# Implementing an IT Risk Program using the NIST Cyber Security Framework

**NY State Cyber Security Conference**

**June 2016**

**Bobby Dominguez**
**Chief Strategy & Security Officer**
**Lynx Technology Partners, Inc.**

https://www.linkedin.com/in/bobbydominguez
https://twitter.com/Moonraker069
bdominguez@lynxtp.com

The content and opinions expressed herein are solely those of the author, and neither represent the views nor describe the current or intended practices of any other entity. The information in this presentation contains references to copyrighted material; The author makes no claims of ownership or rights to such material.

Copyright © 2016 Lynx Technology Partners, Inc. All Rights Reserved.

# Obligatory Disclaimer

- Any statements made in the course of this presentation should not be relied on as a commitment of present or future, directly on behalf of my employer, this forum's management, the National Football League, or any other major institution that your barracuda lawyer may opt to pursue in the name of earning his or her outrageous legal fees.
- The opinions expressed herein are not necessarily those of my employer, not necessarily mine, and probably not necessary.
- My opinions are subject to change without notice.
- Thanks for disagreeing.

# Abstract

The NIST Cyber Security Framework (CSF) from 2013, based on existing standards, was created to reduce cyber risks to critical infrastructure. In this session Bobby Dominguez will describe the key elements of the NIST CSF, and will focus on best practices for leveraging the CSF to implement an IT Risk Program. Specific examples and tools for operationalizing the framework will be reviewed.

The discussion will be of value to those who have already deployed the CSF and to those who are new to the framework and its benefits. Interaction with those that have not deployed the CSF will be encouraged, and they will be asked to share their intentions and expectations for deploying the CSF.



LYNX TECHNOLOGY PARTNERS

# Biography

- **Certifications**
  - CISSP, CPP, CRISC, ITIL, PMP, PPMC, GISO, GSLC, C|CISO, EIEIO
- **Organizations**
  - Infragard – President, Board of Directors
    - FBI Sector Chief for Financial Services
    - FBI Citizens Academy 2014 Graduate
  - USSS Electronic Crimes Task Force
  - ISSA – Vice President, Board of Directors
- **Awards**
  - 2008 Top 5 “Best Security Team in the US” SC Magazine
  - 2009, 2010, 2013 Top 5 “CSO of the Year” SC Magazine
  - 2012 Finalist Information Security Leadership Award (ISC)2
  - 2012 ISE North America Executive Leadership Award Nominee

Internet entrepreneur & über geek who groks e-commerce, IT, security, risk & privacy management caffeinated beverages, Padrón cigars, 18-yo single malt scotch & dark beers

LYNX TECHNOLOGY PARTNERS

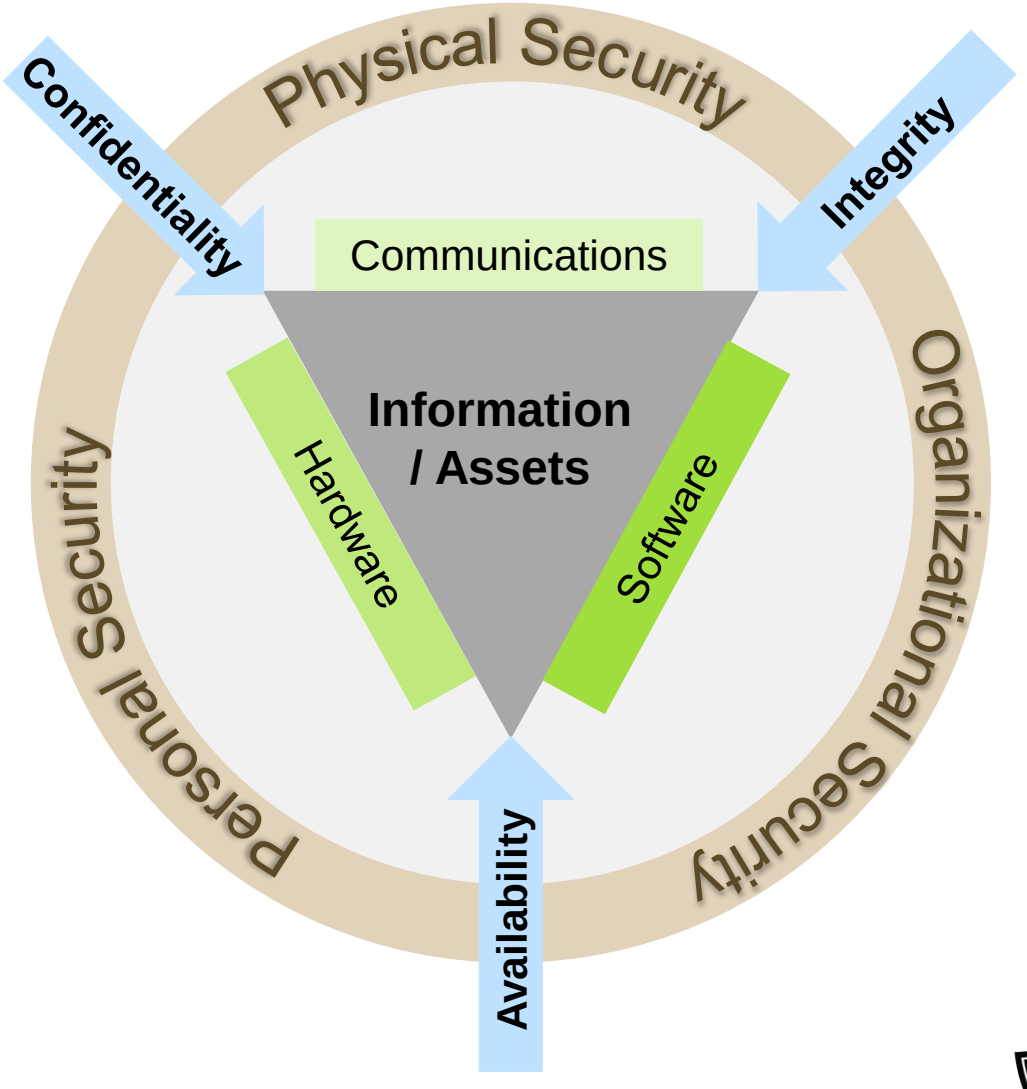
# CSO Magazine – Sept 28, 2013

”Some of the harshest assessments of the framework flow from cybersecurity specialists steeped in their disciplines and typically responsible for the day-to-day oversight of cybersecurity systems. **"Our industry keeps fracturing security standards**," one Chief Information Risk Officer for a major financial institution said, referring to the multiplicity of frameworks that his and other organizations are currently attempting to follow. "**The NIST framework is just another fracture. This is just another layer and it will create more work.**"

LYNX TECHNOLOGY PARTNERS

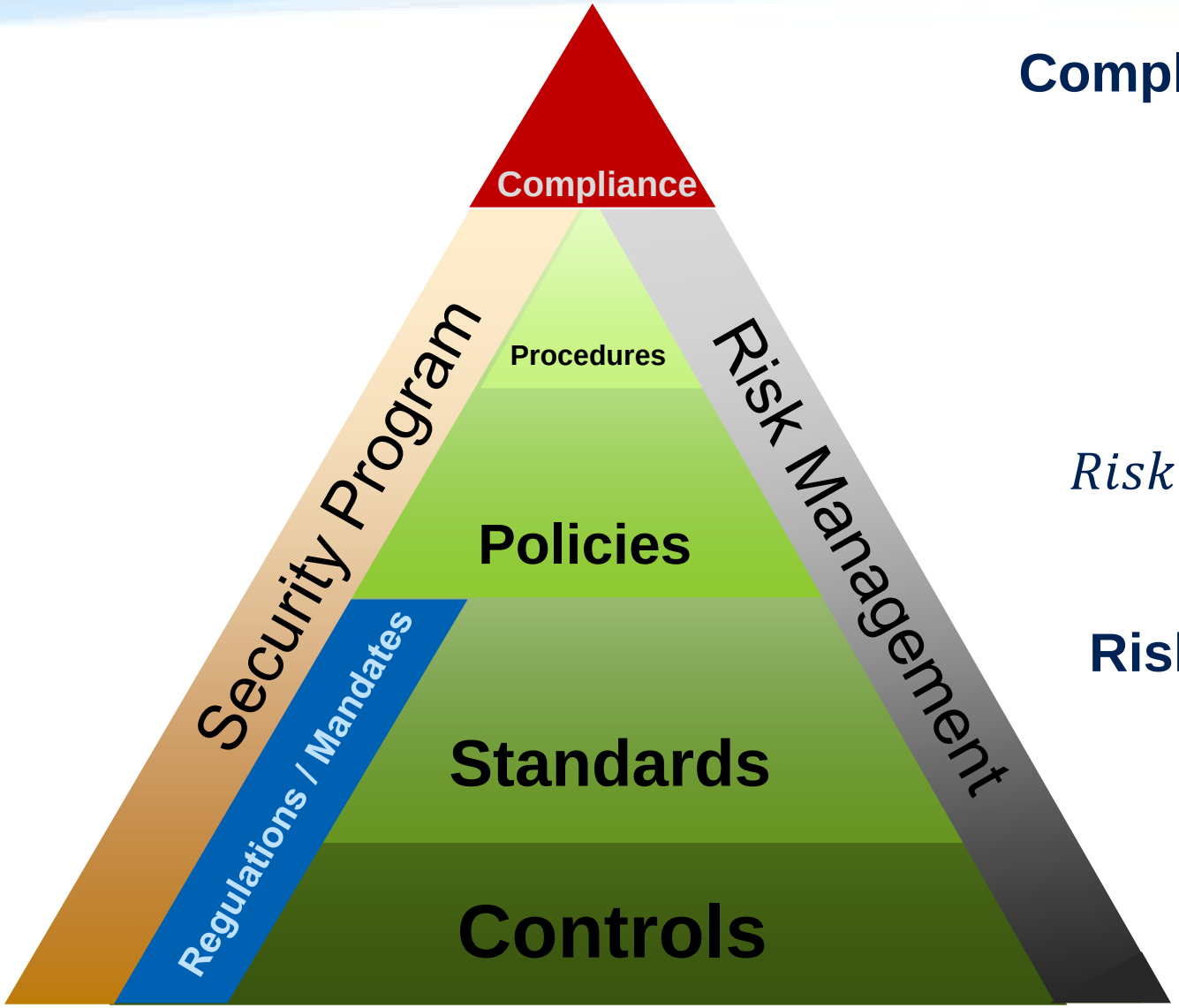
# Basic Definitions – IT Security

The practice of defending something from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction




**Confidentiality, Integrity, Availability**

# Basic Definitions – IT Risk & Compliance

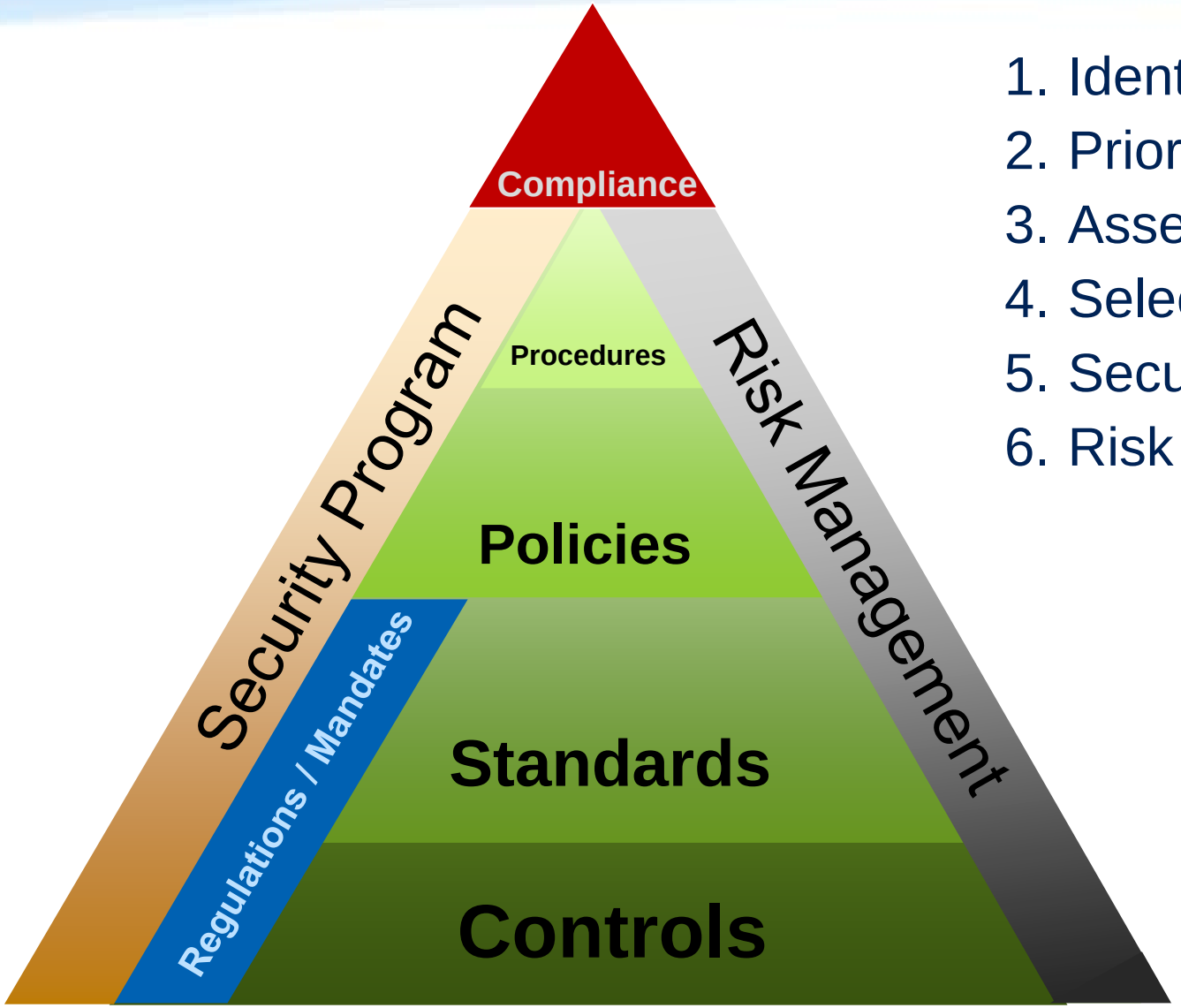



**Compliance** = a state of being in accordance with established guidelines or specifications, or the process of becoming so.

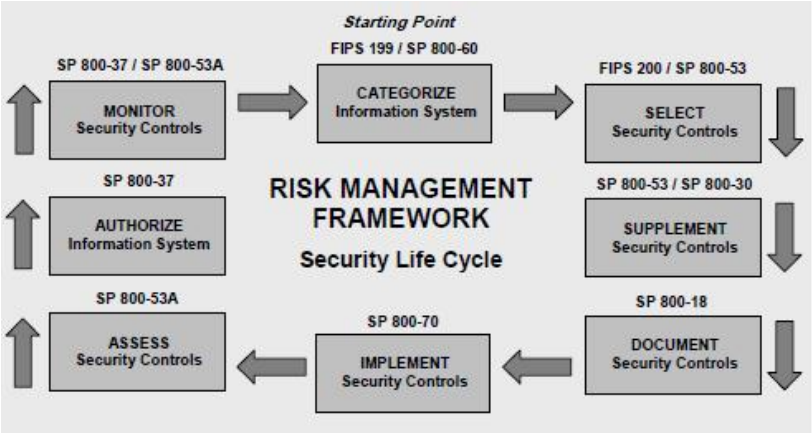
$$Risk = \frac{(Vulnerability\ x\ Threat)}{Counter\ Measure\ Score}\ x\ Valuation$$

**Risk** = Likelihood (probability) *x* Impact ($$)

# Basic Definitions – IT Risk & Compliance




1. Identify the assets
2. Prioritize importance to business
3. Assess risks
4. Select controls that address risks
5. Security Program implements controls
6. Risk Management Lifecycle



# Executive Order 13636
## Improving Critical Infrastructure CyberSecurity

- February 12, 2013, President Obama signed Executive Order

  http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

- **Identification of Critical Infrastructure**
- **IT Carve-out** – Prohibition from identifying any commercial information technology products or consumer information technology services
- **Cyber Security Framework (CSF)**
- **Agency Review** – Preliminary CSF to be reviewed by all Executive Branch agencies and regulatory agencies encouraged to use CSF within their own domains.
- **Voluntary Adoption of Framework** – Propose legislative incentives
- **Information Sharing**

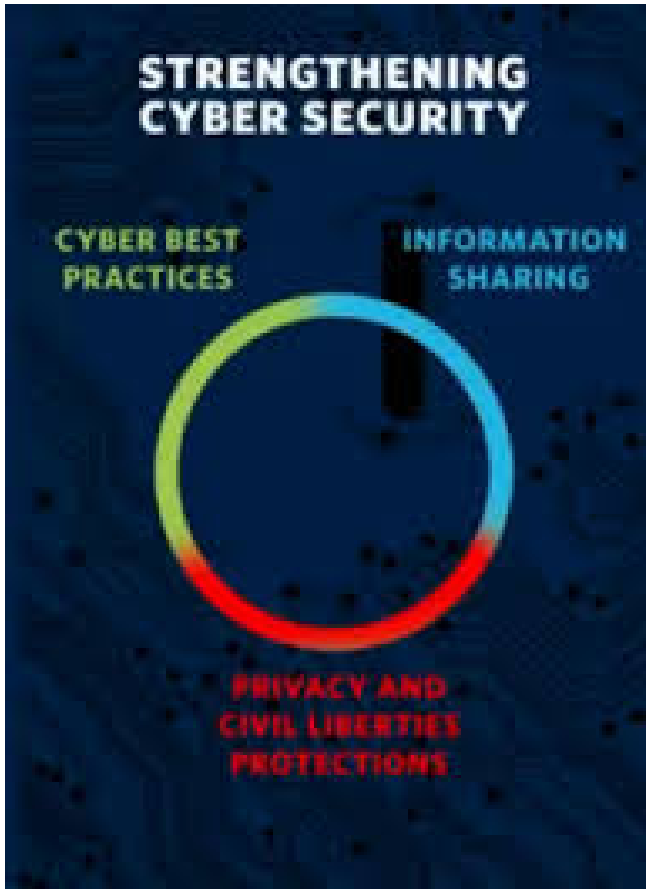


LYNX TECHNOLOGY PARTNERS

# Cyber Security Framework (CSF)

Framework provides a common language and mechanism for organizations to:

1) Describe their current cyber security posture
2) Describe their target state for cyber security
3) Identify and prioritize opportunities for improvement within the context of risk management
4) Assess progress toward the target state
5) Foster communications among internal and external stakeholders



# Overview of CSF: Core

The Framework is a risk-based approach composed of three parts: **Core**, **Profile**, and **Tiers**

## Framework Core

- 5 core functions
- 20 categories
- 97 sub-categories
- Informative references:
  - COBIT, ISA, ISO 27000, NIST SP800-53r4, CCS CSC, HIPAA, PCI DSS, GLBA, etc.
- Privacy methodology for each function

Figure 1: Framework Core Structure

| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| ID | Identify | AM | Asset Management |
| | | BE | Business Environment |
| | | GV | Governance |
| | | RA | Risk Assessment |
| | | RM | Risk Management |
| PR | Protect | AC | Access Control |
| | | AT | Awareness & Training |
| | | DS | Data Security |
| | | IP | Information Protection Processes & Procedures |
| | | PT | Protective Technology |
| DE | Detect | AE | Anomalies & Events |
| | | CM | Security Continuous Monitoring |
| | | DP | Detection Processes |
| RS | Respond | CO | Communications |
| | | AN | Analysis |
| | | MI | Mitigation |
| | | IM | Improvements |
| RC | Recover | RP | Recovery Planning |
| | | IM | Improvements |
| | | CO | Communications |

# CSF as a Foundation

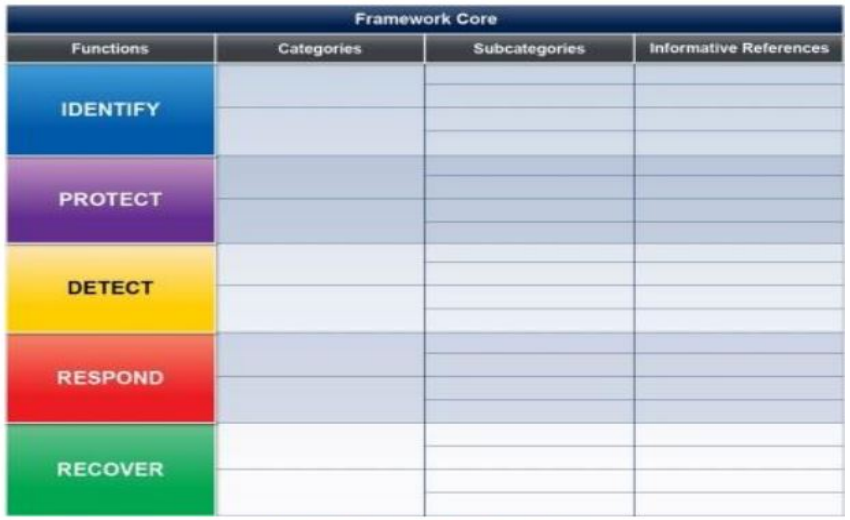



Figure 1: Framework Core Structure

- Tolerance Levels
- Monitoring
- Metrics
- Reporting

- Policies
- Procedures
- Standards
- Technologies

The CSF can be the **foundation** that drives the creation of **policy** and **control activities** to **mitigate risk**. Tolerance levels can be set to measure **control effectiveness** and influence future **risk mitigation activities**.



LYNX TECHNOLOGY PARTNERS

# Example of How Core Maps to Controls

- The **Protect** Function
  - Includes the Category **Data Security**
    - Sub-Category PR.DS-2: “Data-in-transit is protected”
      - An Informative Reference ***ISO/IEC 27001 Control A.10.8.3***, “Data during transportation / transmission is protected to achieve confidentiality, integrity, and availability goals”



LYNX TECHNOLOGY PARTNERS

# Overview of CSF: Profile

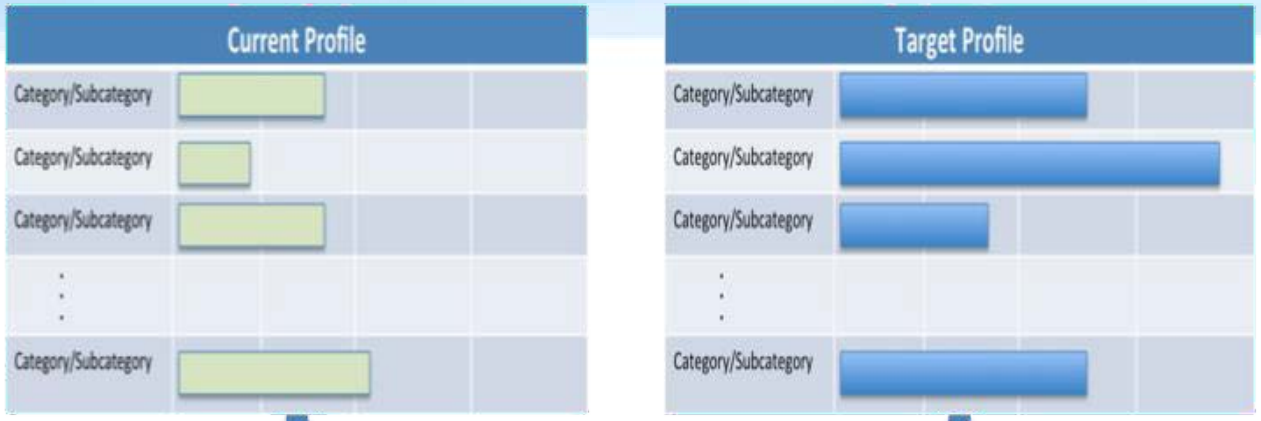
## Framework Profile

- The Profile is the alignment of the Functions, Categories, Subcategories and Controls (industry standards and best practices) with the business requirements, risk tolerance, and resources of the organization
- Helps establish a roadmap for reducing cybersecurity risk that is well aligned with organization and sector goals, considers legal /regulatory requirements and industry best practices, and reflects risk management priorities
- Lets you identify opportunities for improving cybersecurity by comparing a “Current” Profile with a “Target” Profile, revealing gaps that should be addressed to meet objectives



LYNX TECHNOLOGY PARTNERS

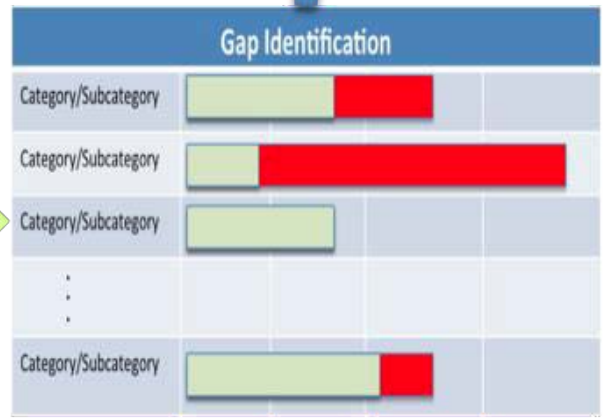
# Profile Calculation




The Current Profile indicates the cybersecurity outcomes that are currently being achieved.

The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals.

The Target Profile is built to support business / mission requirements and aid in the communication of risk within and between organizations.




Identifying the gaps between the Current Profile and the Target Profile allows the creation of a prioritized roadmap that organizations will implement to reduce cybersecurity risk.

The prioritization of the gaps is driven by the organization's Risk Management Processes and serve as an essential part for resource and time estimates needed that are critical to prioritization decisions.

**Target State – Current State = Gaps**



LYNX TECHNOLOGY PARTNERS

# Example of Profile Calculation

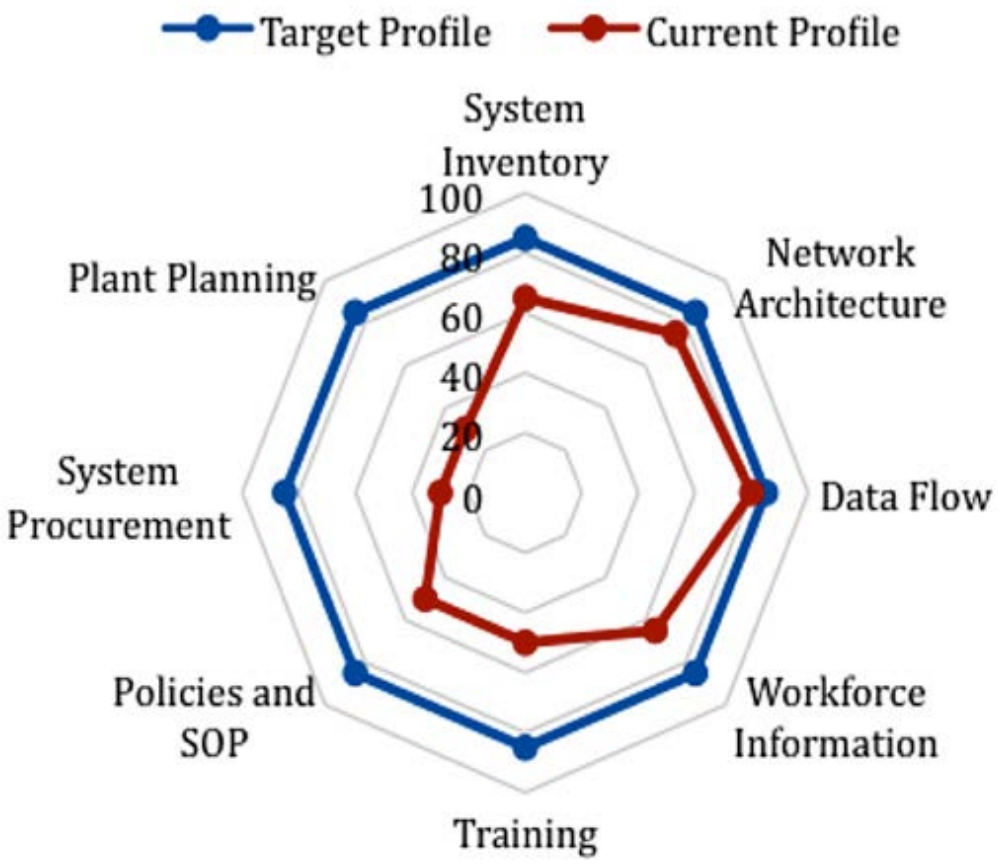
- The *"Protect"* **Function**
  - *"Data Security"* **Category**
    - *"Data-in-transit is protected"* **Sub-Category PR.DS-2**
      - *"ISO/IEC 27001 Control A.10.8.3"* **Informative Reference**
        - *"Data during transportation / transmission is protected to achieve confidentiality, integrity, and availability goals"* **Control**
          - *"Confidential data must always be encrypted when stored on computer media (magnetic tapes, floppy, optical disks, etc.), including backup media or when electronically transmitted via any method."* **Policy Statement**
            - *"% of PII applications with encryption"* **Metric**
              - **Rating**

| Function | Category | Control Expectation | Metric | Rating |
|---|---|---|---|---|
| Protect | Data Security | All PII will be encrypted at all times | % of PII applications with encryption | 75% |



LYNX TECHNOLOGY PARTNERS

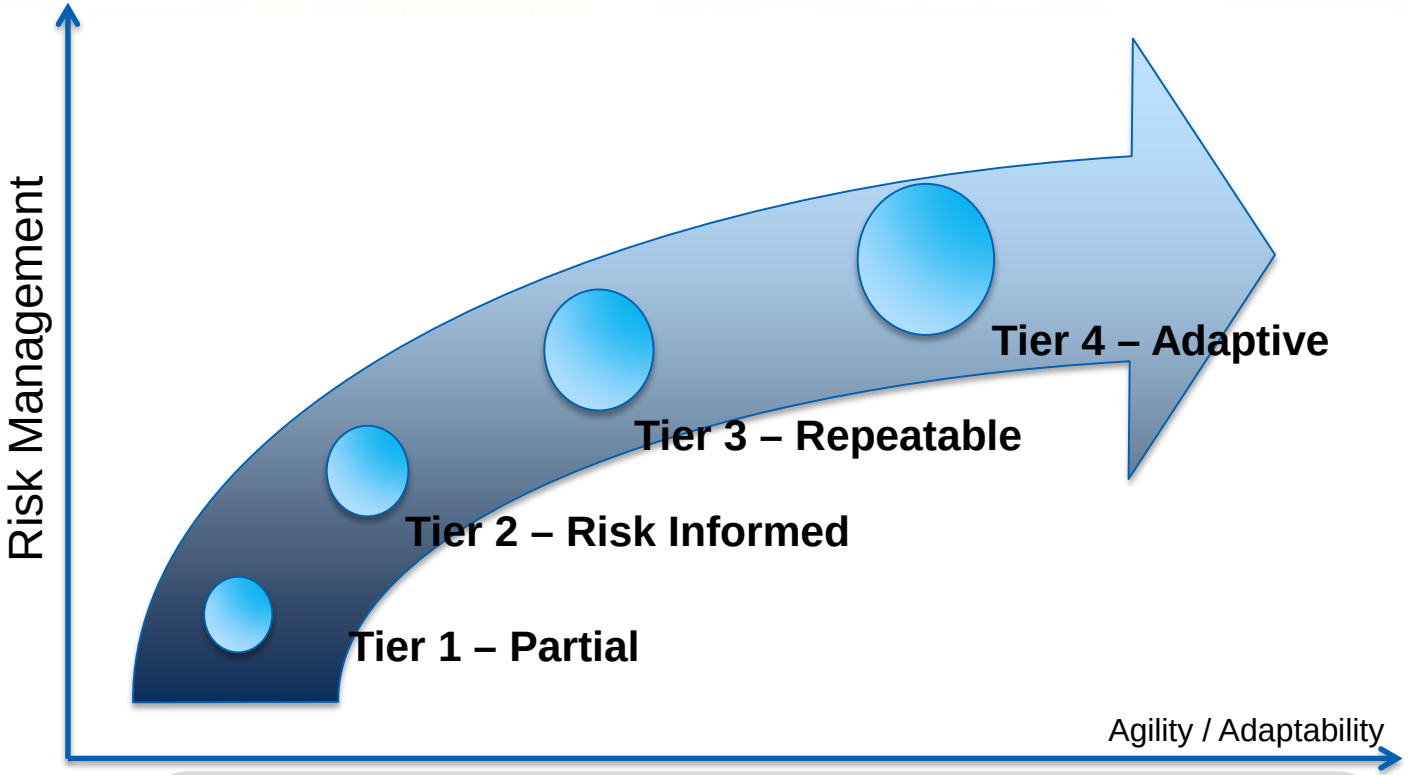
# Example of Profile for ICS



# Overview of CSF: Tiers

## Framework Tiers

- The Tier selection process considers an organization's current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.
- The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4), progressing from informal, reactive implementations to approaches that are agile and risk-informed.




- Defensive
- Tactical
- Event-driven
- Retrospective metrics
- Internal data
- Plan for imagined events

Maturity

- Offensive
- Strategic
- Contextual
- Prospective metrics
- External data
- Foresee unimagined events



LYNX TECHNOLOGY PARTNERS

# Steps to Apply CSF

The following recommended recursive steps illustrate how an organization could use the Framework to create a new cybersecurity program or improve an existing cybersecurity program:

1. **Identify** – The organization identifies its mission objectives, related systems and assets, regulatory requirements and overall risk approach.

2. **Create a Current Profile** – Beginning with the Categories specified in the Framework Core, the organization develops a Current Profile that reflects its understanding of its current cybersecurity outcomes based on its implementation of the Identify Function.

3. **Conduct a Risk Assessment** – The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that critical infrastructure organizations seek to incorporate emergent risks and outside threat data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.



LYNX TECHNOLOGY PARTNERS

# Steps to Apply CSF (continued)

4. **Create a Target Profile** – The organization creates a Target Profile that focuses on the assessment of the Framework Elements (e.g., Categories, Subcategories) describing the organization's desired cybersecurity outcomes.

5. **Determine, Analyze, and Prioritize Gaps** – The organization compares the Current Profile and the Target Profile to determine gaps, and then determines resources necessary to address the gaps. The organization creates a prioritized action plan that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The use of Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports cost/benefit analysis, and enables the organization to perform targeted improvements.

6. **Implement Action Plan** – The organization implements the steps defined in the action plan and monitors its current cybersecurity practices against the Target Profile.



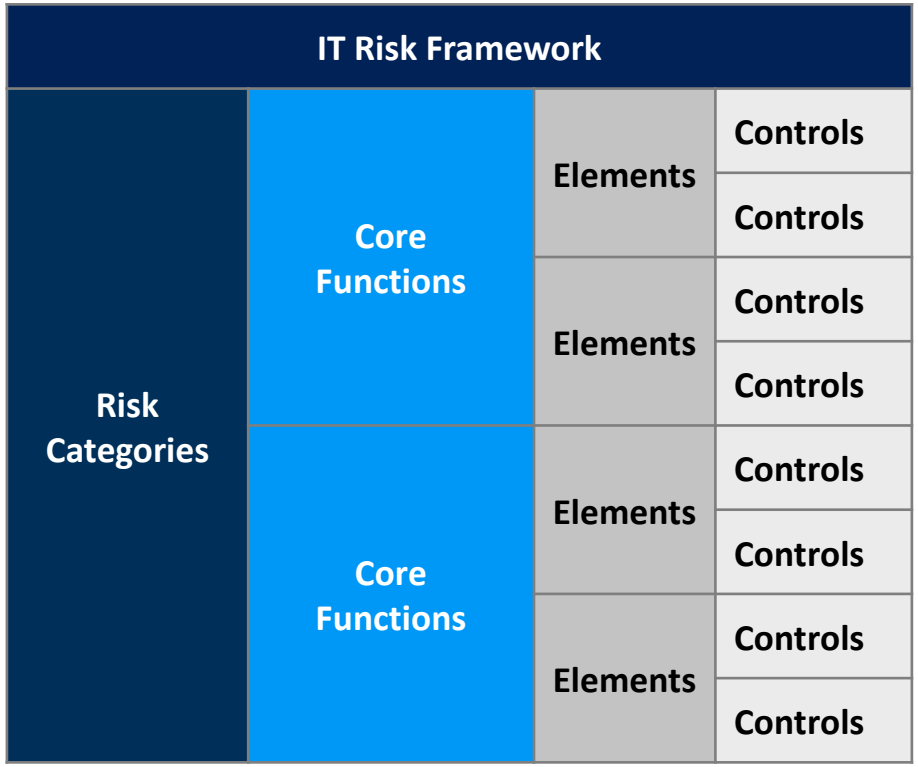
LYNX TECHNOLOGY PARTNERS

# A Real World Example of a Risk Framework

Common Practices
(COBIT, ISO, SANS)

Industry Standards
(NERC CIP, FFIEC, PCI)

Laws & Regulations
(OCC, GLBA, HIPAA)




- Enterprise control coverage with functional ownership
- Demonstrates adherence to
  - Industry best practices and standards
  - Applicable laws
  - Regulatory requirements
- Reports Core Function through 5 risk categories
- Note differences between original CSF and this Framework

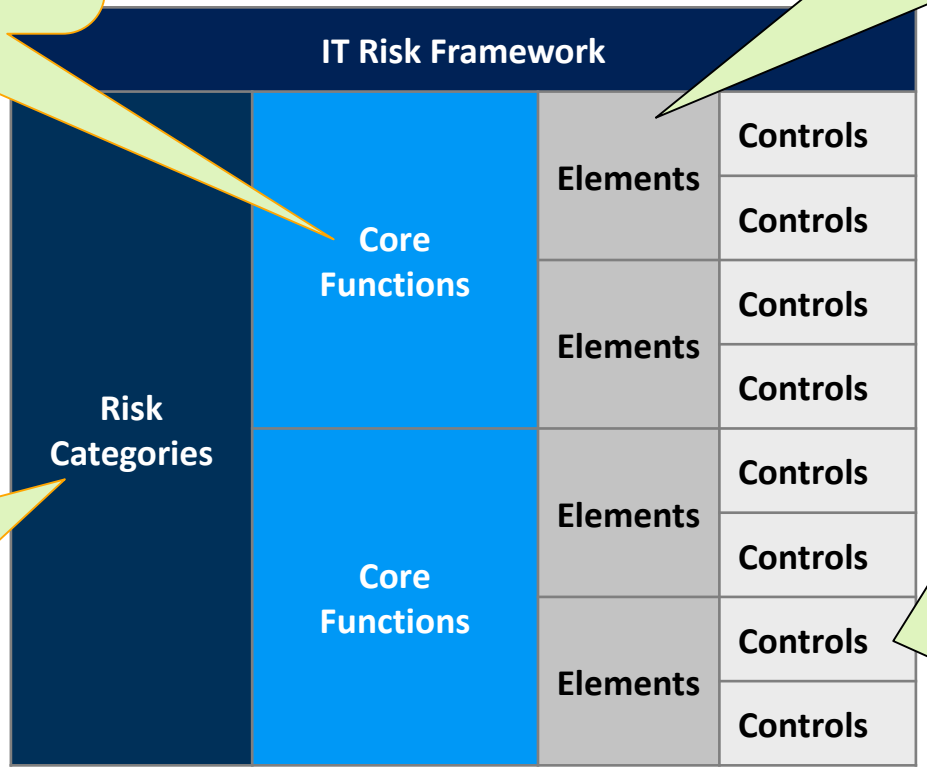


LYNX TECHNOLOGY PARTNERS

# A Real World Example of a Risk Framework

**Core Function**
IT Capability (e.g. , Access Management)

**Element** – a specific IT process (e.g., Privileged Access Controls)



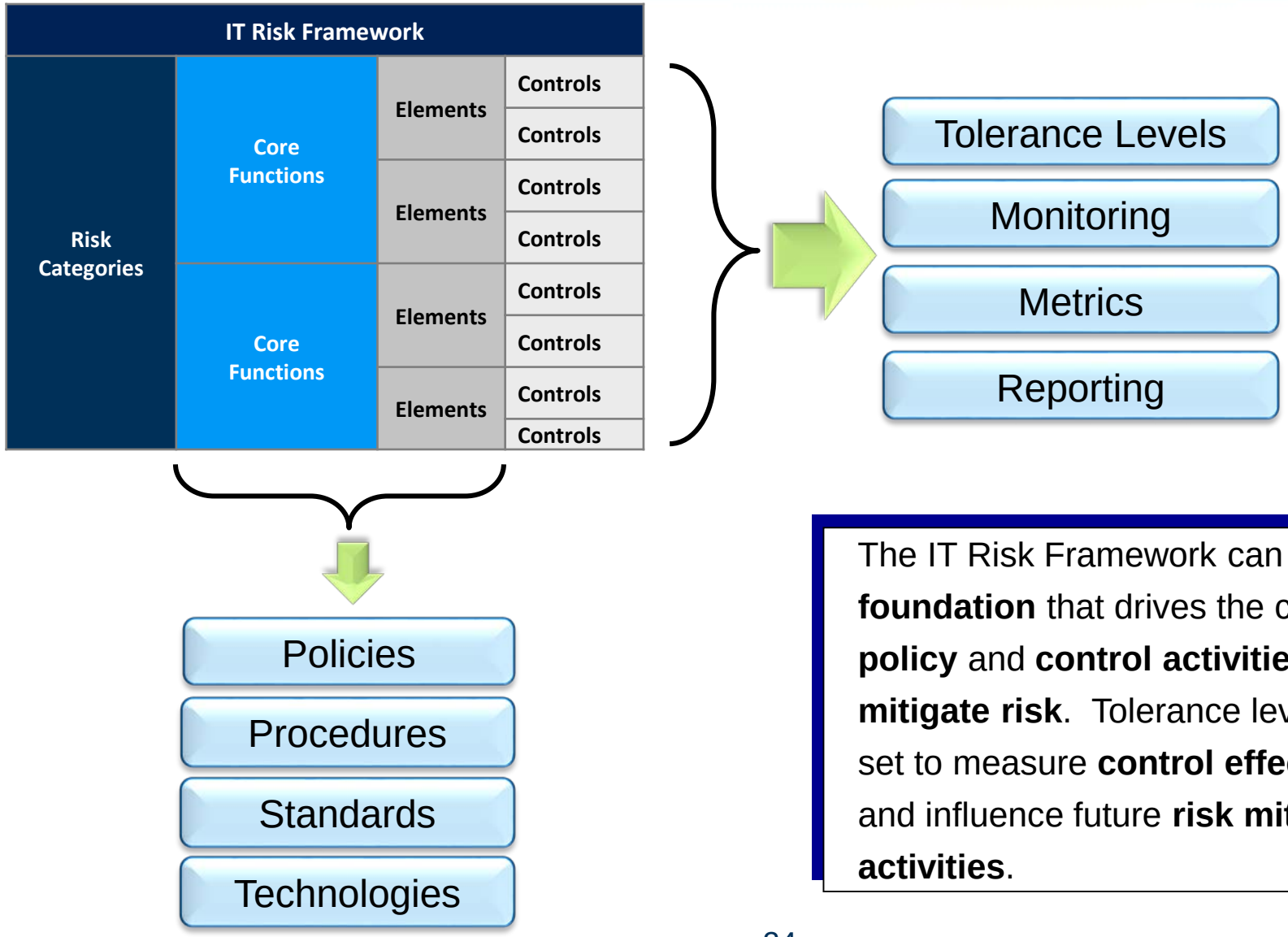

**Control**
A specific activity performed by persons or systems designed to ensure that business objectives are met. (e.g. Periodic review of access)

**Risk Category**
An aggregate view of core functions (e.g., Cyber Security)



LYNX TECHNOLOGY PARTNERS

# A Real World Example of a Risk Framework

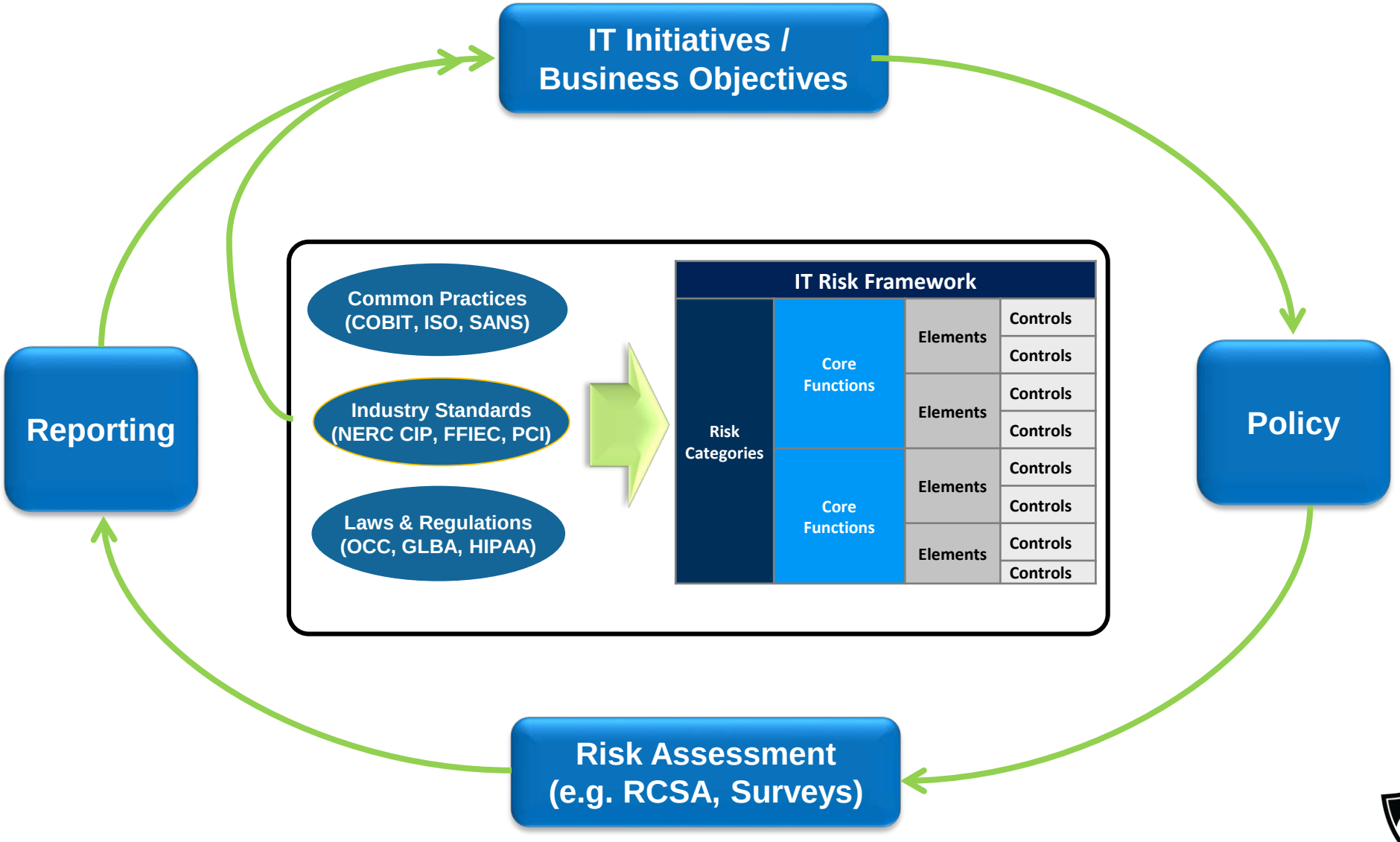



The IT Risk Framework can be the **foundation** that drives the creation of **policy** and **control activities** to **mitigate risk**. Tolerance levels can be set to measure **control effectiveness** and influence future **risk mitigation activities**.



LYNX TECHNOLOGY PARTNERS

# IT Risk Framework Interdependencies





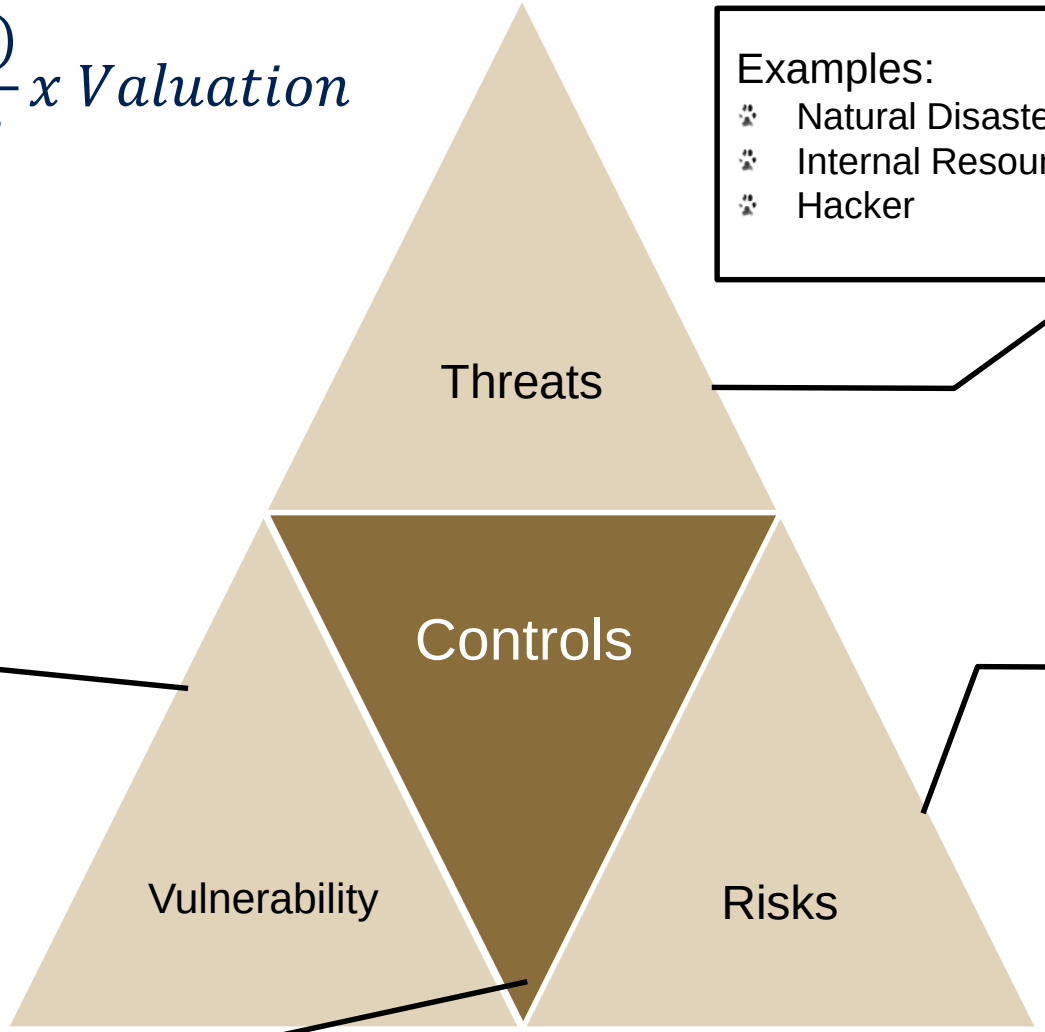

LYNX TECHNOLOGY PARTNERS

# What are your Risks?

$$Risk = \frac{(Vulnerability\ x\ Threat)}{Counter\ Measure\ Score}\ x\ Valuation$$

Examples:
- Natural Disaster
- Internal Resource
- Hacker
- Malicious Code
- Technical Failure
- External Parties

Examples:
- Lack of procedures for **Cyber Security – Access**
- Lack of procedures for **Business Continuity Management**




Authorization processes which do not control user privileges **may result in users gaining access to information beyond an appropriate level** based on their job function.

Implement & monitor controls to mitigate risk



LYNX TECHNOLOGY PARTNERS

# Create a Risk Library

| 1 | Major Risk Category (Basel) | Major Risk Category Description | # | Significant Risk Category | Significant Risk Category Definition | # | Detailed Risk | Detailed Risk Definition | Includes | Excludes |
|---|---|---|---|---|---|---|---|---|---|---|
| 36 | **Damage to Physical Assets** | Losses arising from loss or damage to physical assets from natural disaster or other events. | 9 | **Damage to Physical Assets** | Risk of damage to physical assets caused by natural disasters, accidents or intentional / malicious actions. | 35 | **Natural Disasters** | Risk of damage to physical assets due to natural disasters. | - Damage from natural elements including rain, snow, wind, lighting, hail, wildfires, floods, earthquakes, volcanic activity, tsunamis, meteor / comets, etc. | - Public safety issues arising from environmental hazards on company property<br>- Willful damage to firm's physical assets<br>- Party motor vehicle liability<br>- Unintentional Facilities Damage-Damage due to accidents (non-willful, non-intentional damage) |
| 37 | **Damage to Physical Assets** | Losses arising from loss or damage to physical assets from natural disaster or other events. | 9 | **Damage to Physical Assets** | Risk of damage to physical assets caused by natural disasters, accidents or intentional / malicious actions. | 36 | **Willful Damage to Physical Assets** | Risk of damage to physical assets due to intentional or malicious acts. | - Terrorism, arson, individual malicious acts of Damage to physical assets, etc. | - Public safety issues arising from environmental hazards on company property<br>- Damage due to natural disasters or accidental damage |
| 38 | **Business Disruption and System Failures** | Losses arising from disruption of business or system failures | 10 | **Internal Technology & Infrastructure Failures** | Risk of disruption to business operations due to internal failures, including application, network, hardware or software failures. | 37 | **Lack of System Data Integrity** | Risk of incidents resulting from a lack of system data integrity. | - Data corruption<br>- Errors in updating data tables by technology | |
| 39 | **Business Disruption and System Failures** | Losses arising from disruption of business or system failures | 10 | **Internal Technology & Infrastructure Failures** | Risk of disruption to business operations due to internal failures, including application, network, hardware or software failures. | 38 | **Internal Technology Availability** | Risk of incidents resulting from software application and/or hardware failures, including load-bearing and capacity constraints. | - Software and hardware unavailability due to capacity shortage, coding Errors, change management issues, etc.<br>- Malicious Damage to Electronic property leading to system unavailability<br>- Technology Availability and performance Problems | - Operator error<br>- Functionality error<br>- Utility outage<br>- Offline Technology failures (macros, etc.) |
| 40 | **Business Disruption and System Failures** | Losses arising from disruption of business or system failures | 10 | **Internal Technology & Infrastructure Failures** | Risk of disruption to business operations due to internal failures, including application, network, hardware or software failures. | 39 | **Internal Technology Functionality and Processing Errors** | Risk of incidents resulting from obsolete / unsupported technology or design, programming, implementation or maintenance issues. | - Error in Functionality due to coding Errors, change management issues, defect management, etc. (example: Errors made with system logic to convert interest rates to another rate)<br>- Processing or transaction errors (inaccurate, untimely, incomplete) due to system functionality issues | - Operator error<br>- System availability issues<br>- Utility outage<br>- Offline Technology failures (macros, etc.) |
| 41 | **Business Disruption and System Failures** | Losses arising from disruption of business or system failures | 10 | **Internal Technology & Infrastructure Failures** | Risk of disruption to business operations due to internal failures, including application, network, hardware or software failures. | 40 | **Malicious Damage of Internal Technology** | Risk of disruption to business operations resulting from exposures to system vulnerabilities. | - Malicious damage to system, application or technology infrastructure<br>- Malicious damage to system code including use of malware | - Public safety issues arising from environmental hazards on company property<br>- Terrorism, arson, individual malicious acts of damage to physical assets, etc. |
| 42 | **Business Disruption and System Failures** | Losses arising from disruption of business or system failures | 11 | **External Service, Technology & Infrastructure Failures** | Risk of disruption to business operations due to external failures, including information systems, public utilities or telecommunication systems failures. | 41 | **External Service, Technology & Infrastructure Failures** | Risk of disruption to business operations due to information system, public utilities, and market exchange or telecommunication systems failures. | - Disruptions to electricity, water, gas / heating, sewer, etc.<br>- Disruptions in phone, internet, wireless, dedicated customer communication services, etc.<br>- Failures or outages of external OSP Technology, exchanges, SWIFT, market (e.g., clearing or settlement systems)<br>- Failures, delays or outages in 3rd party services<br>- Risk of outside data or service provider unable to supply systems or services when required due to technical failures<br>- Risk of service provider unable to supply Non-data, system or application related services when required | |
| | **Business Disruption and System Failures** | Losses arising from disruption of business or system failures | 12 | **Workforce Disruption** | Risk of disruption to business operations resulting from events that prevent personnel | 42 | **Workforce Disruption from Health Concerns** | Risk of pandemic or epidemic illness that prevents normal | - H1N1 Virus<br>- Zombie epidemic | - Losses or disruptions from individual absenteeism due to illness |

A risk library can be as detailed or high level as you need:

- Major Risk Category
- Major Risk Category Description
- Significant Risk Category
- Significant Risk Category Definition
- Detailed Risk
- Detailed Risk Definition
- Includes
- Excludes



LYNX TECHNOLOGY PARTNERS

| Risk Category | Core Function | Element |
|---|---|---|
| 1. Governance & Risk Management | 1. IT Risk Management | 1. Risk Monitoring |
| | | 2. Risk Response |
| | | 3. Risk Estimation & Evaluation |
| | | 4. Risk Identification |
| | | 5. Risk Universe |
| | 2. IT Compliance Management | 1. Regulatory Standards & Research |
| | | 2. Regulatory & Exam Management |
| | | 3. IT Compliance Remediation |
| | | 4. IT Compliance Monitoring |
| | 3. Organizational Security & Awareness | 1. Training & Awareness |
| | | 2. Roles & Responsibility |
| | | 3. Personnel Security |
| | | 4. Communication |
| | 4. Information Security Program Management | 1. Information Security Strategy & IT Architecture |
| | | 2. Finance Management |
| | | 3. Policy and Standards Management |
| | | 4. Standards Exception Management |
| | 5. Governance & Operating Model | 1. Governance & Operating Model |
| 2. Identity & Access Mgmt | 1. Identity and Access Management | 1. Identity Authoritative Sources |
| | | 2. ID Provisioning & De-provisioning |
| | | 3. Access Certification |
| | | 4. ID Life Cycle Management |
| | | 5. Attribute & Role Based Access Management |
| 3. Business Resiliency | 1. Business Continuity | 1. Business Impact Analysis |
| | | 2. Disaster Recovery & Availability |
| | | 3. Service Level Management |
| | | 4. Capacity Management |
| 4. Threat and Vulnerability Management | 1. Threat and Vulnerability Management | 1. Threat Assessment |
| | | 2. Vulnerability Assessment & Remediation |
| | | 3. Application Security |
| | | 4. Incident Response |
| | | 5. Forensics |
| | | 6. Event Monitoring |
| 5. Information Protection | 1. Information Protection | 1. Business Process Alignment / Ownership |
| | | 2. Information Protection Strategy |
| | | 3. Information Monitoring |
| | 2. Third Party Security | 1. Third Party Evaluation and Selection |
| | | 2. Third Party Contract & Service Initiation |
| | | 3. Third Party Contract & Service Termination |
| | | 4. Third Party Monitoring |
| 6. Application Infrastructure and Controls | 1. Application Development Management | 1. Application Portfolio Management |
| | | 2. Application Development Lifecycle |
| | | 3. Application Project Management |
| | | 4. Integration with IT Operations |
| | | 5. Application Change & Release Management |
| | 2. IT Operations | 1. IS Operations |
| | | 2. Incident & Problem Management |
| | | 3. Configuration Management |
| | | 4. Change & Release Management |
| | 3. Physical & Environmental | 1. Physical & Environmental Security Controls |
| | | 2. Equipment Security |
| | | 3. Physical Media Handling |
| | | 4. Contact With Authorities |
| | 4. Information and Asset Management | 1. Information & Asset Inventory |
| | | 2. Information & Asset Classification |
| | | 3. Information Records Management |
| | | 4. Information & Asset Monitoring |

| Req No. | Requirement | Capabilities | Elements | Risk Statement | Threats | Vulnerabilities | Control Objectives | Minimum Standard | PII/PHI Key Control | SOX Key Control | Basel Key Control | Control ID | Control Activity |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Access Control - Application and Information Access Control | Identity and Access Management | Role Based Access Management | Inadequate mechanisms and system configurations for controlling access to information resources, application software, system utilities and unattended equipment may expose information to unauthorized access and/or potential security threats from malicious code or by users overriding system and application controls. | Internal resource | Lack of controls/procedures for Access Control | [CobiT v5 - Management Process DSS06] Controls have been defined to ensure that information related to and processed by in-house or outsourced business processes satisfies all relevant information control requirements. | X | x | | | 1-a(i) | a.i. Logical access to application software and information is restricted to authorized users. Application systems are configured to:<br>i. Control user access to information and application system functions, in accordance with a defined access control policy<br>ii. Not compromise other systems with which information resources are shared. |
| 1 | Access Control - Application and Information Access Control | Identity and Access Management | Role Based Access Management | Inadequate mechanisms and system configurations for controlling access to information resources, application software, system utilities and unattended equipment may expose information to unauthorized access and/or potential security threats from malicious code or by users overriding system and application controls. | Internal resource | Lack of controls/procedures for Access Control | [CobiT v5 - Management Process DSS06] Controls have been defined to ensure that information related to and processed by in-house or outsourced business processes satisfies all relevant information control requirements. | | x | | | 1-a(ii) | a(ii).i. Application systems are configured to provide protection from unauthorized access by any utility, operating system software, and malicious software that is capable of overriding or bypassing system or application controls |
| 1 | Access Control - Application and Information Access Control | Identity and Access Management | Role Based Access Management | Inadequate mechanisms and system configurations for controlling access to information resources, application software, system utilities and unattended equipment may expose information to unauthorized access and/or potential security threats from malicious code or by users overriding system and application controls. | Internal resource | Lack of controls/procedures for Access Control | [CobiT v5 - Management Process DSS06] Controls have been defined to ensure that information related to and processed by in-house or outsourced business processes satisfies all relevant information control requirements. | | | | x | 1-b | b.i. System utility programs that could override system and application controls are restricted and tightly controlled. |
| 2 | Access Control - Application and Information Access Control - Sensitive system isolation | IT Operations | IS Operations | Insufficient segregation of highly sensitive systems from other systems may expose sensitive information resources to unauthorized access. | Hacker | Lack of controls/procedures for Access Control | [CobiT v5 - Management Process DSS05] Controls have been defined to establish and maintain information security roles and access privileges and to perform security monitoring. | | | | | 2-a | a.i. Groups of information services, users and information systems are segregated on networks. Sensitive systems have a dedicated (isolated) computing environment. |
| 2 | Access Control - Application and Information Access Control - Sensitive system isolation | IT Operations | IS Operations | Insufficient segregation of highly sensitive systems from other systems may expose sensitive information resources to unauthorized access. | Hacker | Lack of controls/procedures for Access Control | [CobiT v5 - Management Process DSS05] Controls have been defined to establish and maintain information security roles and access privileges and to perform security monitoring. | | x | | | 2-b(i) | b(i).i. For systems subject to PCI requirements, card data is not stored in any internet facing systems. |
| 2 | Access Control - Application and Information Access Control - Sensitive system isolation | IT Operations | IS Operations | Insufficient segregation of highly sensitive systems from other systems may expose sensitive information resources to unauthorized access. | Hacker | Lack of controls/procedures for Access Control | [CobiT v5 - Management Process DSS05] Controls have been defined to establish and maintain information security roles and access privileges and to perform security monitoring. | | x | | | 2-b(ii) | b(ii).i. Confidential data is not stored in any internet facing systems. |

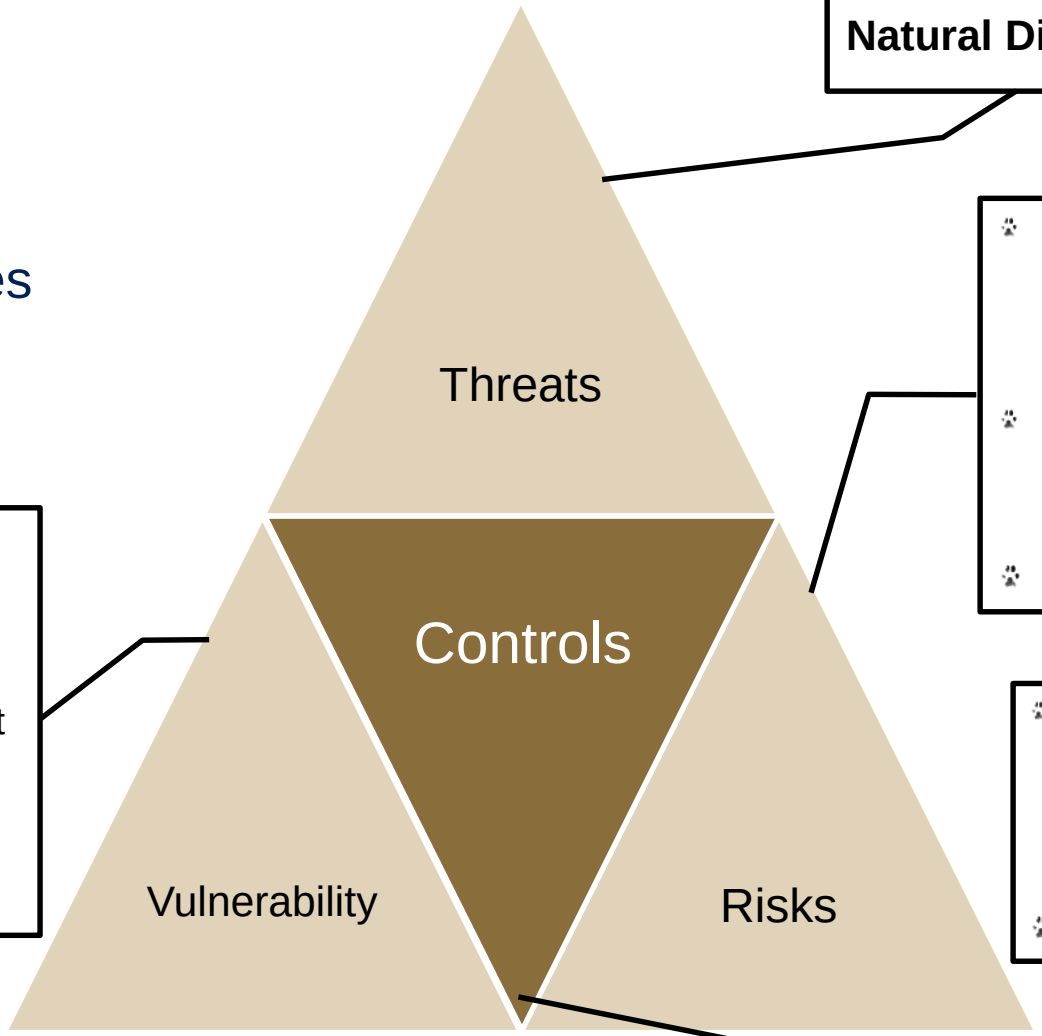
# Scenario

**Profile:**

- 40 Requirements
- 5 unique Elements
- 10 unique Vulnerabilities
- 73 Control Activities

**Natural Disaster**

- Failure to embed the BCM Program within the core values and culture of the organization may result in an unsuccessful program that cannot meet business requirements during a disaster.
- Failure to properly document and include sufficient information in the incident management plan may result in the failure of the plan during execution
- etc…




- Lack of controls related to Policies & Guidance
- Lack of controls / procedures for Service Continuity & Availability Management
- Lack of controls / procedures for Incident Management
- Lack of controls / procedures for Governance bodies
- etc…

- DR plans and procedures are developed, documented, and implemented to maintain or restore operations and provide availability of information at the required level and in the required time scales following interruption to, or failure of critical business processes.
- etc…

LYNX TECHNOLOGY PARTNERS

| Function | Category | Control Expectations | Metric | Rating |
|---|---|---|---|---|
| 1. Technology Operations | 1. Technology Operations | a. Backups are effectively executed and logged | % Failed Backup Jobs | |
| | | b. Hardware assets are effectively monitored for availability | % Prod systems monitored | |
| | | c. Operating System & Middleware effectively monitored | % Prod systems monitored | |
| | | d. Operating Systems effectively maintained (patched) | % critical patches not applied | |
| 2. Incident & Problem Management | 2. Incident & Problem Management | a. Technology incidents are recorded, categorized and prioritized. | % of open technology incidents assigned correct severity and priority | |
| | | b. Root Cause are completed for all Severity 1 Technology incidents | % of Severity 1 Technology incidents documented in Root Cause | |
| | | | % of Root Causes Tickets with root cause identified and completed action plans implemented | |
| | | c. Escalation guidelines defined and adhered to for Severity 1 Technology incidents | % of escalation occurrences adherring to guidelines | |
| 3. Configuration Management | 3. Configuration Management | a. Configuration standards are defined | % of standards defined | |
| | | b. Process defined for identifying configurable items | % of complete CIs needed to support Change/Incident Management | |
| | | c. Configuration item logical model for services defined | % of logical model defined | |
| 4. Change & Release Management | 4. Change & Release Management | a. Change requests classification are defined and documented | % of approved changes by change category: standard, normal, emergency | |
| | | b. Change control governance designed and implemented | % of change governance designed and implemented | |
| | | c. Only approved Problem Tickets / Change Requests are promoted to Production | % of code managed by an enterprise change control system. | |
| | | | % of infrastructure changes included in Configuration Management | |
| | | | % of infrastructure implemented successfully | |
| | | d. Approved Change Requests are implemented and tested | % of successful changes | |
| 5. Capacity Management | 5. Capacity Management | a. Current Services monitored | % of IT Services monitored for performance and throughput | |
| | | b. Performance Incidents | % of capacity and performance incidents by IT Services | |
| | | a. Capacity planning policies, procedures and standards are defined and approved by management | % of capacity planning policies, procedures, and standards defined and implemented | |

# Residual Risk

Continuous Monitoring and Incident Response

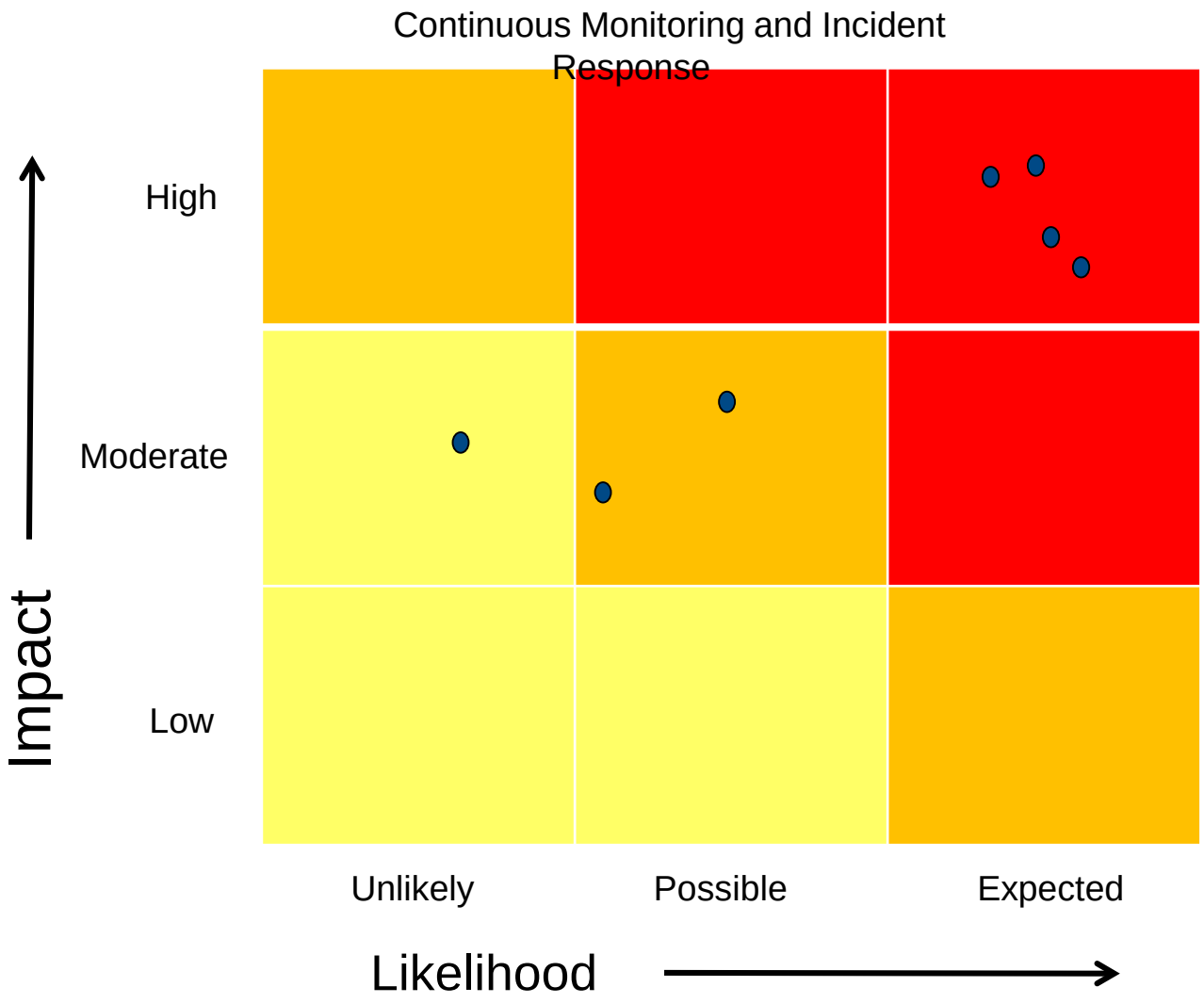
**Threats:** Internal Resource, Former Internal Resource, External Party, Hacker, Cyber-Criminals, Malicious Code

| High | | Satisfactory | | High |
|---|---|---|---|---|
| **Inherent Risk** | + | **Control Effectiveness** | = | **Residual Risk** |
| • Theft and Fraud by Internal or External Party<br>• Internal IT Failures (i.e. malicious damage)<br>• Business Disruption | | • Immature Processes and Controls<br>• Lack of Detection Capabilities<br>• Limited Ability to Conduct Real Time Monitoring<br>• Staffing Levels Not Adequate | | • Limited ability to conduct real-time monitoring<br>• Lack of visibility makes it difficult to defend during cyber events. |



LYNX TECHNOLOGY PARTNERS

# Residual Risk Matrix (9-box)



# Closing Thoughts

- Qualitative vs Quantitative IT Risk
- Keep it simple (risk = likelihood x impact)
- Threats will always out pace our efforts
- Business impact as differentiator for selecting controls
- Detective controls reduce impact

- What does this have to do with the CSF?

*Business risk management strives to adjust behavior to reduce the impact of threats to business strategies and objectives. In IT Security, risk management is the fundamental goal. Security functions need a risk-based, agile, contextual approach that is core to risk management.*



LYNX TECHNOLOGY PARTNERS

# Closing Thoughts

- Qualitative vs Quantitative IT Risk
- Keep it simple (risk = likelihood x impact)
- Threats will always out pace our efforts
- Business impact as differentiator for selecting controls
- Detective controls reduce impact

- What does this have to do with the CSF?

*Business risk management strives to adjust behavior to reduce the impact of threats to business strategies and objectives. In IT Security, risk management is the fundamental goal. Security functions need a risk-based, agile, contextual approach that is core to risk management.*



LYNX TECHNOLOGY PARTNERS

# Closing Thoughts

- Qualitative vs Quantitative IT Risk
- Keep it simple (risk = likelihood x impact)
- Threats will always out pace our efforts
- Business impact as differentiator for selecting controls
- Detective controls reduce impact

- What does this have to do with the CSF?

*Business risk management strives to adjust behavior to reduce the impact of threats to business strategies and objectives. In IT Security, risk management is the fundamental goal. Security functions need a risk-based, agile, contextual approach that is core to risk management.*



LYNX TECHNOLOGY PARTNERS

# Supplemental

- Critical Infrastructure (CI)
- Information & Decision Flows within an Organization
- Criticisms & Shortcomings
- Resources



LYNX TECHNOLOGY PARTNERS

# Critical Infrastructure

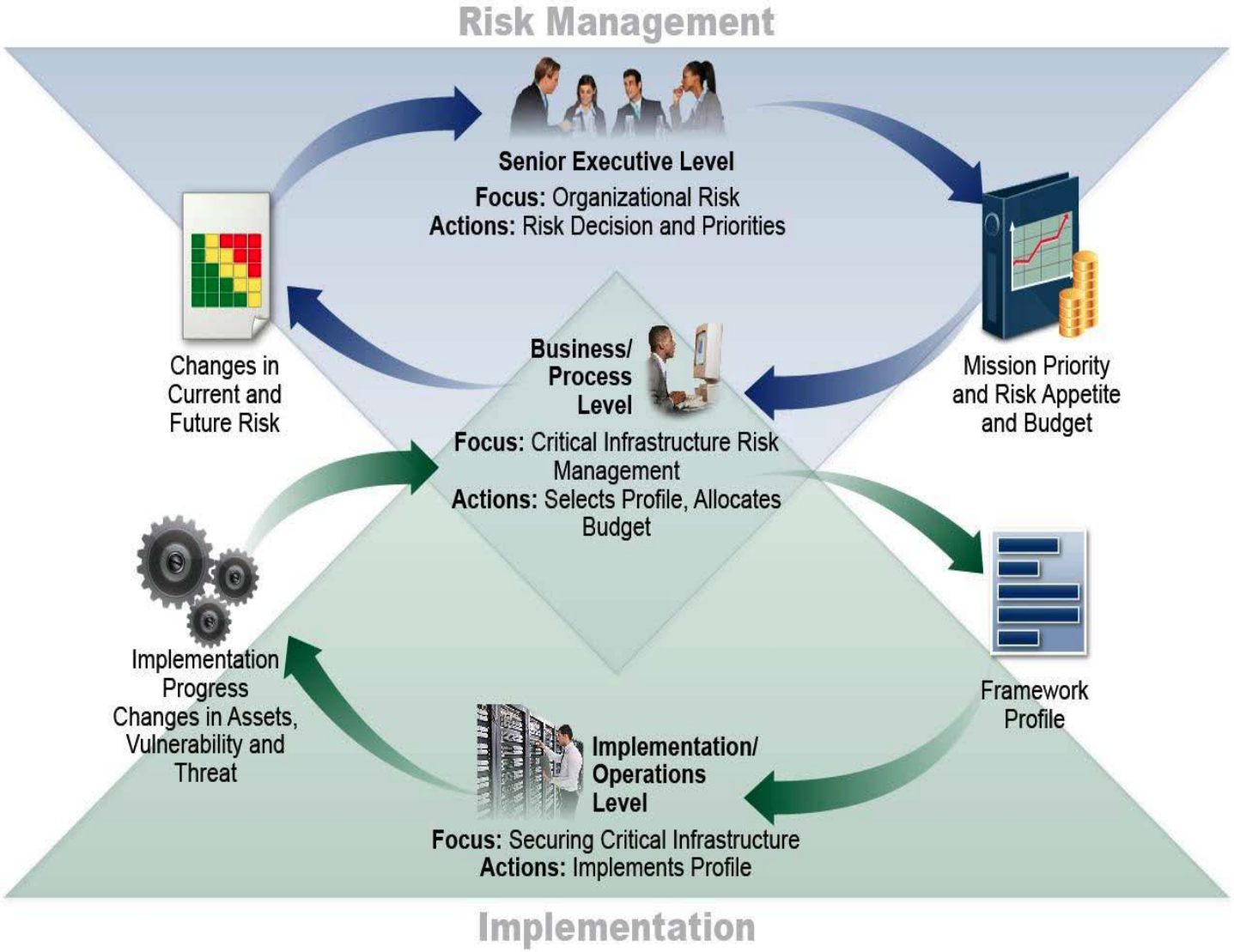
- Critical Infrastructure (CI) and designated Sector-Specific Authority (SSA):
  - Chemical (DHS)
  - Commercial Facilities (DHS)
  - Communications (DHS)
  - Critical Manufacturing (DHS)
  - Dams (DHS)
  - Defense Industrial Base (DoD)
  - Emergency Services (DHS)
  - Energy (Department of Energy)
  - Financial Services (Treasury)
  - Food and Agriculture (USDA & HHS)
  - Government Facilities (DHS & GSA)
  - Healthcare & Public Health (HHS)
  - Information Technology (DHS)
  - Nuclear Reactors, Materials & Waste (DHS)
  - Transportation Systems (DHS & DOT)
  - Water & Wastewater Systems (EPA)

http://www.dhs.gov/critical-infrastructure



LYNX TECHNOLOGY PARTNERS

# Information & Decision Flows within an Organization




The **Senior Executive Level** communicates the mission priorities, available resources, and overall risk tolerance to the business/process level

The **Business/Process Level** uses the Implementation/Ops Level information to perform an impact assessment, and then collaborates with the Implementation/Ops Level to create a Profile.

The **Implementation/Operation Level** uses the outcomes of the impact assessment to report to the Senior Executive Level to inform the organization's overall risk management process.

# Overview of CSF: Tiers

## Tier 1: Partial

- Risk Management Process – Organizational cybersecurity risk management practices are not formalized and risk is managed in an ad hoc and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- Integrated Program – There is a limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources.
- External Participation – An organization may not have the processes in place to participate in coordination or collaboration with other entities.



LYNX TECHNOLOGY PARTNERS

# Overview of CSF: Tiers (continued)

## Tier 2: Risk-Informed

- Risk Management Process – Risk management practices are approved by management but may not be established as organizational-wide policy.
- Integrated Program – There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established. Risk-informed, management-approved processes and procedures are defined and implemented and staff has adequate resources to perform their cybersecurity duties.
- External Participation – The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.



LYNX TECHNOLOGY PARTNERS

# Overview of CSF: Tiers (continued)

## Tier 3: Risk-Informed and Repeatable

- Risk Management Process – The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to a changing threat and technology landscape.
- Integrated Program – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and validated. Consistent methods are in place to effectively respond to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.
- External Participation – The organization understands its dependencies and partners and receives information from these partners enabling collaboration and risk-based management decisions within the organization in response to events.



LYNX TECHNOLOGY PARTNERS

# Overview of CSF: Tiers (continued)

## Tier 4: Adaptive

- Risk Management Process – The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous cybersecurity activities. Through a process of continuous improvement, the organization actively adapts to a changing cybersecurity landscape and responds to emerging/evolving threats in a timely manner.
- Integrated Program – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.
- External Participation – The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before an event occurs.



LYNX TECHNOLOGY PARTNERS

# Criticisms & Shortcomings

**Voluntary**

- The CSF will likely be viewed as the minimum level of care and integrity within critical infrastructure sectors: "…critical infrastructure operators have a responsibility to adopt the recommended IT best practices."

- If you ignore the CSF and are breached, you open yourself up to negligence, shareholder and breach of contract lawsuits, regulatory fines, and other liability claims
- EO leaves federal agencies in charge of each sector to push adoption through incentives and "other market driven means"
- At a minimum you will need to show what you are doing is as effective: Self assessment and gap analysis



LYNX TECHNOLOGY PARTNERS

# Criticisms & Shortcomings (continued)

## Increased Liability Risks

- Companies that want to share threat-information with other firms will have to first scrub the data so it's clean of PII.
- IP addresses, E-mail, URLs, account enumeration lists are all PII in some states

## Fear & Uncertainty

- CSF may become yet another compliance regiment
- Incentives tied to insurance rates and other economic factors may be result in less of a risk management approach and more of a cost management strategy
- Framework allows cherry picking controls and may provide false sense of security if you miss controls that are too costly
- Costs of implementation will be passed on to consumers
- The CSF will likely be viewed as the minimum level of care and integrity within critical infrastructure sectors: "…critical infrastructure operators have a responsibility to adopt the recommended IT best practices."



LYNX TECHNOLOGY PARTNERS

# Resources

ISACA - Operationalize CSF with COBIT:

http://www.isaca.org/Education/COBIT-Education/Pages/Implementing-NIST-Cybersecurity-Framework-Using-COBIT-5.aspx

Phil Agcaoili's CSF Job Aid with CSA MappingsL

https://app.box.com/s/2qd8fs7d9xxdgmg7euhc

NIST CyberSecurity Framework

http://www.nist.gov/cyberframework/index.cfm

NIST "C3" Voluntary Program

https://www.dhs.gov/ccubedvp



LYNX TECHNOLOGY PARTNERS

LYNX
TECHNOLOGY PARTNERS

IT Risk & Cyber Security Experts

FIERCELY PROTECTING OUR CLIENTS

+1.800.314.0455
sales@lynxtp.com

GLOBAL HEADQUARTERS
100 Church Street
8th Floor
New York, NY 10007

PITTSBURGH, PA
309 Smithfield Street
3rd Floor
Pittsburgh, PA 15222

WASHINGTON, DC
20 F. Street Northwest
7th Floor
Washington, DC 20001

lynxgrc.com

# Thank you!