

RSA[®]Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: CXO-T08

How to Make Sense of Cybersecurity Frameworks

Frank Kim

Founder / Instructor
ThinkSec / SANS Institute
@fykim
www.frankkim.net



#RSAC



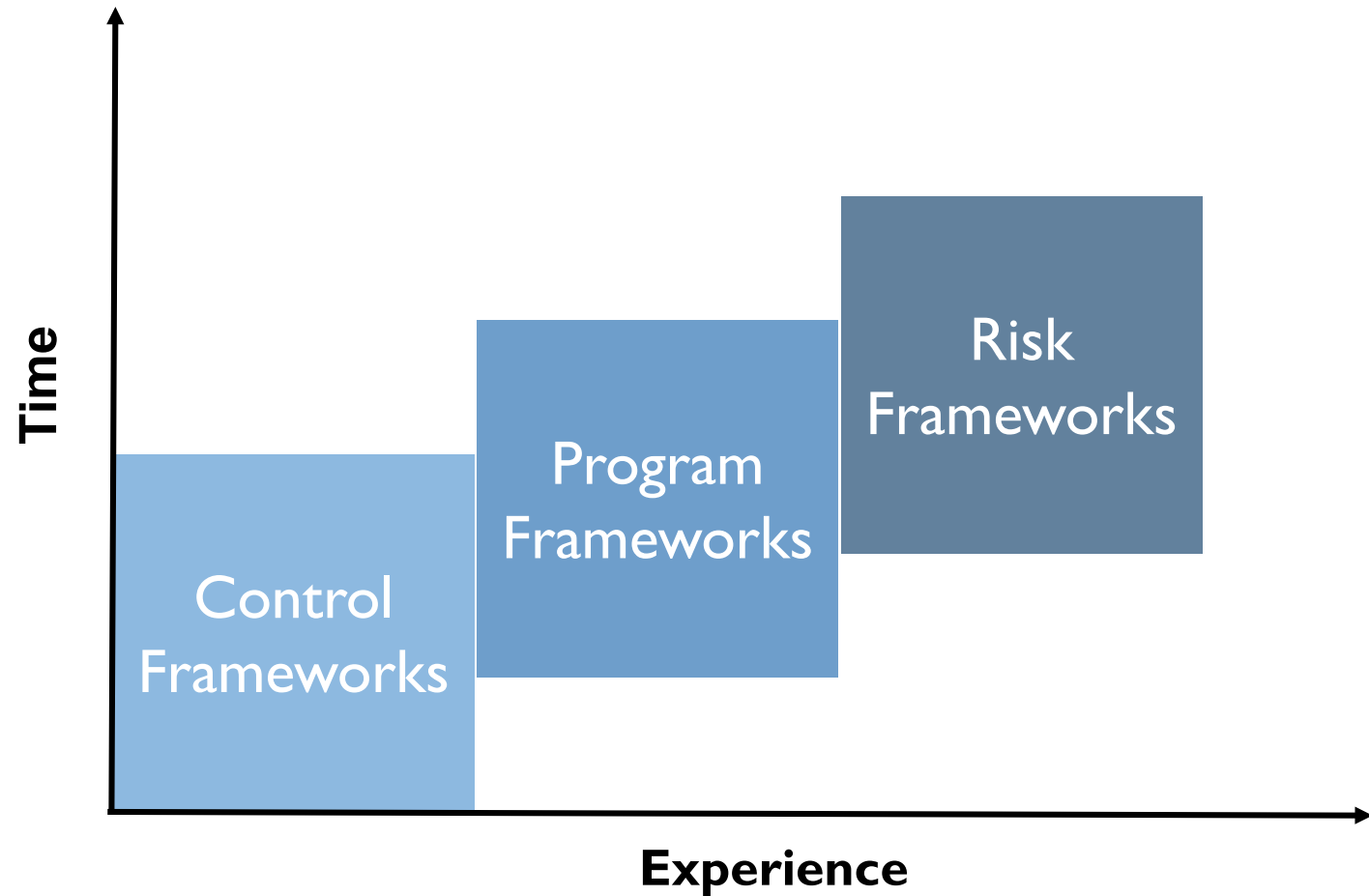






Three Types of Security Frameworks

- Control Frameworks
 - NIST 800-53
 - CIS Controls (CSC)
- Program Frameworks
 - ISO 27001
 - NIST CSF
- Risk Frameworks
 - NIST 800-39, 800-37, 800-30
 - ISO 27005
 - FAIR



RSAConference2019

Control Frameworks



Using a Control Framework

- Use a Control Framework to:
 - Identify baseline set of controls
 - Assess state of technical capabilities
 - Prioritize implementation of controls
 - Develop an initial roadmap for the security team

NIST SP 800-53

Access Control (AC)	Configuration Management (CM)	Media Protection (MP)	Risk Assessment (RA)
Awareness and Training (AT)	Contingency Planning (CP)	Physical & Env. Protection (PE)	System and Services Acquisition (SA)
Audit and Accountability (AU)	Identification and Authentication (IA)	Planning (PL)	System & Comms Protection (SC)
Security Assessment & Authz (CA)	Incident Response (IR)	Personnel Security (PS)	System & Info Integrity (SI)
	Maintenance (MA)	Program Management (PM)	

NIST SP 800-53 Overview

- Comprehensive control catalog of security and privacy controls
 - Family
 - Control
 - Control Enhancement
- Controls can be implemented based on:
 - Priority
 - P1, P2, P3, P0
 - Security Control Baselines
 - Low-Impact, Moderate-Impact, High-Impact

NIST SP 800-53 Control Example

Cntl No.	Control Name	Priority	Initial Control Baselines		
			Low	Mod	High
AC-1	Access Control Policy & Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-5	Separation of Duties	P1	Not selected	AC-5	AC-5
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-9	Previous Logon (Access) Notification	P0	Not selected	Not selected	Not selected
AC-11	Session Lock	P3	Not selected	AC-11 (1)	AC-11 (1)

Family

Control Enhancement

CIS Controls

Basic

- 1 Inventory and Control of Hardware
- 2 Inventory and Control of Software
- 3 Continuous Vuln Management
- 4 Controlled Use of Admin Privileges
- 5 Secure Config for Hardware & Software
- 6 Maint., Monitoring & Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protect
- 8 Malware Defenses
- 9 Limit & Control of Port, Protocol, Services
- 10 Data Recovery Capabilities
- 11 Secure Config for Network Devices
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access on Need to Know
- 15 Wireless Access Control
- 16 Account Monitor and Control

Organizational

- 17 Security Awareness & Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests & Red Team Exercises

CIS Controls Success Stories

- Large enterprises
 - United States Department of State
 - 90% Risk Reduction in Year 1
 - Australian Defense Services Directorate
 - Stopped 85% of intrusions
 - United States Federal Reserve System
 - Basis for Internal Audit to assess Cyber Security
- Smaller organizations
 - “A Small Business No Budget Implementation”

Management Takeaways

- Free resources
 - AuditScripts Control Master Mapping
 - Maps Controls to nearly every known regulatory compliance standard
 - AuditScripts Control Manual Assessment Tool
 - Self-assessment of current state of Controls implementation
 - CIS Controls Implementation Guide
 - Key questions to ask when implementing the Controls

RSA®Conference2019

Program Frameworks



Using a Program Framework

- Use a Program Framework to:
 - Assess state of the overall security program
 - Build a comprehensive security program
 - Measure maturity and conduct industry comparisons
 - Simplify communications with business leaders

ISO 27000 Series Overview

Requirements

27001

ISMS Requirements

27006Requirements for
certification bodies**27009**Sector specific
requirements

Guidelines

27002Implementation guidance
for controls**27003**Implementation guidance
for management**27004**Monitoring, measurement,
analysis, evaluation**27005**

Risk management

27007

Guidance for audits

27008

Guidance for auditors

27014

Governance

27021Competence reqs for
security professionals

Sector-specific

27011

Telecom

27017

Cloud services

27018

PII in public clouds

27019

Energy and Utility

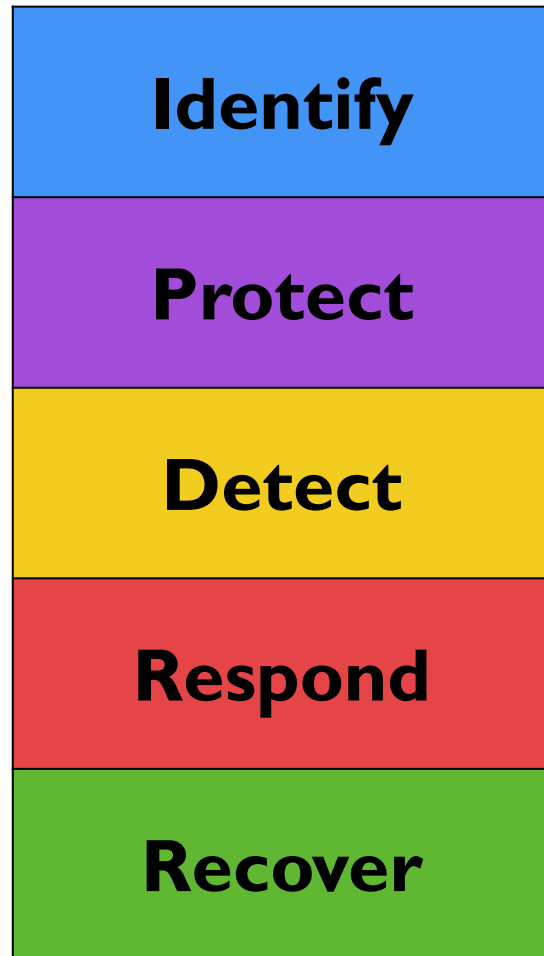
ISO 27001

- ISO 27001
 - Information Security Management System (ISMS) requirements
- Defines areas of focus in building a security program
 - Organizational context
 - Leadership
 - Planning
 - Support
 - Documentation
 - Operation
 - Performance evaluation
 - Improvement

ISO 27001 Control Objectives

Information security policies	Access control	Communications security	Information security incident management
Organization of information security	Cryptography	System acquisition, development, and maintenance	Security aspects of business continuity management
Human resource security	Physical and environmental security	Test data	Compliance
Asset management	Operations security	Supplier relationships	

NIST Cybersecurity Framework (CSF)



- Composed of three parts
 - Core, Implementation Tiers, and Profiles
- Defines a common language for managing risk
 - Core has five functions that provide a high-level, strategic view of the security life cycle
- Helps organizations ask:
 - What are we doing today?
 - How are we doing?
 - Where do we want to go?
 - When do we want to get there?

Framework Categories

Function	Category
Identify	Asset Management Business Environment Governance Risk Assessment Risk Management Strategy Supply Chain Risk Management
Protect	Identity Management, Authn & Access Control Awareness & Training Data Security Information Protection Processes & Procedures Maintenance Protective Technology
Detect	Anomalies & Events Security Continuous Monitoring Detection Processes
Respond	Response Planning Communications Analysis Mitigation Improvements
Recover	Recovery Planning Improvements Communications

- Composed of three parts
 - Core, Implementation Tiers, and Profiles
- Defines a common language for managing security risk
 - Core has five functions that provide a high-level, strategic view of the security life cycle
- Helps organizations ask:
 - What are we doing today?
 - How are we doing?
 - Where do we want to go?
 - When do we want to get there?

Framework Subcategory Examples

Function	Category	Subcategory	Informative References
Protect	ID Mgt, Authn, Access (PR.AC)	PR.AC-1: Identities and credentials are managed PR.AC-2: Physical access to assets is managed PR.AC-3: Remote access is managed PR.AC-4: Access permissions are managed PR.AC-5: Network integrity is protected	CSC 1, 5, 15, 16; NIST 800-53 AC-1, AC-2; NIST 800-53 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8 CSC 12; NIST 800-53 AC-1, AC-17, AC-19, AC-20, SC-15 CSC 3, 5, 12, 14, 15, 16, 18; NIST 800-53 AC-1, AC-2, AC-3, AC-5, AC-16, AC-14 CSC 9, 14, 15, 18; NIST 800-53 AC-4, AC-10, SC-7
	Awareness & Training (PR.AT)	PR.AT-1: All users are informed and trained PR.AT-2: Privileged users understand roles & responsibilities PR.AT-3: Third-party stakeholders understand roles and responsibilities PR.AT-4: Senior executives understand roles and responsibilities PR.AT-5: Physical & security personnel understand roles and responsibilities	CSC 17, 18; NIST 800-53 AT-2, PM-13 CSC 5, 17, 18; NIST 800-53 AT-3, PM-13 CSC 17; NIST 800-53 PS-7, SA-9, SA-16 CSC 17, 19; NIST 800-53 AT-3, PM-13 CSC 17; NIST 800-53 AT-3, IR-2, PM-13
	Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected PR.DS-2: Data-in-transit is protected PR.DS-3: Assets are formally managed PR.DS-4: Adequate capacity to ensure availability PR.DS-5: Protections against data leaks are implemented PR.DS-6: Integrity checking mechanisms are used	CSC 13, 14; NIST 800-53 MP-8, SC-12, SC-28 CSC 13, 14; NIST 800-53 SC-8, SC-11, SC-12 CSC 1; NIST 800-53 CM-8, MP-6, PE-16 CSC 1, 2, 13; NIST 800-53 AU-4, CP-2, SC-5 CSC 13; NIST 800-53 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13 CSC 2, 3; NIST 800-53 SC-16, SI-7
	Info Protection Processes & Procedures (PR.IP)	PR.IP-1: Baseline configuration created and maintained PR.IP-2: System Development Life Cycle implemented PR.IP-3: Configuration change control processes PR.IP-4: Backups conducted, maintained, and tested PR.IP-5: Policy and regulations of physical environment PR.IP-6: Data is destroyed according to policy PR.IP-7: Protection processes are continuously improved PR.IP-8: Effectiveness of protection technologies is shared PR.IP-9: Response & recovery plans in place PR.IP-10: Response and recovery plans are tested PR.IP-11: Cybersecurity is included in HR PR.IP-12: Vulnerability management plan	CSC 3, 9, 11; NIST 800-53 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 CSC 18; NIST 800-53 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17 CSC 3, 11; NIST 800-53 CM-3, CM-4, SA-10 CSC 10; NIST 800-53 CP-4, CP-6, CP-9 NIST 800-53 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 NIST 800-53 MP-6 NIST 800-53 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 NIST 800-53 AC-21, CA-7, SI-4 CSC 19; NIST 800-53 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17 CSC 19, 20; NIST 800-53 CP-4, IR-3, PM-14 CSC 5, 16; NIST 800-53 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21 CSC 4, 18, 20; NIST 800-53 RA-3, RA-5, SI-2
	Protective Technology (PR.MA)	PR.PT-1: Audit/log records reviewed per policy PR.PT-2: Removable media is protected PR.PT-3: Least functionality is implemented PR.PT-4: Communications & control networks protected	CSC 1, 3, 5, 6, 14, 15, 16; NIST 800-53 AU Family CSC 8, 13; NIST 800-53 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8 CSC 3, 11, 14; NIST 800-53 AC-3, CM-7 CSC 8, 12, 15; NIST 800-53 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21

NIST CSF to CIS Control Mapping

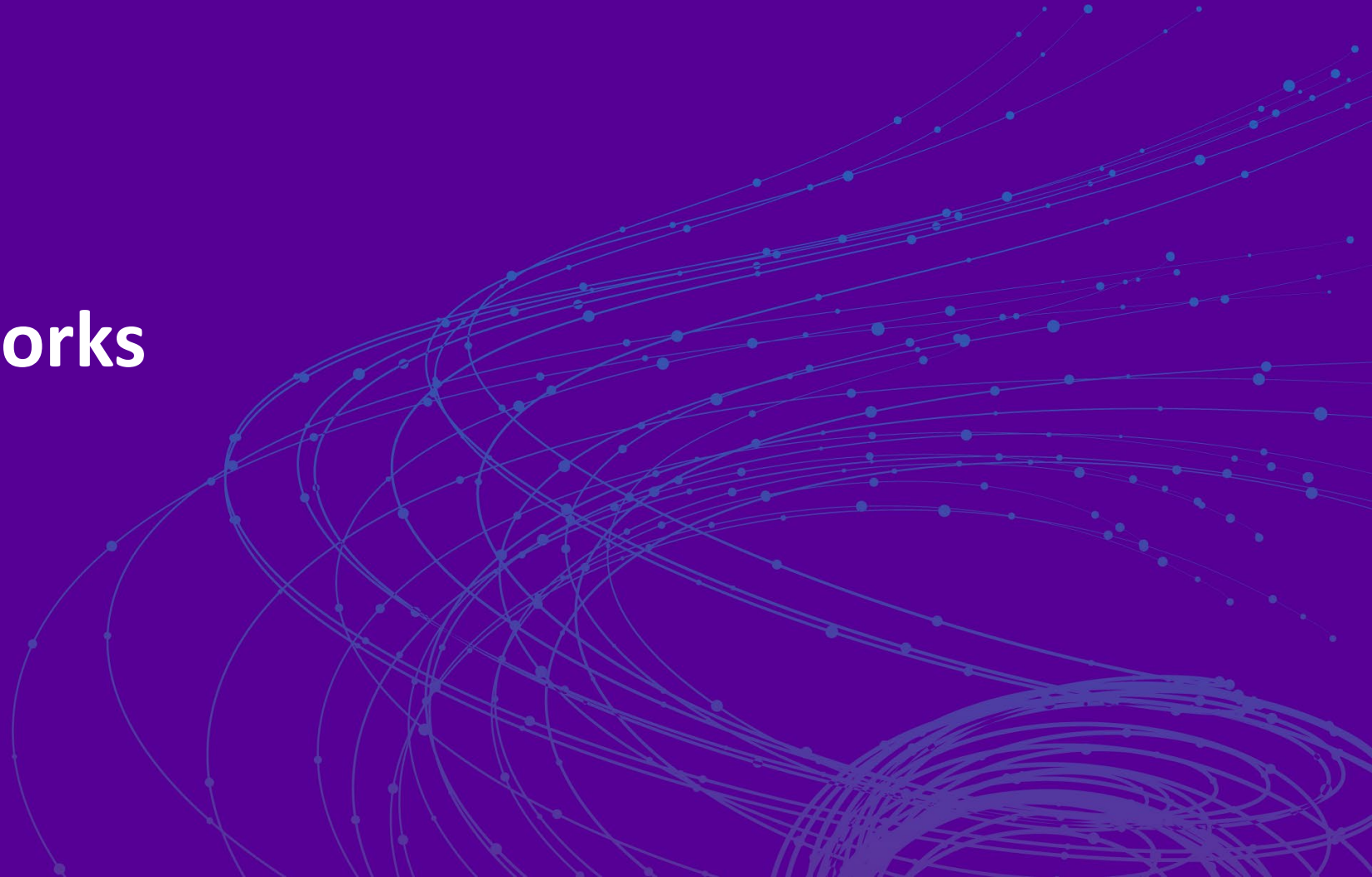
Function	Category	CIS Control
Identify	Asset Management Business Environment Governance Risk Assessment Risk Management Strategy Supply Chain Risk Management	CIS Control #1, 2 CIS Control #3
Protect	Identity Management, Authentication and Access Control Awareness & Training Data Security Information Protection Processes and Procedures Maintenance Protective Technology	CIS Control #4, 9, 11, 12, 13, 14, 16 CIS Control #4, 17 CIS Control #1, 2, 13, 14, 18 CIS Control #3, 5, 7, 10, 11 CIS Control #4, 12 CIS Control #4, 6, 8, 11, 13, 14, 16
Detect	Anomalies & Events Security Continuous Monitoring Detection Processes	CIS Control #6, 9, 12, 19 CIS Control #3, 8, 19 CIS Control #6
Respond	Response Planning Communications Analysis Mitigation Improvements	CIS Control #19 CIS Control #19 CIS Control #3, 19 CIS Control #3, 19 CIS Control #19
Recover	Recovery Planning Improvements Communications	CIS Control #19 CIS Control #19 CIS Control #19

Mapping Between Frameworks

- Control and Program Frameworks
 - Can be used together
 - Are not mutually exclusive
 - Support each other
- Mapping connects them together
 - NIST CSF Mapping
 - Maps CSF to CSC, NIST 800-53, ISO 27001, COBIT, ISA
 - AuditScripts Master Mapping
 - Maps CSC to over 30 frameworks and compliance regimes

RSA®Conference2019

Risk Frameworks

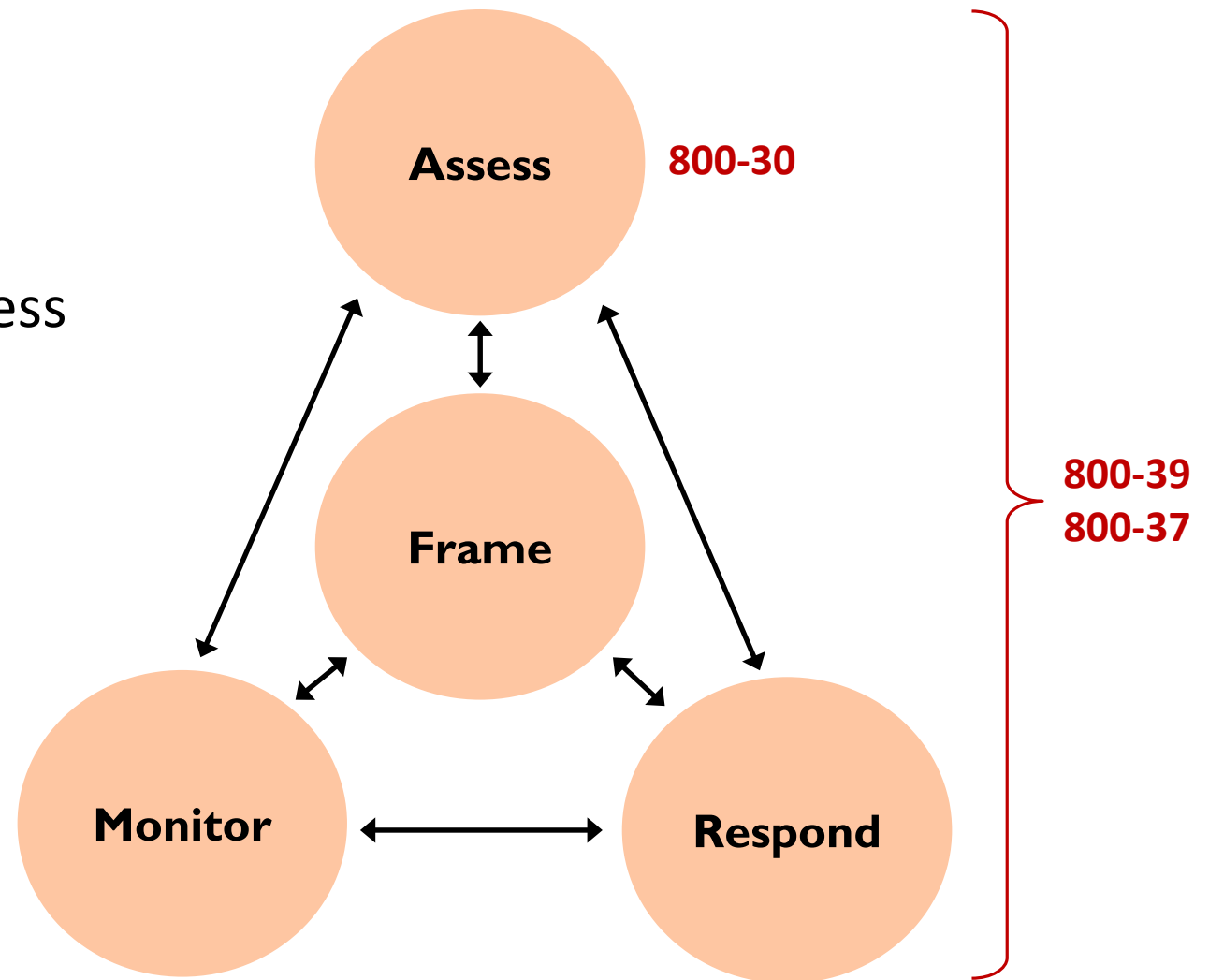


Using a Risk Framework

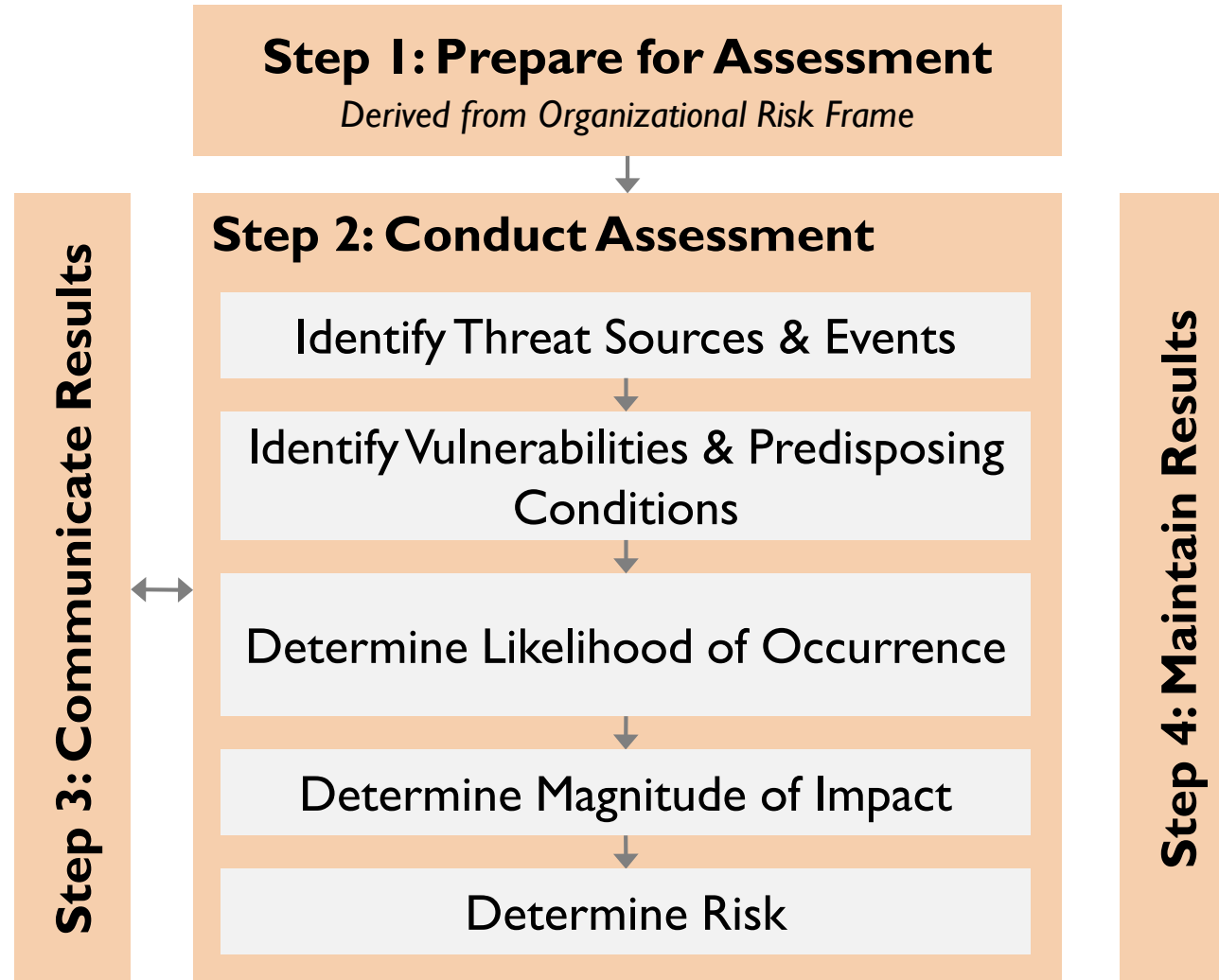
- Use a Risk Framework to:
 - Define key process steps for assessing and managing risk
 - Structure risk management program
 - Identify, measure, and quantify risk
 - Prioritize security activities

NIST Security Risk Standards

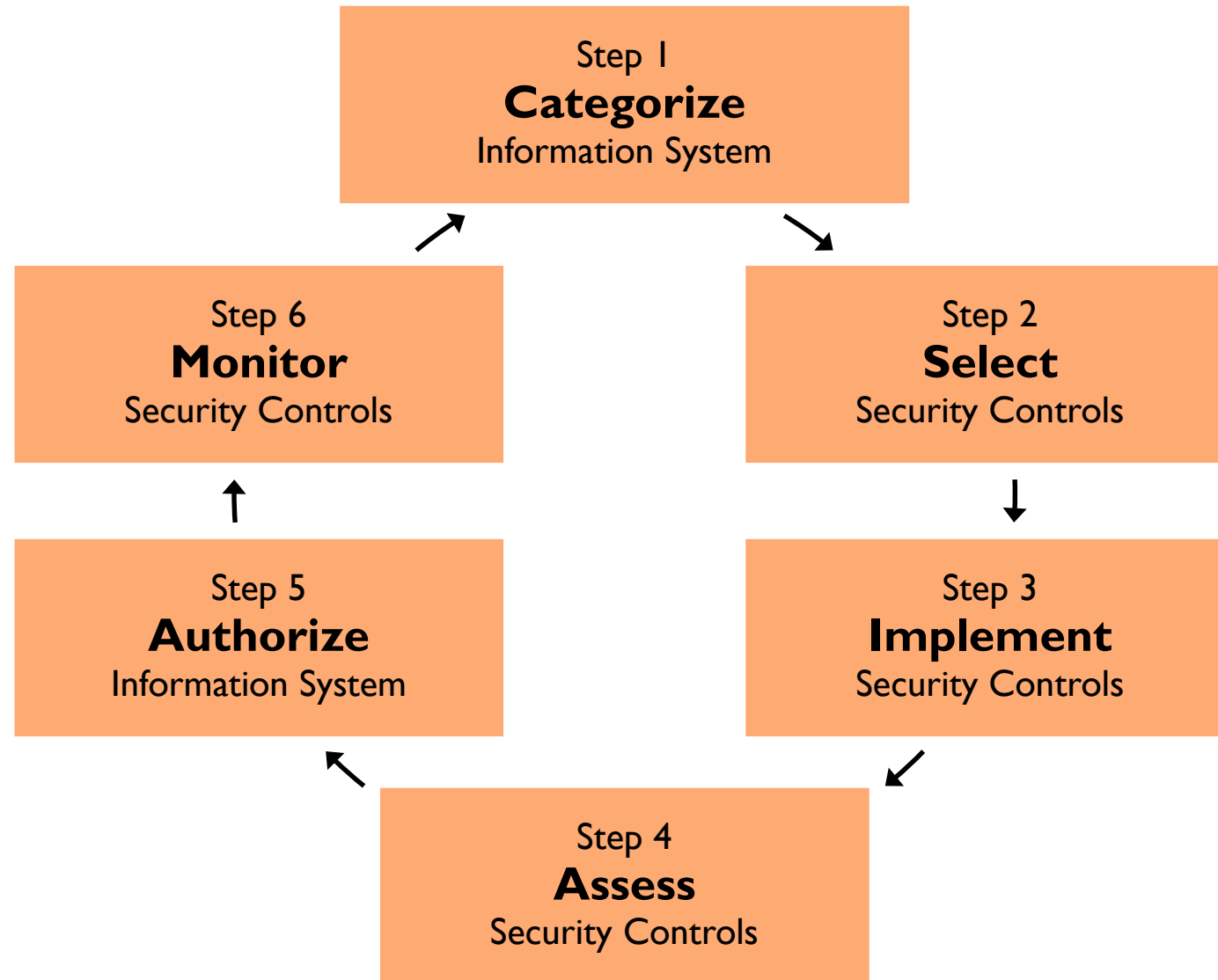
- Risk management
 - NIST SP 800-39
 - Overall risk management process
 - NIST SP 800-37
 - Risk management framework (RMF) for federal information systems
- Risk assessment
 - NIST SP 800-30
 - Risk assessment process



NIST Risk Assessment Process

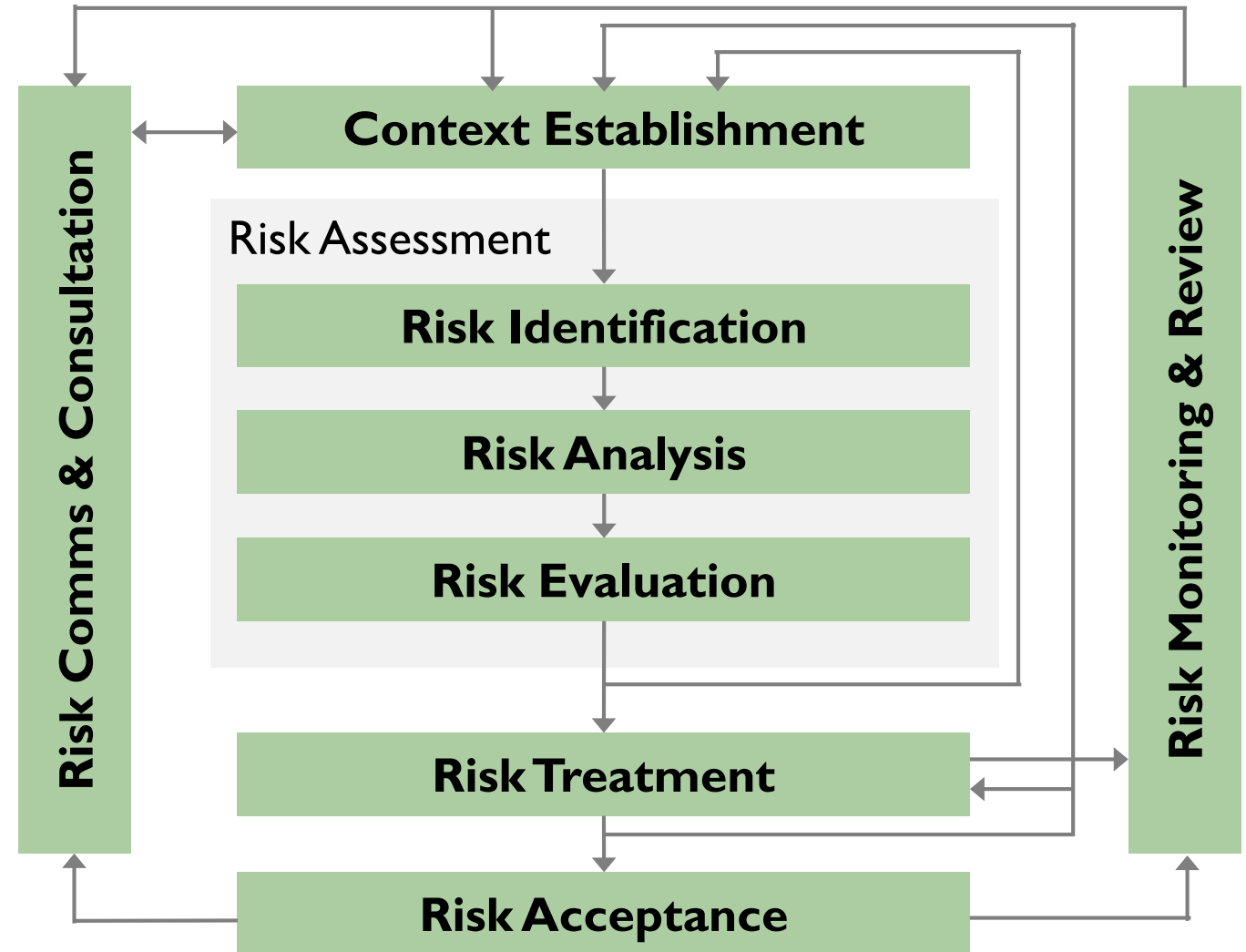


NIST Risk Management Framework (RMF)



ISO 27005

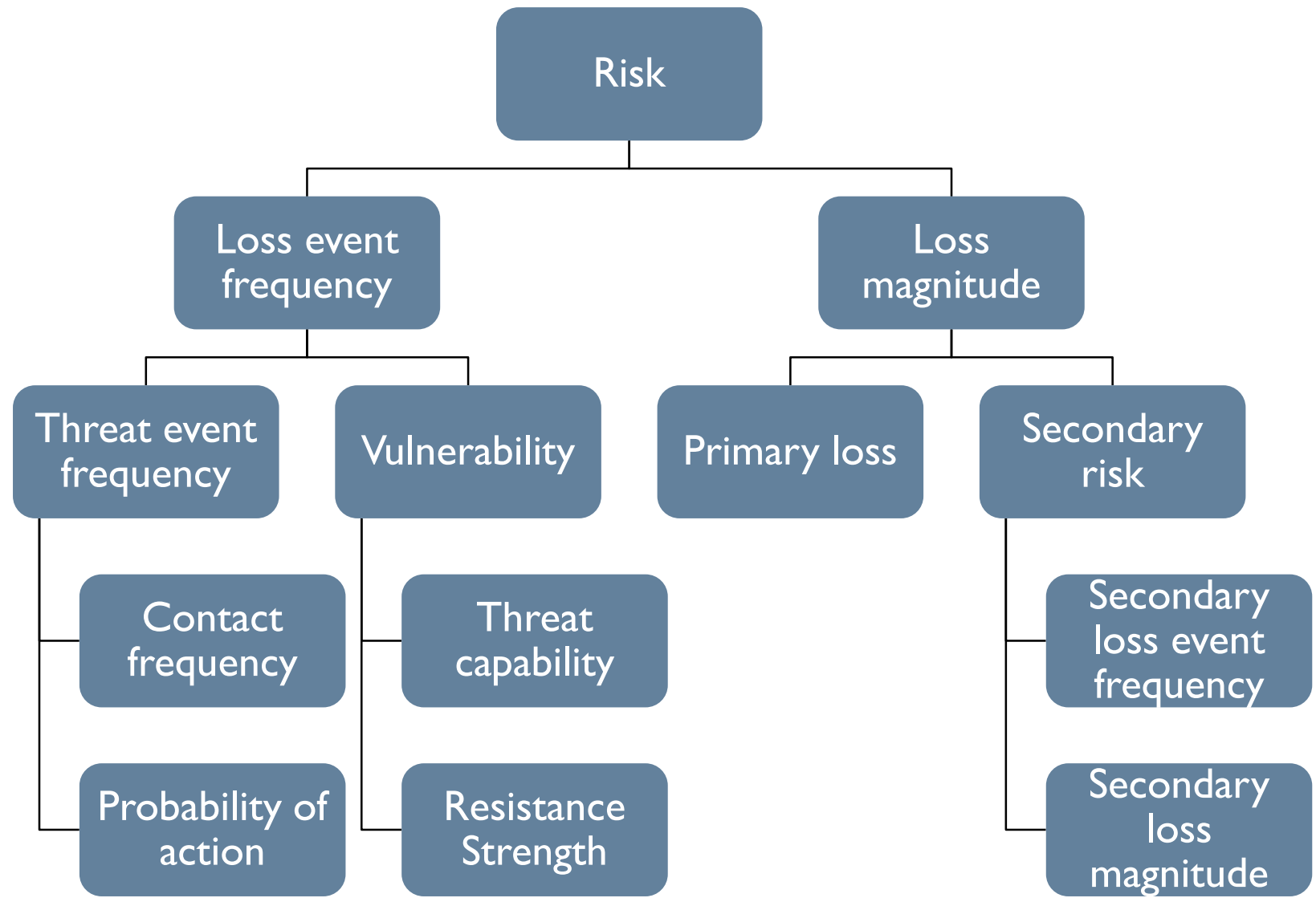
- ISO 27005
 - Information Security Risk Management
- Defines a systematic approach to manage risks for an organization



Factor Analysis of Information Risk (FAIR)

- International standard
 - Quantifying information security and operational risk
 - Provides a standard taxonomy and ontology for measuring risk
 - Complement to other risk assessment and management frameworks
- Supported by two organizations
 - FAIR Institute
 - Promotes FAIR
 - Open Group
 - Publishes Open FAIR risk taxonomy and analysis standards

FAIR Model



Risk Definition

$$\text{Risk} = \text{Impact} \times \text{Likelihood}$$

$$\text{Risk} = \text{Impact} \times (\text{Vulnerability} \times \text{Threat})$$

- NIST definition
 - “A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence”
- FAIR definition
 - “Probable frequency and magnitude of future loss”

Intrusion Kill Chain

- Attackers must progress through each phase of the chain to achieve their goal
 - Breaking just one link in the chain disrupts the adversary
 - By understanding the attackers' perspective, defenders can gain an edge
 - Against even the most sophisticated attackers
 - Protect against zero-day exploits
 - Which is just one link in the chain



Recon

Weaponization

Delivery

Exploitation

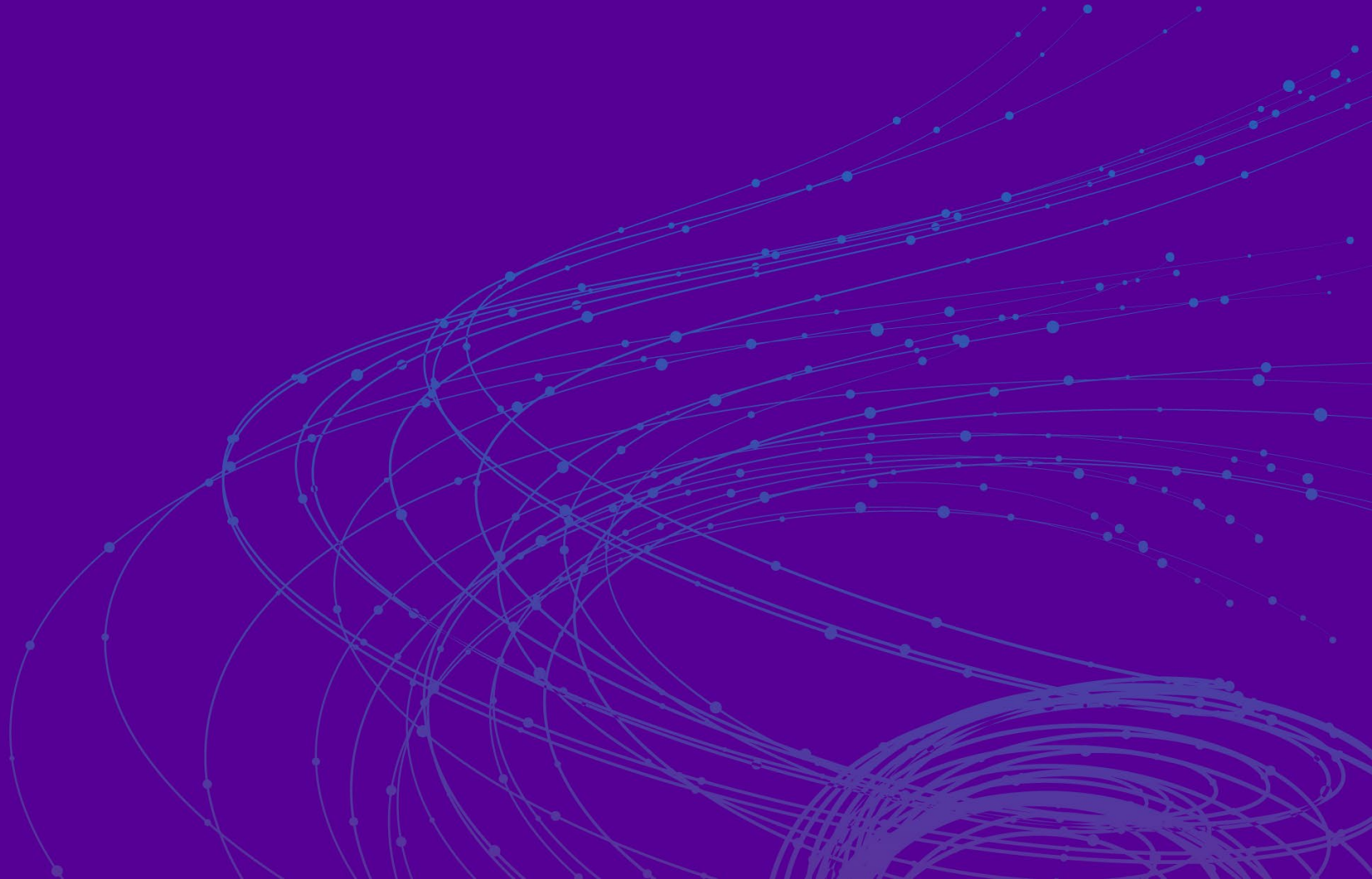
Installation

C2

Actions

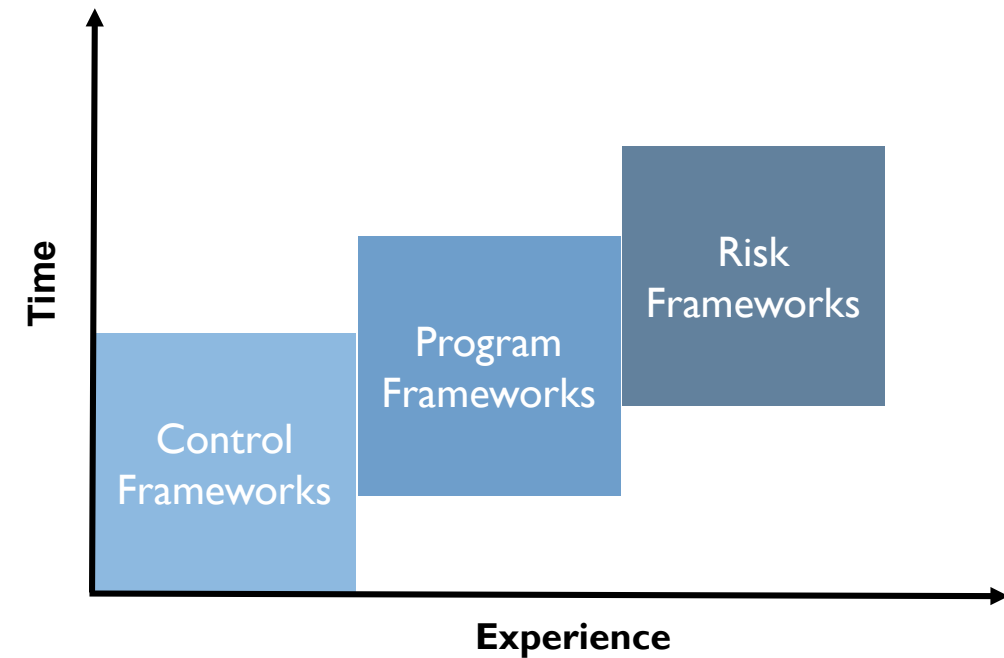
RSA[®]Conference2019

Summary



In Summary

- As you mature your security program
 - Choose one (or more) framework from each category
- Control Framework
 - Identify baseline controls to implement
- Program Framework
 - Build a comprehensive security program
 - Simplify communications with business
- Risk Framework
 - Prioritize security activities appropriately



Key Action Items

- Next week you should:
 - Identify the security frameworks used within your organization
- Within three months you should:
 - Understand how those frameworks are leveraged
 - Define how they are mapped to each other
- Within six months you should:
 - Update your security program plan to leverage each of the three types of frameworks
 - Socialize the plan with technical, operations, and executive leaders

RSA[®]Conference2019

Frank Kim

@fykim

frank.kim@thinksec.com

www.frankkim.net

*Material based on SANS MGT512
Security Leadership Essentials for Managers*