

CYBERSECURITY

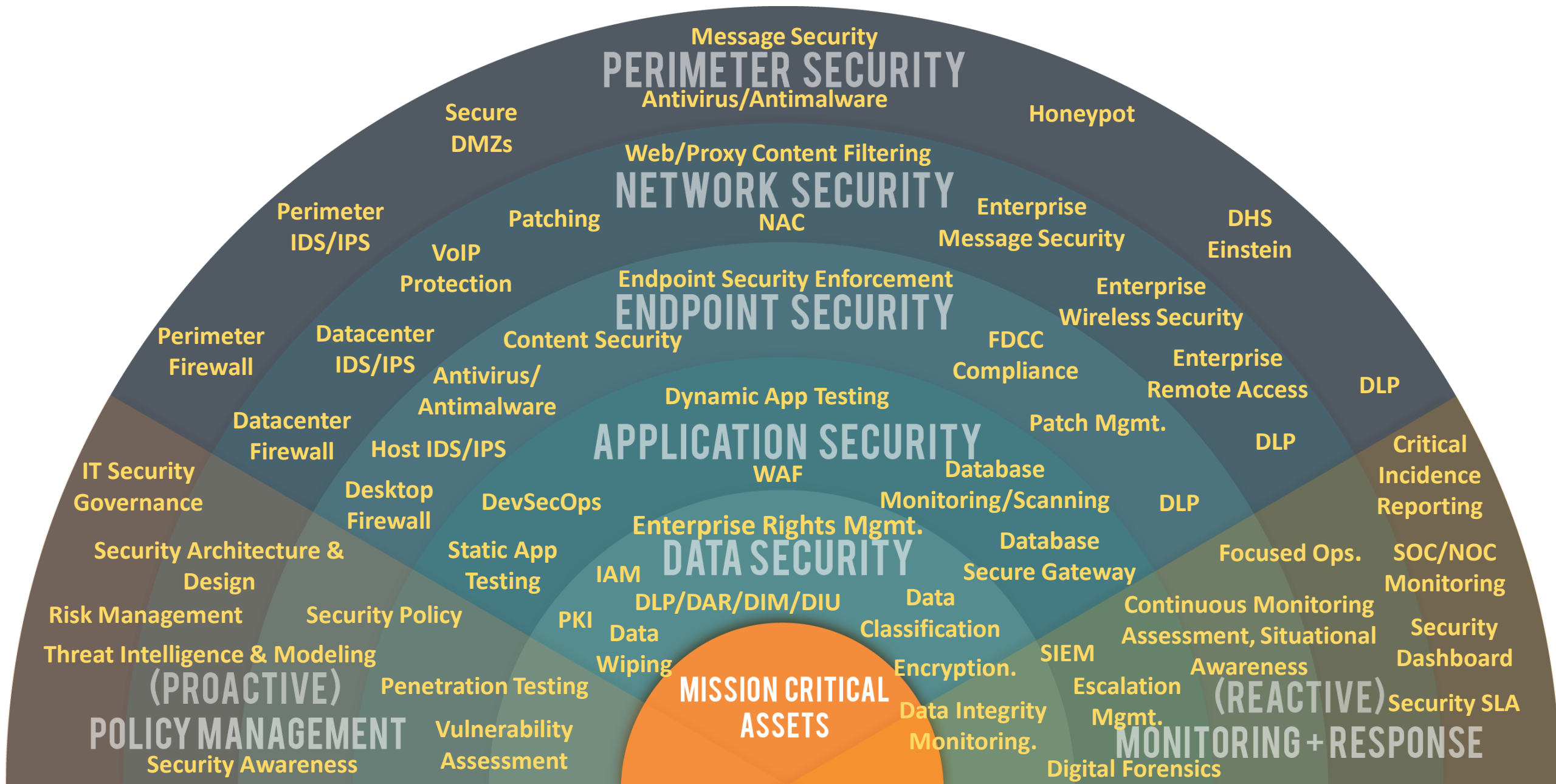
SESSION 2

**TEXAS SKILLS DEVELOPMENT FUND
TRAINING PARTNERSHIP**

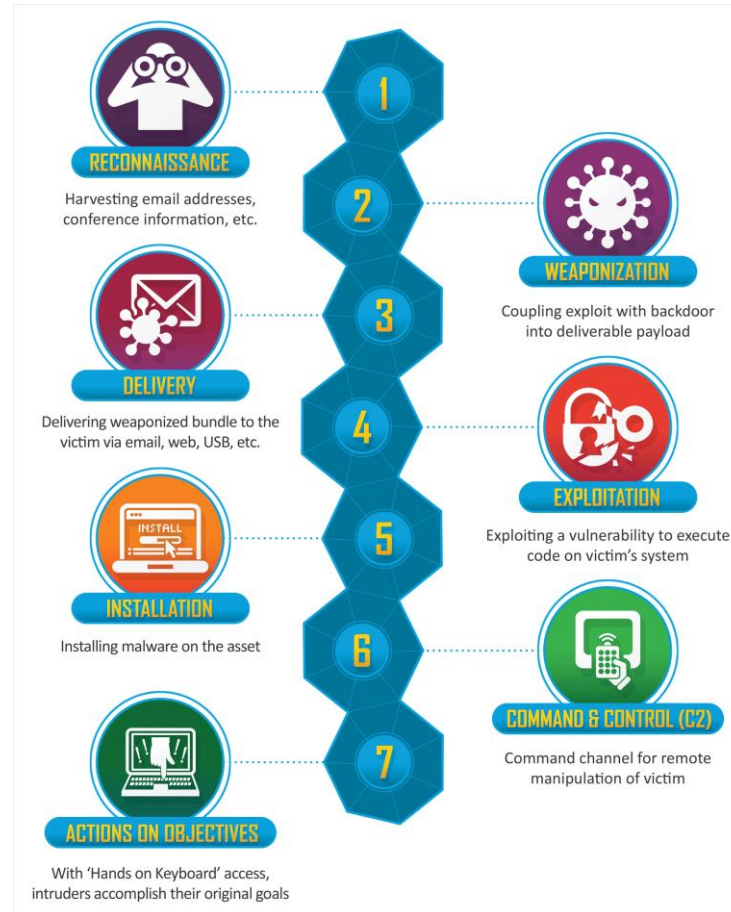


Cybersecurity Domains

- Foundational Security
 - Essential boundary protection
- Data Protection
 - Data integrity, Data privacy
- Security Operations
 - Business security assessment
 - Management & Response
- Cloud Security
 - Cloud services security
- Application Security
 - Software security gaps/flaws
- Risk & Compliance
 - Enterprise, operational, 3rd party
 - Information Technology
 - Remediation
- Identity Management
 - Authentication, Authorization
 - Identity challenges, Exposure
- IoT/ICS
 - Analytics, Operations, Assets
 - Communication Protocols
 - Remote monitoring, Detection



Lockheed Martin Kill Chain Framework



Kill Chain

Kill Chain Phase	Detect	Deny	Disrupt	Degrade	Deceive	Limit	Restore
Reconnaissance I							
Delivery							
Exploitation							
Installation							
Command and Control (C2)							
Reconnaissance II							
Actions on Objectives							

[Cybersecurity Threats, Malware Trends, and Strategies:](#)

[Learn to mitigate exploits, malware, phishing, and other social engineering attacks](#)

Kill Chain

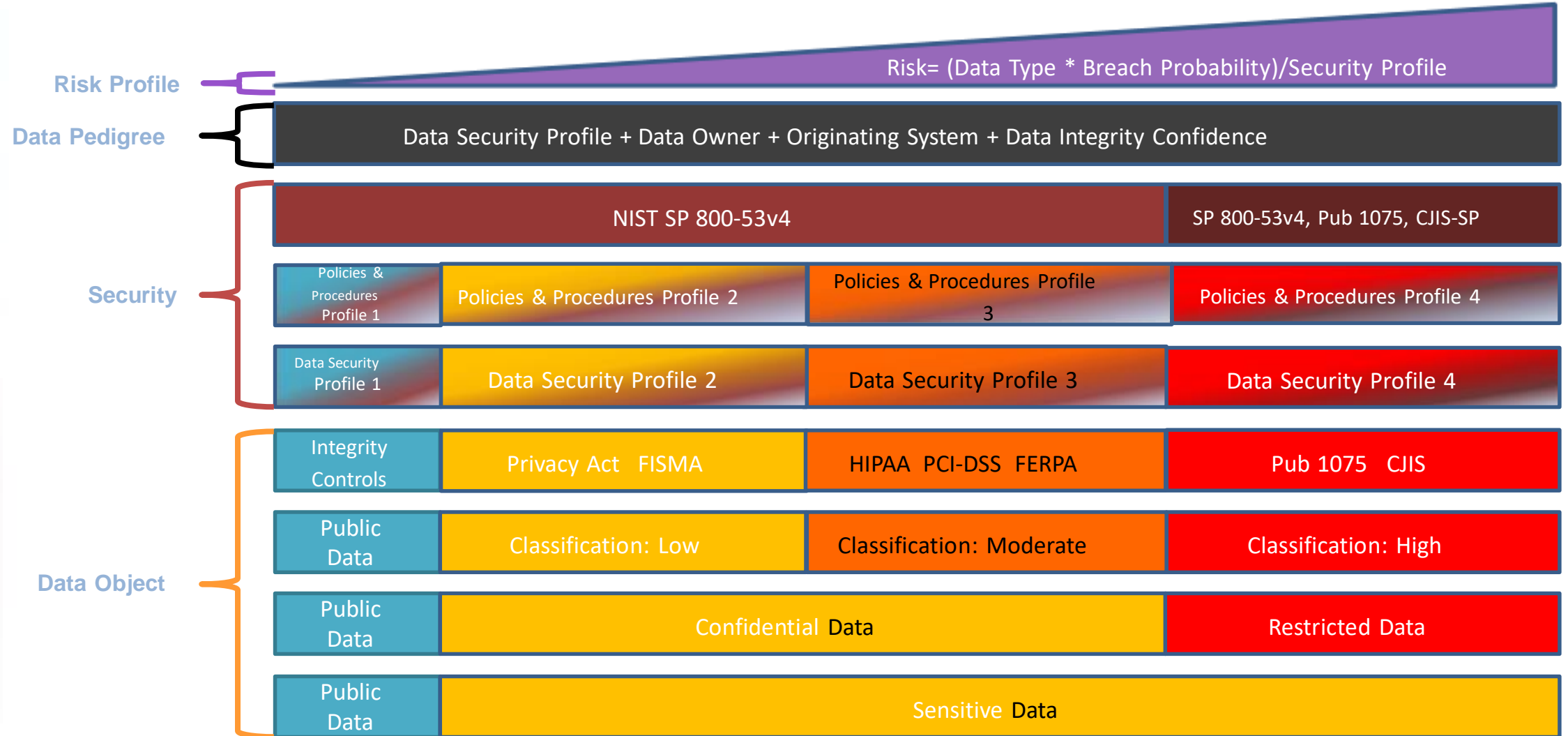
Kill Chain Phase	Detect	Detect Description	Detect Maturity Index (1-5)	Detect Data Consumer	Detect Consumer PoC	Detect Renewal Date	Deny	Deny Description	Deny Maturity Index (1-5)	Deny Data Consumer	Deny Consumer PoC	Deny Renewal Date
Reconnaissance I												
Delivery	control_name	Network IDS/IPS	3	SOC	Leonard Nimoy	09/15/24	control_name	email spam filter	2	eMail Administrator	Will Smith	01/01/24
Delivery	control_name	System image agent	1	IR Team	Bruce Dern	06/03/22	control_name	USB disable policy	2	Server Support	Bruno Mars	n/a
Exploitation	control_name	Windows Error Reporting	1	No one	No one	n/a	control_name	Anti-virus suite	4	SOC	Leonard Nimoy	04/15/21
Exploitation	control_name	System Integrity Monitor	2	SOC	Leonard Nimoy	06/09/22	control_name	File Integrity Monitoring	2	SOC	Leonard Nimoy	06/15/22
Exploitation	control_name	Anti-virus suite	4	Desktop Support	Kathy Bates	04/15/21	control_name	ASLR	5	Desktop Support	Kathy Bates	n/a
Installation	control_name	File Integrity Monitoring	2	Desktop Support	Kathy Bates	06/15/22	control_name	Anti-virus suite	4	Desktop Support	Kathy Bates	04/15/21
Installation	control_name	File Integrity Monitoring	2	Server Support	Bruno Mars	06/15/22	control_name	Anti-virus suite	4	Server Support	Bruno Mars	04/15/21
Installation	control_name	Anti-virus suite	4	SOC	Leonard Nimoy	04/15/21						
Installation	control_name	Anti-virus suite	4	IR Team	Bruce Dern	04/15/21						
Command and Control (C2)	control_name	Network IDS/IPS	3	NOC	Keanu Reeves	09/15/24	control_name	Network IDS/IPS	3	NOC	Keanu Reeves	09/15/24
Command and Control (C2)	control_name	Network IDS/IPS	3	SOC	Leonard Nimoy	09/15/24						
Reconnaissance II	control_name	Network IDS/IPS	3	NOC	Keanu Reeves	09/15/24	control_name	Network IDS/IPS	3	NOC	Keanu Reeves	09/15/24
Reconnaissance II	control_name	Network IDS/IPS	3	SOC	Leonard Nimoy	09/15/24						
Actions on Objectives	control_name	File Integrity Monitoring	2	Server Support	Bruno Mars	06/15/22	control_name	File Integrity Monitoring	2	Server Support	Bruno Mars	06/15/22
Actions on Objectives	control_name	File Integrity Monitoring	2	Desktop Support	Kathy Bates	06/15/22	control_name	File Integrity Monitoring	2	Desktop Support	Kathy Bates	06/15/22
Actions on Objectives	control_name	Deception technology	2	SOC	Leonard Nimoy	05/31/25						

[Cybersecurity Threats, Malware Trends, and Strategies:](#)

[Learn to mitigate exploits, malware, phishing, and other social engineering attacks](#)

MITRE ATT&CK Framework

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
<div>Active Scanning <small>(0/2)</small></div> <div>Gather Victim Host Information <small>(0/4)</small></div> <div>Gather Victim Identity Information <small>(0/3)</small></div> <div>Gather Victim Network Information <small>(0/6)</small></div> <div>Gather Victim Org Information <small>(0/4)</small></div> <div>Phishing for Information <small>(0/3)</small></div> <div>Search Closed Sources <small>(0/2)</small></div> <div>Search Open Technical Databases <small>(0/5)</small></div> <div>Search Open Websites/Domains <small>(0/2)</small></div> <div>Search Victim-Owned Websites</div>	<div>Acquire Infrastructure <small>(0/6)</small></div> <div>Compromise Accounts <small>(0/2)</small></div> <div>Compromise Infrastructure <small>(0/6)</small></div> <div>Develop Capabilities <small>(0/4)</small></div> <div>Establish Accounts <small>(0/2)</small></div> <div>Obtain Capabilities <small>(0/6)</small></div>	<div>Drive-by Compromise</div> <div>Exploit Public-Facing Application</div> <div>External Remote Services</div> <div>Hardware Additions</div> <div>Phishing <small>(0/3)</small></div> <div>Replication Through Removable Media</div> <div>Supply Chain Compromise <small>(0/3)</small></div> <div>Trusted Relationship</div> <div>Valid Accounts <small>(0/4)</small></div>	<div>Command and Scripting Interpreter <small>(0/8)</small></div> <div>Exploitation for Client Execution</div> <div>Inter-Process Communication <small>(0/2)</small></div> <div>Native API</div> <div>Scheduled Task/Job <small>(0/6)</small></div> <div>Shared Modules</div> <div>Software Deployment Tools</div> <div>System Services <small>(0/2)</small></div> <div>User Execution <small>(0/2)</small></div> <div>Windows Management Instrumentation</div>	<div>Account Manipulation <small>(0/4)</small></div> <div>BITS Jobs</div> <div>Boot or Logon Autostart Execution <small>(0/12)</small></div> <div>Boot or Logon Initialization Scripts <small>(0/5)</small></div> <div>Browser Extensions</div> <div>Compromise Client Software Binary</div> <div>Create Account <small>(0/3)</small></div> <div>Create or Modify System Process <small>(0/4)</small></div> <div>Event Triggered Execution <small>(0/15)</small></div> <div>Event Triggered Execution <small>(0/15)</small></div> <div>Group Policy Modification</div> <div>Hijack Execution Flow <small>(0/11)</small></div> <div>Hijack Execution Flow <small>(0/11)</small></div> <div>Implant Container Image</div> <div>Office Application Startup <small>(0/6)</small></div> <div>Pre-OS Boot <small>(0/5)</small></div> <div>Scheduled Task/Job <small>(0/6)</small></div> <div>Server Software Component <small>(0/3)</small></div>	<div>Abuse Elevation Control Mechanism <small>(0/4)</small></div> <div>Access Token Manipulation <small>(0/5)</small></div> <div>Boot or Logon Autostart Execution <small>(0/12)</small></div> <div>Boot or Logon Initialization Scripts <small>(0/5)</small></div> <div>Create or Modify System Process <small>(0/4)</small></div> <div>Event Triggered Execution <small>(0/15)</small></div> <div>Exploitation for Privilege Escalation</div> <div>Group Policy Modification</div> <div>Hijack Execution Flow <small>(0/11)</small></div> <div>Process Injection <small>(0/11)</small></div> <div>Scheduled Task/Job <small>(0/6)</small></div> <div>Valid Accounts <small>(0/4)</small></div>	<div>Abuse Elevation Control Mechanism <small>(0/4)</small></div> <div>Access Token Manipulation <small>(0/5)</small></div> <div>BITS Jobs</div> <div>Deobfuscate/Decode Files or Information</div> <div>Direct Volume Access</div> <div>Execution Guardrails <small>(0/1)</small></div> <div>Exploitation for Defense Evasion</div> <div>File and Directory Permissions Modification <small>(0/2)</small></div> <div>Group Policy Modification</div> <div>Hide Artifacts <small>(0/7)</small></div> <div>Hijack Execution Flow <small>(0/11)</small></div> <div>Impair Defenses <small>(0/7)</small></div> <div>Indicator Removal on Host <small>(0/6)</small></div> <div>Indirect Command Execution</div> <div>Masquerading <small>(0/6)</small></div> <div>Modify Authentication Process <small>(0/4)</small></div> <div>Modify Cloud Compute Infrastructure <small>(0/4)</small></div>	<div>Brute Force <small>(0/4)</small></div> <div>Credentials from Password Stores <small>(0/3)</small></div> <div>Exploitation for Credential Access</div> <div>Forced Authentication</div> <div>Input Capture <small>(0/4)</small></div> <div>Man-in-the-Middle <small>(0/2)</small></div> <div>Modify Authentication Process <small>(0/4)</small></div> <div>Network Sniffing</div> <div>OS Credential Dumping <small>(0/8)</small></div> <div>Steal Application Access Token</div> <div>Steal or Forge Kerberos Tickets <small>(0/4)</small></div> <div>Steal Web Session Cookie</div> <div>Two-Factor Authentication Interception</div> <div>Unsecured Credentials <small>(0/6)</small></div>	<div>Account Discovery <small>(0/4)</small></div> <div>Application Window Discovery</div> <div>Browser Bookmark Discovery</div> <div>Cloud Infrastructure Discovery</div> <div>Cloud Service Dashboard</div> <div>Cloud Service Discovery</div> <div>Domain Trust Discovery</div> <div>File and Directory Discovery</div> <div>Network Service Scanning</div> <div>Network Share Discovery</div> <div>Network Sniffing</div> <div>Password Policy Discovery</div> <div>Peripheral Device Discovery</div> <div>Permission Groups Discovery <small>(0/3)</small></div> <div>Process Discovery</div> <div>Query Registry</div> <div>Remote System Discovery</div> <div>Software Discovery <small>(0/1)</small></div>	<div>Exploitation of Remote Services</div> <div>Internal Spearphishing</div> <div>Lateral Tool Transfer</div> <div>Remote Service Session Hijacking <small>(0/2)</small></div> <div>Remote Services <small>(0/6)</small></div> <div>Replication Through Removable Media</div> <div>Software Deployment Tools</div> <div>Taint Shared Content</div> <div>Use Alternate Authentication Material <small>(0/4)</small></div>	<div>Archive Collected Data <small>(0/3)</small></div> <div>Audio Capture</div> <div>Automated Collection</div> <div>Clipboard Data</div> <div>Data from Cloud Storage Object</div> <div>Data from Configuration Repository <small>(0/2)</small></div> <div>Data from Information Repositories <small>(0/2)</small></div> <div>Data from Local System</div> <div>Data from Network Shared Drive</div> <div>Data from Removable Media</div> <div>Data Staged <small>(0/2)</small></div> <div>Email Collection <small>(0/3)</small></div> <div>Input Capture <small>(0/4)</small></div> <div>Man in the Browser</div> <div>Man-in-the-Middle <small>(0/2)</small></div> <div>Screen Capture</div> <div>Video Capture</div>	<div>Application Layer Protocol <small>(0/4)</small></div> <div>Communication Through Removable Media</div> <div>Data Encoding <small>(0/2)</small></div> <div>Data Obfuscation <small>(0/3)</small></div> <div>Dynamic Resolution <small>(0/3)</small></div> <div>Encrypted Channel <small>(0/2)</small></div> <div>Fallback Channels</div> <div>Ingress Tool Transfer</div> <div>Multi-Stage Channels</div> <div>Non-Application Layer Protocol</div> <div>Non-Standard Port</div> <div>Protocol Tunneling</div> <div>Proxy <small>(0/4)</small></div> <div>Remote Access Software</div> <div>Traffic Signaling <small>(0/1)</small></div> <div>Web Service <small>(0/3)</small></div>	<div>Automated Exfiltration <small>(0/1)</small></div> <div>Data Transfer Size Limits</div> <div>Exfiltration Over Alternative Protocol <small>(0/3)</small></div> <div>Exfiltration Over C2 Channel</div> <div>Exfiltration Over Other Network Medium <small>(0/1)</small></div> <div>Exfiltration Over Physical Medium <small>(0/1)</small></div> <div>Exfiltration Over Web Service <small>(0/2)</small></div> <div>Scheduled Transfer</div> <div>Transfer Data to Cloud Account</div>	<div>Account Access Removal</div> <div>Data Destruction</div> <div>Data Encrypted for Impact</div> <div>Data Manipulation <small>(0/3)</small></div> <div>Defacement <small>(0/2)</small></div> <div>Disk Wipe <small>(0/2)</small></div> <div>Endpoint Denial of Service <small>(0/4)</small></div> <div>Firmware Corruption</div> <div>Inhibit System Recovery</div> <div>Network Denial of Service <small>(0/2)</small></div> <div>Resource Hijacking</div> <div>Service Stop</div> <div>System Shutdown/Reboot</div>



Data Protection

Data integrity, Data privacy

DATA LOSS PREVENTION PROVIDERS

CA Technologies	McAfee
Check Point	Netskope
Code42	Proofpoint
CoSoSys	Somansa
Digital Guardian	SuperCom
Fidelis CyberSecurity	Symantec/Blue Coat
Forcepoint	X1
IS Decisions	Zecurion

e-DISCOVERY PROVIDERS

AccessData	OpenText/ Guidance Software
BlackBag Technologies	Logicube
Consilio	MSAB
Digital Intelligence	Nuix
Fidelis Cybersecurity	Relativity
Forcepoint	Symantec
Ground Labs	

DATA DISCOVERY AND CLASSIFICATION PROVIDERS

1TOUCH.io	OneTrust
BigID	Protegrity
Cognigo	Seclore
Covata	Tanium
IBM Security	Titus
Imperva	Varonis
Microsoft	

FILE INTEGRITY PROTECTION PROVIDERS

FireEye	Symantec
LogRhythm	Tripwire
McAfee	Varonis Systems
STEALTHbits Technologies	

ENCRYPTION PROVIDERS

Certes Networks	Ionic
Check Point	Kindite
CipherCloud	McAfee
CryptoMove	PKWARE
Cyphre	Proofpoint
DataLocker	Protegrity
Duality Technologies	SecurityFirst
Enveil	Thales
Gemalto	Vaultive
HP	

DATABASE SECURITY PROVIDERS

DB Networks	Imperva
Fortinet	McAfee
IBM Security	Oracle

PUBLIC KEY INFRASTRUCTURE PROVIDERS

Acertia	RSA
Certes Networks	Symantec
Futurex	Thales
Gemalto	Venafi
HydrantID	

DATA ACCESS GOVERNANCE PROVIDERS

Bolden James	Netskope
Covertix	SailPoint Technologies
Druva	STEALTHbits Technologies
IS Decisions	Veritas

RISK MANAGEMENT PROVIDERS

Allure Security

FinalCode

Ionic

Microsoft

Seclore

Vera

Virtru

Votiro

TOKENIZATION PROVIDERS

Gemalto

TokenEX

SECURE COLLABORATION PROVIDERS

Box

Mattermost

Wiretap

BLOCKCHAIN PROVIDERS

Chainalysis

Leonovus

Security Operations

Monitoring & Operations, Change Management, Orchestration & Automation
Vulnerability Assessment & Management, Threat Detection & Analysis
Incident Management & Response – Forensics, Legal, Containment

ANALYTICS PROVIDERS

APCON	Outcold Solutions
Bricata	Palo Alto Networks
Confluent	Paterva
Corelight	Patrocinium Systems
CorrelationX	Preempt Security
Cybraics	RSA
DomainTools	SecBI
Elastic	SevOne
ExtraHop	Splunk
Gigamon	SS8
Indegy	ThetaRay
Insight Engines	ThreatModeler
IPsoft	TIBCO
JASK	Twingo
Knowi	UpGuard
LogRhythm	Verizon/ProtectWise
NetBrain	
Netsurion/ EventTracker	

SECURITY INFORMATION AND EVENT MANAGEMENT/LOGGING PROVIDERS

Alert Logic	LogRhythm
AT&T/AlienVault	McAfee
BlackStratus	Micro Focus
Chronicle	Microsoft
Cisco	Netsurion/EventTracker
CorreLog	New Relic
Delphix	Paessler AG
Devo	RSA
Exabeam	Splunk
Fortinet	Statseeker
IBM Security	Sumo Logic
JASK	TIBCO
LogPoint	Uplevel Security

APPLICATION PERFORMANCE MONITORING PROVIDERS

AppDynamics
ExtraHop
ManageEngine
New Relic

Riverbed Technology
SolarWinds
Symantec

ASSET MANAGEMENT PROVIDERS

1E
Absolute Software
Axonius
Blackberry/Cylance

Jamf Software
NetSupport
Symantec
VMware

NETWORK PERFORMANCE MONITORING PROVIDERS

Aruba
Arista
Cisco
Corelight
Gigamon
IDERA

Keysight
NetBrain
NetScout
Statseeker
Tridium

PATCH AND SYSTEM MANAGEMENT PROVIDERS

1E
Autonomic Software
Center for Internet Security
GFI Software
IBM Security
LogRhythm
Microsoft

Net New
Technologies (NNT)
Semperis
STEALTHbits
Symantec
Tanium

USER BEHAVIOR ANALYTICS/ ENTITY AND USER BEHAVIOR ANALYTICS PROVIDERS

Aruba	Forcepoint
Balabit	Gurukul
Bay Dynamics	Interset
BehavioSec	Jazz Networks
BioCatch	Prelert
Cylance	RSA/Fortscale
Dtex Systems	Securonix
Ekran System	Splunk
Exabeam	VMware/E8 Security

CONFIGURATION MANAGEMENT DATABASE PROVIDERS

Cisco	ServiceNow
McAfee	Skybox Security
Palo Alto Networks	Symantec

SECURITY ORCHESTRATION AND AUTOMATED RESPONSE PROVIDERS

Ayehu	Palo Alto Networks/
CyberInt	Demisto
CyberSponse	Proofpoint
FireEye	ServiceNow
IBM Security	Siemplify
LogRhythm	Splunk
Microsoft	Swimlane
NetBrain	VMware

ROBOTIC PROCESS AUTOMATION PROVIDERS

Automation Anywhere	OpenConnect
Blue Prism	WorkFusion

DevOps AUTOMATION PROVIDERS

AppViewX
Chef
Puppet

Red Hat
SaltStack

PENETRATION TESTING PROVIDERS

Rapid7

RiskSense

USER TESTING/SOCIAL ENGINEERING PROVIDERS

Barracuda Networks
Cofense
KnowBe4

MediaPRO
Proofpoint

VULNERABILITY MANAGEMENT AND TESTING PROVIDERS

Arxan
AttackIQ
Automox
Balbix
BeyondTrust
Code DX
Conventus
Cymulate
Expanse (formerly Qadium)
IBM Security
Joval
Outpost24
Pcysys
Qualys
Rapid7

Risk Based Security
RiskRecon
RiskSense
SafeBreach
SAINT Corporation
SCYTHE
Shodan
Tenable
ThirdPartyTrust
Titania
UpGuard
Verodin
Vulcan
WhiteHat Security
XM Cyber

THREAT INTELLIGENCE PROVIDERS

4iQ	IntSights
Anomali	Jigsaw Security
Bandura Cyber	McAfee
BinaryEdge AG	OPSWAT
Blueliv	Palo Alto Networks
BrandProtect	Perch Security
Centripetal Networks	Recorded Future
CrowdStrike	ReversingLabs
CyberInt	RiskIQ
DarkOwl	Seclytics
Digital Defense	Silobreaker
Digital Shadows	Sixgill
Expanse (formerly Qadium)	SpyCloud
Flashpoint	ThreatConnect
FireEye	ThreatMetrix
Forescout	ThreatQuotient
GreatHorn	TruSTAR Technology
GroupSense	VirusTotal
Intel 471	

CYBER RANGE PROVIDERS

Cyberbit

CYBERGYM

ADVANCED MALWARE DETECTION PROVIDERS

BluVector	McAfee
Bricata	ODIX
Check Point	Palo Alto Networks
Cisco	Proofpoint
Juniper Networks/Cyphort	ReversingLabs
Fidelis Cybersecurity	SonicWall
FireEye	Sophos
Forcepoint	Symantec
Fortinet	Trend Micro
Joe Security	Votiro
Lastline	

CONTAINMENT AND ISOLATION PROVIDERS

Carbon Black	Palo Alto Networks
CyberInt	SentinelOne
Fortinet	Symantec
Illumio	Trend Micro
Juniper Networks	VMware
McAfee	

ELIMINATION AND REMEDIATION PROVIDERS

1E	Iron Mountain
Blanco	LogicHub
CarbonHelix	Malwarebytes
CyberInt	One Identity/Balabit
Fidelis Cybersecurity	WhiteCanyon Software
Infocyte	

FORENSICS PROVIDERS

AccessData	FireEye
BlackBag Technologies	Intezer
Cisco	LSoft Technologies
Consilio	OpenText/ Guidance Software
CounterTack	Silicon Forensics
Cylance	Sumuri
Datiphy	TZWorks
DF Labs	WhiteCanyon Software
Digital Intelligence	
Fidelis Cybersecurity	





















LEGAL RESPONSE PROVIDER

OpenText/Guidance Software

Compliance

Security Regulations & Controls

Simplified compliance

Global	 ISO/IEC 27001	 SOC 1	 SOC 2	 PCI DSS L1 version 3	 Cloud Security Alliance Cloud Security Matrix	
United States	 FedRAMP	 HIPAA (Healthcare)	 FIPS 140-2	 Life Sciences GxP	 Family Educational Rights & Privacy Act	
Regional	 European Union Model Clause	 United Kingdom G-Cloud	 China Multi Layer Protection Scheme	 China CCCPPF	 Singapore Multi-Tier Cloud Security	 Australian Signals Directorate I-RAP Assessment
Coming soon	 Sarbanes Oxley	 Criminal Justice Information System	 Defense Information Systems Agency L2	 ITAR	 Defense Information Systems Agency L3-5	 ISO / IEC 27018

NIST 800-53

Abstract

This publication provides a catalog of security and privacy controls for federal information systems and organizations and

a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation),

organizational assets, individuals, other organizations, and the Nation from a

diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors.

IRS – Pub 1075

1.2 Overview of Publication 1075

This publication provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, or contractors adequately protect the confidentiality of FTI.

Enterprise security policies address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance to implement all applicable security controls. This document contains the managerial, operational, and technical security controls that must be implemented as a condition of receipt of FTI.

The guidelines outlined herein apply to all FTI, no matter the amount or the media in which it is recorded. FTI must be afforded the same levels of protection regardless of it residing on paper or electronic form. Systematic, procedural, or manual security policies must minimize circumvention.

IRS – Pub 1075

2.0 Federal Tax Information and Reviews	
2.1 General	
2.2 Authorized Use of FTI	
2.3 Secure Data Transfer	
2.4 State Tax Agency Limitations	
2.5 Coordinating Safeguards within an Agency	
2.6 Safeguard Reviews	
2.7 Conducting the Review	
Table 1 – Safeguard Review Cycle	
2.7.2 Computer Security Review Process	
Table 2 – IT Testing Techniques	
2.8 Corrective Action Plan	
2.9 Voluntary Termination of Receipt of FTI	
2.9.1 Termination Documentation	
2.9.2 Archiving FTI Procedure (for agencies terminating receipt of FTI but required by statute retain FTI for designated periods)	

3.0 Recordkeeping Requirement – IRC 6103 (p)(4)(A)	15
3.1 General	15
3.2 Electronic and Non-Electronic FTI Logs	15
4.0 Secure Storage—IRC 6103(p)(4)(B)	
4.1 General	
4.2 Minimum Protection Standards	
Table 3 – Minimum Protection Standards	
4.3 Restricted Area Access	
Figure 2 – Sample Visitor Access Log	
4.3.1 Use of Authorized Access List	
4.3.2 Controlling Access to Areas Containing FTI	
4.3.3 Control and Safeguarding Keys and Combinations	
4.3.4 Locking Systems for Secured Areas	
4.4 FTI in Transit	
4.5 Physical Security of Computers, Electronic, and Removable Media	
4.6 Media Off-Site Storage Requirements	
4.7 Telework Locations	
4.7.1 Equipment	
4.7.2 Storing Data	
4.7.3 Other Safeguards	

IRS – Pub 1075

Table 3 – Minimum Protection Standards

Secured Perimeter	The perimeter is enclosed by slab-to-slab walls constructed of durable materials and supplemented by periodic inspection. Any lesser-type partition must be supplemented by electronic intrusion detection and fire detection systems. All doors entering the space must be locked in accordance with Locking Systems for Secured Areas. In the case of a fence/gate, the fence must have intrusion detection devices or be continually guarded, and the gate must be either guarded or locked with intrusion alarms.
Security Room	A security room is a room that has been constructed to resist forced entry. The entire room must be enclosed by slab-to-slab walls constructed of approved materials (e.g., masonry brick, concrete) and supplemented by periodic inspection, and entrance must be limited to specifically authorized personnel. Door hinge pins must be non-removable or installed on the inside of the room.
Badged Employee	During business hours, if authorized personnel serve as the second barrier between FTI and unauthorized individuals, the authorized personnel must wear picture identification badges or credentials. The badge must be clearly displayed and worn above the waist.
Security Container	A security container is a storage device (e.g., turtle case, safe/vault) with a resistance to forced penetration, with a security lock with controlled access to keys or combinations.

Global

- ☰ Azure Policy Regulatory Compliance (preview)
- ☰ CIS benchmark
- ☰ CSA STAR attestation
- ☰ CSA STAR certification
- ☰ CSA STAR self-assessment
- ☰ SOC 1, 2, 3
- ☰ WCAG

Global

- ☰ ISO 20000-1
- ☰ ISO 22301
- ☰ ISO 27001
- ☰ ISO 27017
- ☰ ISO 27018
- ☰ ISO 27701
- ☰ ISO 9001

US government

- ☰ CJIS
- ☰ CNSSI 1253
- ☰ DFARS
- ☰ DoD DISA L2, L4, and L5
- ☰ DoE 10 CFR Part 810
- ☰ EAR

US government

- ☰ FedRAMP
- ☰ FERPA (US)
- ☰ FIPS 140-2
- ☰ IRS 1075
- ☰ ITAR
- ☰ NIST 800-171
- ☰ NIST CSF
- ☰ Section 508 VPATs

Financial services

- ☰ 23 NYCRR Part 500 (US)
- ☰ AFM and DNB (Netherlands)
- ☰ AMF and ACPR (France)
- ☰ APRA (Australia)
- ☰ CFTC 1.31 (US)
- ☰ EBA (EU)
- ☰ FCA and PRA (UK)
- ☰ FFIEC (US)
- ☰ FINMA (Switzerland)
- ☰ FINRA 4511 (US)
- ☰ FISC (Japan)
- ☰ FSA (Denmark)

Financial services

- ☰ GLBA (US)
- ☰ KNF (Poland)
- ☰ MAS and ABS (Singapore)
- ☰ NBB and FSMA (Belgium)
- ☰ OSFI (Canada)
- ☰ PCI DSS
- ☰ RBI and IRDAI (India)
- ☰ SEC 17a-4 (US)
- ☰ SEC Regulation SCI (US)
- ☰ Shared Assessments
- ☰ SOX (US)
- ☰ TruSight

Health

- ☰ HDS (France)
- ☰ HIPAA & HITECH (US)
- ☰ HITRUST (US)
- ☰ MARS-E (US)
- ☰ NEN 7510 (Netherlands)

Media and manufacturing

- ☰ CDSA
- ☰ DPP (UK)
- ☰ FACT (UK)
- ☰ GxP (FDA 21 CFR Part 11)
- ☰ MPAA
- ☰ NERC (US)
- ☰ TISAX (Germany)

Regional

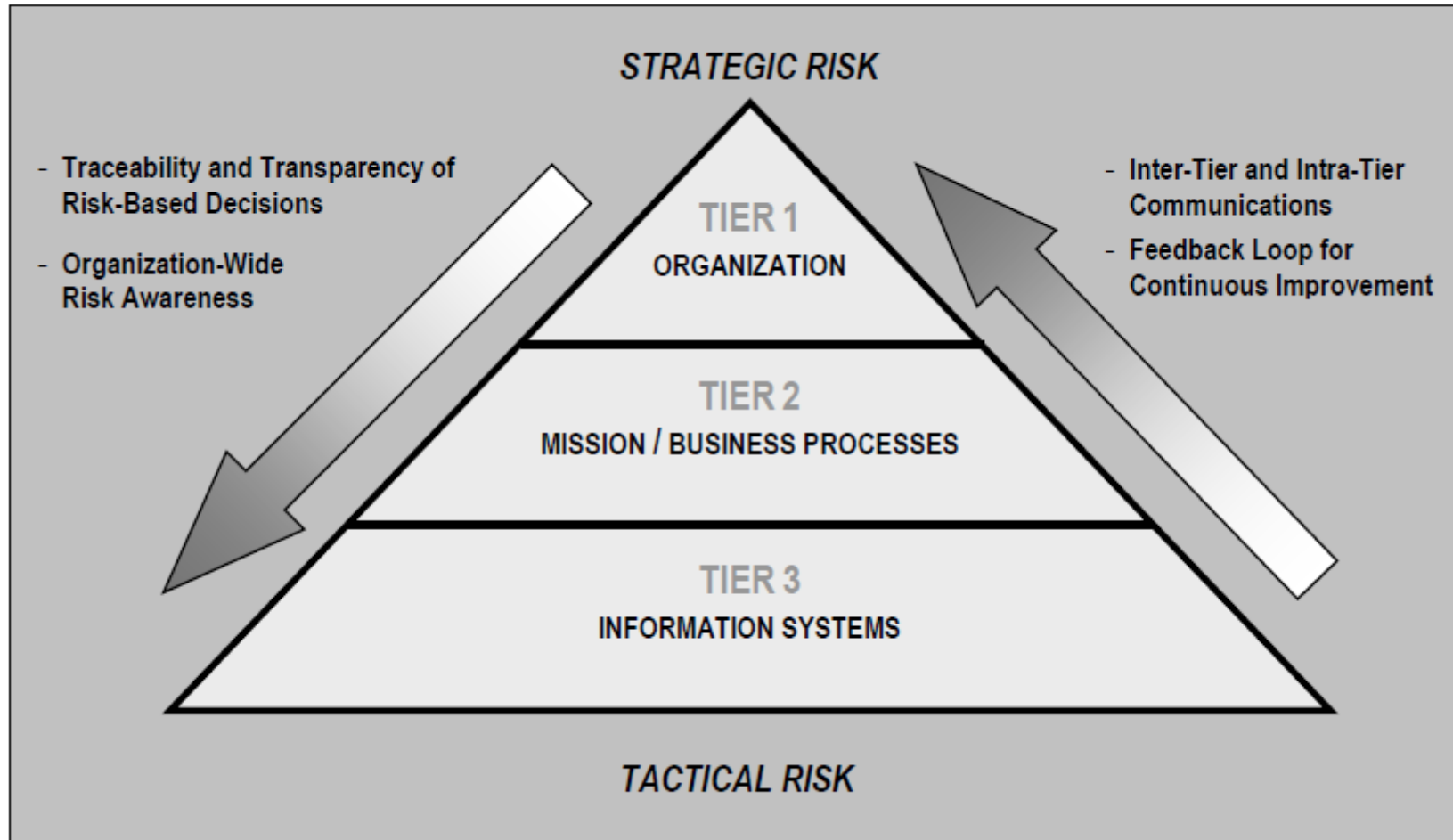
- ☰ BIR 2012 (Netherlands)
- ☰ C5 (Germany)
- ☰ CCPA (US California)
- ☰ IRAP and CCSL (Australia) ¹²
- ☰ CS Gold Mark (Japan)
- ☰ Cyber Essentials PLUS (UK)
- ☰ Canadian Privacy Laws
- ☰ DJCP (China) ¹²

Regional

- ☰ EN 301 549 (EU)
- ☰ ENS (Spain)
- ☰ ENISA IAF (EU)
- ☰ EU Model Clauses
- ☰ EU-US Privacy Shield
- ☰ GB 18030 (China) ¹²
- ☰ GDPR (EU)
- ☰ G-Cloud (UK)
- ☰ ISMS (Korea)

Regional

- ☰ IT-Grundschutz (Germany)
- ☰ DPA (Spain)
- ☰ MeitY (India)
- ☰ MTCS (Singapore) ¹²
- ☰ My Number (Japan)
- ☰ NZ CC (New Zealand) ¹²
- ☰ PASF (UK)
- ☰ PDPA (Argentina)
- ☰ TRUCS (China) ¹²



Architecture Description

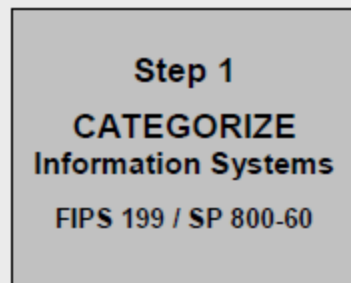
- Mission/Business Processes
- FEA Reference Models
- Segment and Solution Architectures
- Information System Boundaries

Organizational Inputs

- Laws, Directives, Policy, Guidance
- Strategic Goals and Objectives
- Information Security Requirements
- Priorities and Resource Availability

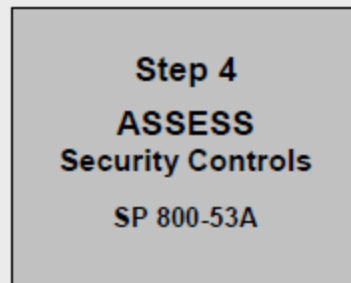
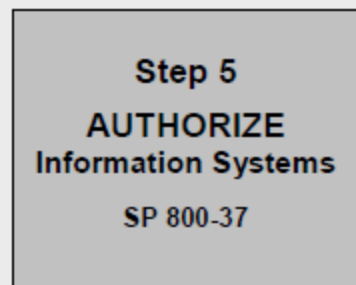
Starting Point

Repeat as necessary



RISK MANAGEMENT FRAMEWORK

Security Life Cycle



Note: CNSS Instruction 1253 provides guidance for RMF Steps 1 and 2 for National Security Systems (NSS).

The generalized format for expressing the security category, SC, of an information system is:

SC information system = $\{(\mathbf{confidentiality}, \textit{impact}), (\mathbf{integrity}, \textit{impact}), (\mathbf{availability}, \textit{impact})\},$

where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

AU-3 CONTENT OF AUDIT RECORDS

Control: The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred). Related controls: AU-2, AU-8, AU-12, SI-11.

Control Enhancements:

(1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION

The information system generates audit records containing the following additional information: [Assignment: organization-defined additional, more detailed information].

Supplemental Guidance: Detailed information that organizations may consider in audit records includes, for example, full-text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest.

(2) CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT

The information system provides centralized management and configuration of the content to be captured in audit records generated by [Assignment: organization-defined information system components].

Supplemental Guidance: This control enhancement requires that the content to be captured in audit records be configured from a central location (necessitating automation). Organizations coordinate the selection of required audit content to support the centralized management and configuration capability provided by the information system. Related controls: AU-6, AU-7.

Priority and Baseline Allocation:

P1	LOW AU-3	MOD AU-3 (1)	HIGH AU-3 (1) (2)
----	----------	--------------	-------------------

Risk and Compliance

Governance

GOVERNANCE, RISK AND COMPLIANCE PROVIDERS

Consilio
CyberOne
CyberSaint Security
Galvanize
LockPath
MetricStream
OneTrust

Panaseer
RSA
SAP
SigmaFlow
SimpleRisk
TrustMapp

FRAUD PROVIDERS

Arkose Labs