Office: 703-299-9171 ext. 103
tuanp@trustedintegration.com
twitter @TrustedAgentGRC
www.trustedintegration.com

Supplement Slides

Useful References

- http://www.nist.gov/cyberframework/
- www.isaca.org/cobit/documents/cobit5-introduction.ppt
- www.27000.org/iso-27001.htm

Categories: Asset Management (ID.AM)

SUBCATEGORY	POSSIBLE ACTIVITIES
ID.AM-1: Physical devices and systems within the organization are inventoried	• Inventory of systems and key applications are documented.
ID.AM-2: Software platforms and applications within the organization are inventoried	• Hardware, software, and devices are documented against the inventories.
ID.AM-3: The organizational communication and data flow is mapped	• Data flows • Architecture diagrams • Boundary diagrams
ID.AM-4: External information systems are mapped and catalogued	• Interconnections • Cloud systems
ID.AM-5: Resources are prioritized based on the classification / criticality / business value of hardware, devices, data, and software	• Type of inventory (MA, GSS, vendor, program, data center) • Sensitivity classification • Security categorization
ID.AM-6: Workforce roles and responsibilities for business functions, including cybersecurity, are established	• Key points of contact are defined and assigned to inventories. • POCs address key roles within organization.

Categories: Business Environment (ID.BE)

SUBCATEGORY	POSSIBLE ACTIVITIES
ID.BE-1: The organization’s role in the supply chain and is identified and communicated	• A participant in any of 16 CI sectors?
ID.BE-2: The organization’s place in critical infrastructure and their industry ecosystem is identified and communicated	• Articulate in organization’s mission and objectives by management, BoD, and organizational staff. • Reflect in annual training of employees
ID.BE-3: Priorities for organizational mission, objectives, and activities are established	• Organization’s CI objectives cascade to individual annual objectives/goals
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	• Identified SLAs or MOUs for interconnections • Cloud deployment models • Cloud service models
ID.BE-5: Resilience requirements to support delivery of critical services are established	• FMEA/FTA/HAZOP or any other criticality assessments performed to determine weaknesses within the supply of the critical services

Categories: Governance (ID.GV)

SUBCATEGORY	POSSIBLE ACTIVITIES
ID.GV-1: Organizational information security policy is established	• Established policies and procedures supporting CI and management of cybersecurity.
ID.GV-2: Information security roles & responsibility are coordinated and aligned	• Established POCs for inventories that address the key security roles.
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	• Identified governing regulations, and standards • Policies and procedures reference applicable regulations, or standards
ID.GV-4: Governance and risk management processes address cybersecurity risks	• Use of risk management approach that is adopted and place into practice by BOD and senior management.

Categories: Risk Assessment (ID.RA)

SUBCATEGORY	POSSIBLE ACTIVITIES
ID.RA-1: Asset vulnerabilities are identified and documented	• Use of vulnerability assessment tools and map findings from tools to impacted assets.
ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources.	• Use of NIST NVD, ISACs • Subscribe through vulnerability assessment tools
ID.RA-3: Threats to organizational assets are identified and documented	• Use of risk assessment per NIST 800-30 and standardized threat vectors
ID.RA-4: Potential impacts are analyzed	• Likelihood and impact levels are determined • Assigned risk levels to identified findings
ID.RA-5: Risk responses are identified.	• Findings include recommended mitigation actions

Categories: Risk Management (ID.RM)

SUBCATEGORY	POSSIBLE ACTIVITIES
ID.RM-1: Risk management processes are managed and agreed to	• Risk management methodology is clearly defined as part of the CI or IS program.
ID.RM-2: Organizational risk tolerance is determined and clearly expressed	• Risk appetite/tolerance is defined.
ID.RM-3: The organization’s determination of risk tolerance is informed by their role in critical infrastructure and sector specific risk analysis	• Risk tolerance must be comparable to the sector.

Categories: Access Control (PR.AC)

SUBCATEGORY	POSSIBLE ACTIVITIES
PR.AC-1: Identities and credentials are managed for authorized devices and users	• Users are uniquely identified and authenticated before granting access to resources.
PR.AC-2: Physical access to resources is managed and secured	• Use of physical security, locks, gates, guards, and perhaps dogs!
PR.AC-3: Remote access is managed	• Remote access requires additional security measures including more complex passwords with shorten validity period. • Multi-factor authentication
PR.AC-4: Access permissions are managed	• User access is reviewed, authorized, based on approved role, before granting access.
PR.AC-5: Network integrity is protected	• Information flow enforcement is place.

Categories: Awareness and Training (PR.AT)

SUBCATEGORY	POSSIBLE ACTIVITIES
PR.AT-1: General users are informed and trained	• Users are trained based on their roles and responsibilities within the organization. • Training covers everyone! • Vendors, suppliers, and other third-party providers acknowledge their roles and responsibilities through contracts.
PR.AT-2: Privileged users understand roles & responsibilities	
PR.AT-3: Third-party stakeholders (suppliers, customers, partners) understand roles & responsibilities	
PR.AT-4: Senior executives understand roles & responsibilities	
PR.AT-5: Physical and information security personnel understand roles & responsibilities	

Categories: Data Security (PR.DS)

SUBCATEGORY	POSSIBLE ACTIVITIES
PR.DS-1: Data-at-rest is protected	• Use of data encryption, firewalls, filtering routers, etc.
PR.DS-2: Data-in-motion is secured	• Communication paths are protected using physical and logical means (SSL, encryption)
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	• Assets are updated from inventories when they are no longer in use.
PR.DS-4: Adequate capacity to ensure availability is maintained.	
PR.DS-5: There is protection against data leaks	• Use of boundary protection mechanisms.
PR.DS-6: Intellectual property is protected	
PR.DS-7: Unnecessary assets are eliminated	• Assets are updated from inventories when they are no longer in use. • Inventories are updated when they disposed (end-of-life).
PR.DS-8: Separate testing environments are used in system development	• Use of DEV and VAL environments separately from PROD environment
PR.DS-9: Privacy of individuals and personally identifiable information (PII) is protected	• Use of recommended privacy controls

Categories: Information Protection Processes and Procedures (PR.IP)

SUBCATEGORY	POSSIBLE ACTIVITIES
PR.IP-1: A baseline configuration of information technology/operational technology systems is created	• Use of security configuration baseline for computing assets (FDCC)
PR.IP-2: A System Development Life Cycle to manage systems is implemented	• Inventories must contain appropriate SDLC status.
PR.IP-3: Configuration change control processes are in place	• CM policies and procedures are in place. • Configuration changes are tracked.
PR.IP-4: Backups of information are managed	• Data backup/archive policies and procedures addressing both onsite and offsite storage.
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.	• Assortments of physical and environment controls are implemented for inventories. Reference NIST PE family.
PR.IP-6: Information is destroyed according to policy and requirements	• Policies and procedures manage destruction of information including archives on data backups.

Categories: Information Protection Processes and Procedures (PR.IP)

SUBCATEGORY	POSSIBLE ACTIVITIES
PR.IP-7: Protection processes are continuously improved	• Ensure a culture of ongoing improvements
PR.IP-8: Information sharing occurs with appropriate parties	• Information are shared with authorized staff to ensure ongoing learning and improvemements
PR.IP-9: Response plans (Business Continuity Plan(s), Disaster Recovery Plan(s), Incident Handling Plan(s)) are in place and managed	• Formal use of BCP and ITCP
PR.IP-10: Response plans are exercised	• Plans are tested on periodic basis
PR.IP-11: Cybersecurity is included in human resources practices (de-provisioning, personnel screening, etc.)	• Management of staff and key personnel access to IT resources accordingly to role changes and termination.

Categories: Maintenance (PR.MA)

SUBCATEGORY	POSSIBLE ACTIVITIES
PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	• Frequency of maintenance is defined • Use of maintenance notifications • Document of organization's facilitated maintenance activities/logs • Document of vendor-provided maintenance activities
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access and supports availability requirements for important operational and information systems.	• Automated audit trails • Readily available for reviews and reports

Categories: Protective Technology (PR.PT)

SUBCATEGORY	POSSIBLE ACTIVITIES
PR.PT-1: Audit and log records are stored in accordance with audit policy	• Audit trails, at the minimum, should contain previous state, current state, by whom, and when.
PR.PT-2: Removable media are protected according to a specified policy	• Safeguards of data backup tapes or removable media.
PR.PT-3: Access to systems and assets is appropriately controlled	• Access is reviewed and authorized. • Use of physical and logic access controls to org assets. • Access is monitored.
PR.PT-4: Communications networks are secured	• Wireless access is managed
PR.PT-5: Specialized systems are protected according to the risk analysis (SCADA, ICS, DCS)	• Depth of protections must be comparable to the type of control systems.

Categories: Anomalies and Events (DE.AE)

SUBCATEGORY	POSSIBLE ACTIVITIES
DE.AE-1: A baseline of normal operations and procedures is identified and managed	• Inventories are subjected to monitoring as part of an enterprise-wide continuous monitoring program. • Monitoring takes place on IT systems both internal and external. • Incidents are reported and managed. Notifications are employed where appropriate. • Impact levels including any regulatory reporting are defined (i.e. HIPAA breach requirements, PII) • Issues are tracked until fully remedied as part of a corrective action management.
DE.AE-2: Detected events are analyzed to understand attack targets and methods	
DE.AE-3: Cybersecurity data are correlated from diverse information sources	
DE.AE-4: Impact of potential cybersecurity events is determined.	
DE.AE-5: Incident alert thresholds are created	

Categories: Security Continuous Monitoring (DE.CM)

SUBCATEGORY	POSSIBLE ACTIVITIES
DE.CM-1: The network is monitored to detect potential cybersecurity events	• Use of IDS and IPS • Notifications of suspicious activities
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	• Cameras, ground/remote sensors, alarms
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	• Access logs are reviewed for pattern of miss-use of unauthorized or repeated failed accesses.
DE.CM-4: Malicious code is detected	• Use of anti-virus and anti-spyware on computing devices. • Staff are trained on what to do in case of detection.
DE.CM-5: Unauthorized mobile code is detected	• Control of user environment - FDCC
DE.CM-6: External service providers are monitored	• Access of non-organizational users should be verified/monitored based on roles, risk profile and frequency.
DE.CM-7: Unauthorized resources are monitored	• Logs should be inspected for attempted access to unauthorized resources.
DE.CM-8: Vulnerability assessments are performed	• Network scans, pen testing are periodically performed. • Frequency and depth should be comparable to cybersecurity risk of the sector

Categories: Detection Processes (DE.DP)

SUBCATEGORY	POSSIBLE ACTIVITIES
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	• POCs are defined for the incident response/BCP and inventories.
DE.DP-2: Detection activities comply with all applicable requirements, including those related to privacy and civil liberties	• Inventories may subject to the requirements of conformity assessment, privacy review, or security authorization processes.
DE.DP-3: Detection processes are exercised to ensure readiness	• Applicable controls are tested for the inventories and their response plans to ensure effectiveness.
DE.DP-4: Event detection information is communicated to appropriate parties	• Notifications are sent to response
DE.DP-5: Detection processes are continuously improved	• Use of automation detection technologies including SIEM, IDS, IPS, etc.

Categories: Response Planning (RS.PL)

SUBCATEGORY	POSSIBLE ACTIVITIES
RS.PL-1: Response plan is implemented during or after an event.	• Incident response process is in place within threshold of incident reporting as established by the organization.

Categories: Communications (RS.CO)

SUBCATEGORY	POSSIBLE ACTIVITIES
RS.CO-1: Personnel know their roles and order of operations when a response is needed	• Annual training on incident response and BCP
RS.CO-2: Events are reported consistent with established criteria	• Thresholds of initial reviews, notifications (internal) and external notifications should be clearly defined along with the oversight required to ensure their practices are consistent to governing regulations.
RS.CO-3: Detection/response information, such as breach reporting requirements, is shared consistent with response plans, including those related to privacy and civil liberties	• If incidents involved PII or PHI, privacy personnel should be included. • Where applicable, depending on size, reports on PII and PHI breach also go to HHS.
RS.CO-4: Coordination with stakeholders occurs consistent with response plans, including those related to privacy and civil liberties	
RS.CO-5: Voluntary coordination occurs with external stakeholders (ex, business partners, information sharing and analysis centers, customers)	• Communication is encouraged, not required.

Categories: Analysis (RS.AN)

SUBCATEGORY	POSSIBLE ACTIVITIES
RS.AN-1: Notifications from the detection system are investigated	• Incident/issue reported must be investigated.
RS.AN-2: Understand the impact of the incident	• Risk analysis to be taken to determine if incident exceeds the risk tolerance defined for the organization requiring additional actions or violates any regulatory requirements.
RS.AN-3: Forensics are performed	• Some incidents may require extended forensic reviews including logs, file reconstructions, file and offsite backups, etc.
RS.AN-4: Incidents are classified consistent with response plans	• Incident management must follow defined policies and procedures, and is according to established thresholds.

Categories: Mitigation (RS.MI)

SUBCATEGORY	POSSIBLE ACTIVITIES
RS.MI-1: Incidents are contained	• Mechanisms to track incidents/issues • Mechanisms to identify activities to contain the incidents. Need to be able to formulate corrective action plan and related milestones and assign them to various owners. • Mechanisms to gain visibility to outstanding CAs/issues and their remediation plan
RS.MI-2: Incidents are eradicated	

Categories: Improvements (RS.IM)

SUBCATEGORY	POSSIBLE ACTIVITIES
RS.IM-1: Response plans incorporate lessons learned	• Use of lessons learned. • Policies and procedures are periodically updated. • Incorporated into annual training
RS.IM-2: Response strategies are updated	• Incident response strategies reflect current P&P.

Categories: Recovery Planning (RC.RP)

SUBCATEGORY	POSSIBLE ACTIVITIES
RC.RP-1: Recovery plan is executed	• Recovery processes are tested and maintained.

Categories: Improvements (RC.IM)

SUBCATEGORY	POSSIBLE ACTIVITIES
RC.IM-1: Plans are updated with lessons learned	• BCP and incident response plan are updated on a regular basis. • Personnel contact updates
RC.IM-2: Recovery strategy is updated	• Changes in technology and practices as well as supporting infrastructure impact recovery strategies.

Categories: Communications (RC.CO)

SUBCATEGORY	POSSIBLE ACTIVITIES
RC.CO-1: Public Relations are managed	• Breach notification according to governing regulations to regulatory bodies • Prompt notifications to impacted consumers.
RC.CO-2: Reputation after an event is repaired	• Credit monitoring offer for one year for impacted people in PII or credit cards (Target, Michaels)