Your Logo
Will Be
Placed Here

INFORMATION ASSURANCE PROGRAM (IAP)

ACME Business Consulting, LLC

IAP
Information Assurance Program

Table of Contents

Notice 5
Intended Audience 5
Referenced Frameworks 5
Executive Summary 6
Overview of Information Assurance Program Activities 7
Logical Flow of Actions 7
Alignment With ACME's Risk Appetite 8
Compliance Use Cases for IAP 9
Shared Risk Management Responsibilities 9
SDLC/PDLC Involvement 9
Hands-On Testing & Evaluation 9
Reporting On Findings – Formal Risk Assessment 10
Cybersecurity & Privacy Decision on Risk 10
Managing Risk Through Information Assurance Program 11
Including Cybersecurity & Privacy Principles by Design 11
Data-Centric Risk Management 12
Key Stakeholders 12
Chief Information Security Officer (CISO) 13
Chief Privacy Officer (CPO) 13
Data Protection Officer (DPO) 13
Chief Risk Officer (CRO) 13
Cybersecurity Department (CSD) 13
Assigned Security Engineer (ASE) 13
Business Process Owner (BPO) 13
Project Manager (PM) 14
Asset Custodians 14
IAP's Phased Approach To Testing 14
IAP Phase 1: Categorize 14
IAP Phase 2: Select 14
IAP Phase 3: Implement 14
IAP Phase 4: Assess 15
IAP Phase 5: Authorize 15
IAP Phase 6: Monitor 15
IAP's Integration of System & Project Management Phases 15
SDLC/PDLC Phase: Initiate 16
SDLC/PDLC Phase: Design, Build & Acquire 16
SDLC/PDLC Phase: Implement & Assess 17
SDLC/PDLC Phase: Operate & Maintain 18
SDLC/PDLC Phase: Dispose 18
Determining The Appropriate Level of Assurance 19
Baseline Security Categorization – Basic or Enhanced Assurance 19
Basic Assurance 19
Enhanced Assurance 19
Determining Mandatory and Discretionary Technology Controls 20
Technology Controls By Assurance Level 20
Determining the Data Sensitivity Rating 21
Data Classification: Restricted 21
Data Classification: Confidential 21
Data Classification: Internal Use 21
Data Classification: Public 22
Determining the Safety & Criticality Rating 22
SC-1: Mission Critical 22
SC-2: Business Critical 22
SC-3: Non-Critical 23

CATEGORIZING CYBERSECURITY & PRIVACY CONTROLS 24
IDENTIFYING CYBERSECURITY & PRIVACY CONTROLS - MINIMUM SECURITY REQUIREMENTS (MSR) 24
ORGANIZATION CONTROLS BY FUNCTION 24
IDENTIFYING CONTROLS 24
PROTECTIVE CONTROLS 24
DETECTIVE CONTROLS 25
RESPONSIVE CONTROLS 25
RECOVERY CONTROLS 25

INFORMATION ASSURANCE PROGRAM ACTIVITIES 26
IAP TIMELINES 26
EXPECTED DELIVERABLES 26
SECURITY & PRIVACY TESTING PLAN (SPTP) 26
PROJECT RISK REGISTER (PRR) 26
SECURITY & PRIVACY ASSESSMENT REPORT (SPAR) 26
TEST OBJECTIVES 26
PERFORMING SECURITY TESTING 27
IAP WORKFLOW OVERVIEW – INPUTS, ACTIONS & DELIVERABLES 27
FORMAL RISK DETERMINATION 28
AUTHORIZATION TO OPERATE (ATO) 28
AUTHORIZATION TO USE (ATU) 28
INTERIM AUTHORIZATION TO OPERATE (IATO) 28
INTERIM AUTHORIZATION TO USE (IATU) 28
DENIED AUTHORIZATION TO OPERATE (DATO) 28
DENIED AUTHORIZATION TO USE (DATU) 28
"GO LIVE" DECISION 28

APPENDICES 29
APPENDIX A - TASKS BY PHASE - PREPARE 29
P-8: MISSION OR BUSINESS FOCUS 29
P-9: SYSTEM STAKEHOLDERS 29
P-10: ASSET IDENTIFICATION 31
P-11: AUTHORIZATION BOUNDARY 31
P-12: INFORMATION TYPES 32
P-13: INFORMATION LIFE CYCLE 32
P-14: RISK ASSESSMENT (SYSTEM) 33
P-15: SECURITY & PRIVACY REQUIREMENTS 34
P-16: ENTERPRISE ARCHITECTURE 34
P-17: REQUIREMENTS ALLOCATION 35
P-18: SYSTEM REGISTRATION 36
APPENDIX B - TASKS BY PHASE - CATEGORIZE 37
C-1: SYSTEM DESCRIPTION 37
C-2: SECURITY CATEGORIZATION 37
C-3: SECURITY CATEGORIZATION REVIEW & APPROVAL 38
APPENDIX C - TASKS BY PHASE - SELECT 39
S-1: CONTROL SELECTION 39
S-2: CONTROL TAILORING 39
S-3: CONTROL ALLOCATION 40
S-4: DOCUMENTATION OF PLANNED CONTROL IMPLEMENTATIONS 41
S-5: CONTINUOUS MONITORING STRATEGY (SYSTEM) 41
S-6: PLAN REVIEW & APPROVAL 42
APPENDIX D - TASKS BY PHASE - IMPLEMENT 43
I-1: CONTROL IMPLEMENTATION 43
I-2: UPDATE CONTROL IMPLEMENTATION INFORMATION 45
APPENDIX E - TASKS BY PHASE - ASSESS 46
A-1: ASSESSOR SELECTION 46
A-2: ASSESSMENT PLAN 46
A-3: CONTROL ASSESSMENTS 47
A-4: ASSESSMENT REPORTS 48
A-5: REMEDIATION ACTIONS 48

A-6: Plan of Action & Milestones (POA&M) 49
Appendix F - Tasks by Phase - Authorize **51**
R-1: Authorization Package 51
R-2: Risk Analysis & Determination 51
R-3: Risk Response 52
R-4: Authorization Decision 52
R-5: Authorization Reporting 54
Appendix G - Tasks by Phase - Monitor **55**
M-1: System & Environment Changes 55
M-2: Ongoing Assessments 55
M-3: Ongoing Risk Response 56
M-4: Authorization Package Updates 58
M-5: Security & Privacy Reporting 58
M-6: Ongoing Authorization 59
M-7: System Disposal 60
Appendix H – Cybersecurity & Privacy Control Selection **61**
Step 1: Download The Latest Version of the Secure Controls Framework (SCF) 61
Step 2: Identify All Applicable Requirements 61
Step 3: Filter Out Non-Applicable Requirements 61
Step 4: Assign Controls To Stakeholders 62

Glossary: Acronyms & Definitions **63**
Acronyms **63**
Definitions **63**

Record of Changes **64**

INTENDED AUDIENCE

Personnel involved in system development and project management activities should use this guide to obtain an understanding of Information Assurance Program (IAP) activities. This document contains program-level guidance that is specifically focused on the following functions internal to ACME and its third-party service providers:

- Business Process Owners (BPOs)
- Project managers
- Program managers
- Business analysts
- Privacy analysts (e.g., Data Protection Officers (DPOs))
- Solutions architects (e.g., IT and cybersecurity architects)
- Systems integrators
- Asset custodians (e.g., system admins)
- Governance, Risk and Compliance (GRC) analysts

REFERENCED FRAMEWORKS

This document leverages numerous leading industry frameworks in an effort to provide a data-centric, holistic approach to securely designing, building and maintaining ACME Business Consulting, LLC (ACME)'s systems, applications and services. The following external content is a non-exhaustive list of frameworks that are referenced by or support this IAP document:

- The National Institute of Standards and Technology (**NIST**): [1]
  - NIST 800-37: Risk Management Framework (RMF) for Information Systems and Organizations.
  - NIST 800-39: Managing Cybersecurity Risk: Organization, Mission and Information System View
  - NIST 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
  - NIST 800-64: Security Considerations in Secure Development Life Cycle
  - NIST 800-122: Guide to Protecting the Confidentiality of Personal Information (PI)
  - NIST 800-128: Guide for Security-Focused Configuration Management of Information Systems
  - NIST 800-160: Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
  - NIST 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations
  - NIST 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
  - NIST IR 7298: Glossary of Key Cybersecurity Terms
  - NIST IR 8179: Criticality Analysis Process Model: Prioritizing Systems and Components [draft]
  - NIST Framework for Improving Critical Cybersecurity (Cybersecurity Framework)
- The International Organization for Standardization (**ISO**):[2]
  - ISO 15288: Systems and Software Engineering -- System Life Cycle Processes
  - ISO 22301: Societal Security – Business Continuity Management Systems – Requirements
  - ISO 27002: Information Technology -- Security Techniques -- Code of Practice for Cybersecurity Controls
  - ISO 31010: Risk Management – Risk Assessment Techniques
- Other Frameworks:
  - Cloud Security Alliance Cloud Controls Matrix (**CSA CCM**)[3]
  - Center for Internet Security (**CIS**)[4]
  - Department of Defense Cybersecurity Agency (**DISA**) Secure Technology Implementation Guides (**STIGs**)[5]
  - European Union General Data Protection Regulation (**EU GDPR**) – Article 35(7)
  - International Association of Privacy Professionals (**IAPP**)[6]
  - Open Web Application Security Project (**OWASP**)[7]
  - Secure Controls Framework (**SCF**)[8]

[1] National Institute of Standards and Technology - http://csrc.nist.gov/publications/PubsSPs.html
[2] International Organization for Standardization - https://www.iso.org
[3] Cloud Security Alliance - https://cloudsecurityalliance.org/
[4] Center for Internet Security - https://www.cisecurity.org/
[5] DoD Information Security Agency - http://iase.disa.mil/stigs/Pages/index.aspx
[6] International Association of Privacy Professionals - https://iapp.org
[7] OWASP - https://www.owasp.org
[8] Secure Controls Framework – https://www.securecontrolsframework.com

EXECUTIVE SUMMARY

Misconfigurations create risk by increasing exposure. The validation of security and privacy controls is an elemental step to reduce unnecessary exposure and risk.

Implementing cybersecurity and privacy protections is a team effort that requires coordinated actions throughout the System / Project Development Lifecycle (SDLC/PDLC) of systems, applications and services. This is crucial for ACME to be able to demonstrate that both security and privacy principles were thoughtfully designed and implemented as part of standard project management processes. This concept is commonly referred to as Information Assurance (IA).

ACME's Cybersecurity Department (CSD) is responsible for implementing and administering the cybersecurity program to both protect assets from reasonable threats and maintain compliance with applicable statutory, regulatory and contractual obligations. To ensure ACME develops and implements secure systems, ACME has instituted an Information Assurance Program (IAP) program, which is designed to support existing risk management processes.

The objectives of the IAP program are to:

- Uncover design, implementation, and operational flaws that may impact cybersecurity and privacy concerns;
- Determine the effectiveness of preventive and detective controls, as well as monitoring/responsive capabilities;
- Assess the degree of consistency between the security and privacy plans and their operational deployment; and
- Maintain evidence of pre-production testing to demonstrate cybersecurity and privacy principles were implemented by design.

This guide serves as a reference for ACME's IAP so that secure processes can be implemented consistently across the organization and facilitate the management of overall risk. The focus of IAP efforts is to evaluate if the appropriate cybersecurity and privacy controls exist to minimize identified risks to an acceptable level. This includes an evaluation of both technical and non-technical safeguards to determine the effectiveness of implemented controls.

As depicted below, risk involves (1) bad actors who wish to harm ACME assets and (2) ACME, which wants to protect its assets. This is where operationalizing cybersecurity and privacy controls reduce risk.

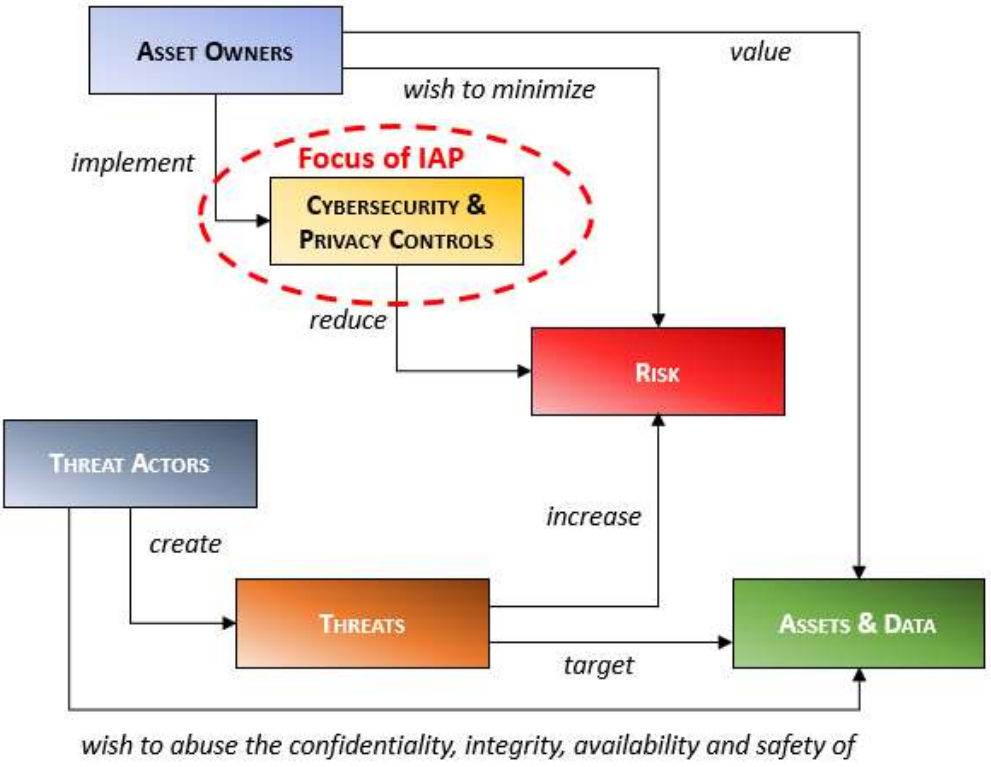


Figure 1: Focus of IAP to reduce risk.

The process of validating and documenting cybersecurity and privacy controls is an evolving expectation that stems from several recent statutory and regulatory developments affecting nearly every industry (e.g., EU GDPR and NIST 800-171). This expectation for "pre-production testing" is a necessary activity for all new systems, applications and services to ensure ACME builds and maintains a secure operating environment.

LOGICAL FLOW OF ACTIONS

From project kickoff to "go live," the diagram below describes the high-level overview of the interactive nature of the IAP process to identify, resolve and manage risks throughout the SDLC/PDLC:

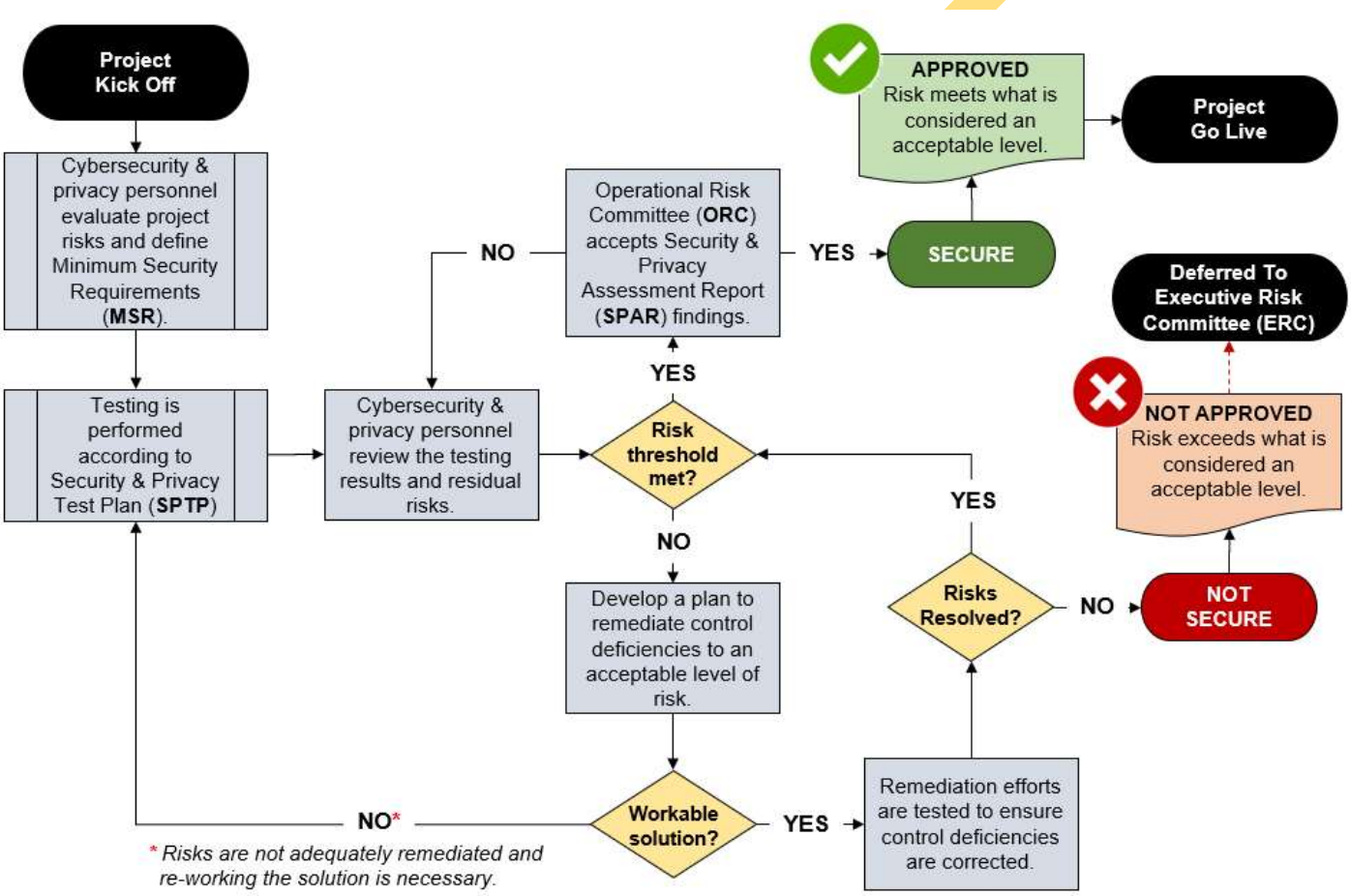


Figure 2: IAP flow chart.

IAP is intended to be non-punitive, where helpful cybersecurity and privacy guidance is provided throughout the development process. However, if security concerns are not addressed during development, it is important to note that the Cybersecurity Department (CSD) does have the authority to temporarily block systems, applications and services from going into production without senior ACME leadership approval (e.g., CIO, COO, CEO, board of directors, etc.) as part of ACME's existing change control process. The escalation will be handled through the Executive Risk Committee (ERC) to either receive the appropriate level of risk acceptance or guidance to suspend/terminate the system/application/service.

Based on the category of risk, ACME's Risk Management Program (RMP) identifies the appropriate management level within ACME to escalate the acceptance of risk, since the BPO's leadership role within the organization may not be senior enough to accept these higher levels of risk.

Alignment With ACME's Risk Appetite

CSD's role in managing risk is to align with ACME's overall strategy and business objectives, so that the assessment of risk is based on an understanding of what drives the business, such that innovation and creativity are uninhibited.

CSD is not the sole owner of risk and it is impossible to reach a state of "100% protection" since there will always be tradeoffs based on budgetary constraints, business needs and technology limitations.

Through the IAP's formal testing methodology, ACME is able to accurately identify, assess and remediate the risks posed from new technologies and projects. The IAP also benefits to the project team by reducing roadblocks and security-related issues through a process of proactive risk management.

CSD utilizes a two-step approach to cybersecurity and privacy-related risk as part of the IAP:

1. Define the Minimum Security Requirements (MSR), based on ACME's overall risk tolerance; and
2. Serve in an operational role to identify, assess and communicate risk.

CSD will communicate risk in a standardized manner that focuses on real-world implications. The definitions of risk come from ACME's Risk Management Program (RMP) and are summarized into five (5) risk categories:

- Low
- Medium
- High
- Severe
- Extreme

In accordance with the RMP, each higher level of risk comes with an elevated level of management that is required to accept the risk on behalf of ACME. These clipping levels are specifically designed to protect the brand, revenue and customers.

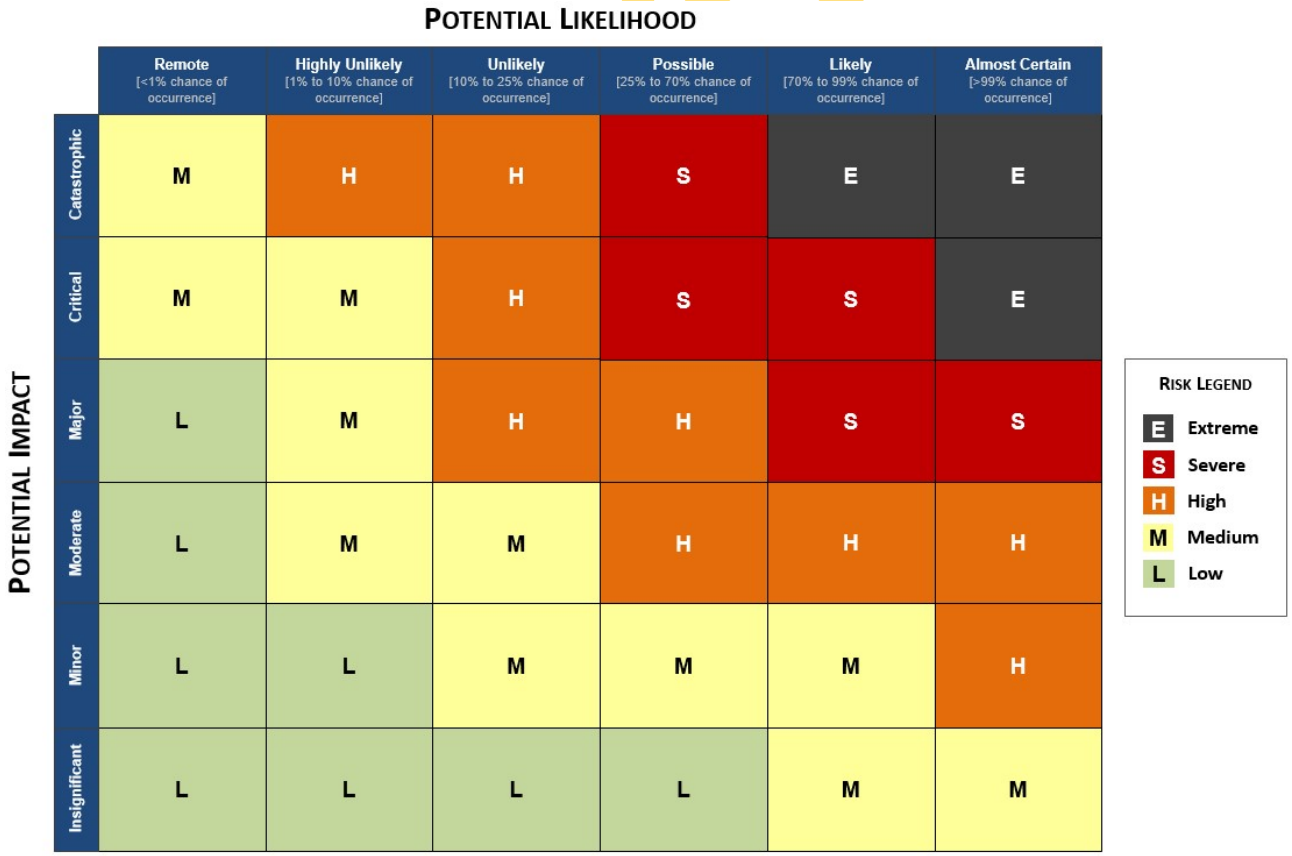


Figure 3: Risk matrix from the RMP.

Compliance Use Cases for IAP

The following are common statutory, regulatory and contractual requirements for "pre-production testing" that IAP addresses:

- **ISO 27002** – 14.2.8
- European Union General Data Protection Regulation (**EU GDPR**) – Article 25
- **NIST 800-171** – 3.12.1, 3.12.3 & Non-Federal Organization (NFO)
- **NIST Cybersecurity Framework** – PR.IP-2, PR.IP-5 & DE.DP-3
- Federal Risk and Authorization Management Program (**FedRAMP**) – Security Assessment & Authorization (CA) controls
- AICPA Trust Services Principles (TSP) **SOC2** – CC7.4
- Center for Internet Security Critical Security Controls (**CIS CSC**) – 18.2, 18.4 & 18.8
- Cloud Security Alliance Cloud Controls Matrix (**CSA CCM**) – CCC-03
- Cloud Computing Compliance Controls Catalogue (**C5**) – BEI-02
- Monitory Authority of Singapore Technology Risk Management (**MAS TRM**) Guidelines - 6.0.1, 6.2.2, 6.2.3, 6.2.4, 6.3.4, 6.4.2, 6.4.3, 6.4.4, A.1.1 & A.1.2
- European Union Agency for Network and Information Security (**ENISA**) Technical Guideline of Security Measures – SO23
- National Industry Security Program Operating Manual (**NISPOM**) – 8-610 & 8-302
- Criminal Justice Information Services (**CJIS**) Security Policy – 5.10.4.1, 5.11.1.1, 5.11.1.2, 5.11.2 & 5.13.4.1
- Massachusetts **MA 201 CMR 17.00** – 17.03(2)(d)(B)(i) & 17.03(2)(h)
- New York Department of Financial Services (**23 NYCRR 500**) – 500.02
- Oregon Consumer Identity Theft Protection Act (**OCITPA**) – 622(2)(B)(i)-(iv)
- Underwriters Laboratories (**UL**) 2900-1 – Section 12
- Payment Card Industry Data Security Standard (**PCI DSS**) – Requirement 6
- Motion Picture Association of America (**MPAA**) Content Security Program – MS-2.0

Shared Risk Management Responsibilities

CSD's role is as a trusted advisor, with the goal of effectively communicating risk and advice such that the Business Process Owner (BPO) can make informed decisions. The BPO is ultimately responsible for making the decision on whether risks are worth taking:

- The CSD, in conjunction with Operational Risk Committee (ORC) and Executive Risk Committee (ERC), is responsible for advising on options the BPO has for managing risks; and
- The BPO is responsible for making a risk-based decision for the best course of action to take.

SDLC/PDLC Involvement

IAP should be viewed as an integral component within the System Development Life Cycle (SDLC) / Project Development Life Cycle (PDLC). Project Managers (PMs) & BPOs should ensure CSD is involved in projects as early as possible in the SDLC/PDLC since adequate, prior planning is needed for security testing:

- Prior CSD involvement will prevent security testing from being a "roadblock" to a project rollout.
- CSD needs to be involved at project kickoff, if at all possible.
    - If CSD is brought in on the later part of a project, the PM and BPO must understand that compressed timelines could negatively impact CSD resources in performing security testing.
    - A lack of resources due to unplanned IAP requirements may also impact the planned "go live" date of the project.

Hands-On Testing & Evaluation

CSD assigns Minimum Security Requirements (MSR) (e.g., cybersecurity and privacy controls) commensurate with the operational significance and projected financial value associated with the system/application/service.

- CSD develops a Security & Privacy Test Plan (SPTP) to evaluate the security and privacy controls of the system/application/service to ensure adequate protection is in place to protect the confidentiality, integrity and availability of the systems and data.
- CSD executes the plan and keeps stakeholders informed of the findings so immediate remediation steps can be taken to fix any identified vulnerabilities or misconfigurations.
- CSD then works with the BPO and PM to schedule a follow-on assessment is performed to ensure adequate remediation of the issues have been properly addressed.

Reporting On Findings – Formal Risk Assessment

Once testing according to the SPTP is complete, CSD analyzes the results and documents the findings in a Security & Privacy Assessment Report (SPAR), which is a risk-based evaluation if the system/application/service meets MSR.

The SPAR will note not only the original, inherent risk, but also the remaining, residual risk after remediation, based on validation of the remediation being performed. This is done to assist in the final decision on risk acceptance.

Cybersecurity & Privacy Decision on Risk

The SPTP is reviewed by the Operational Risk Committee (ORC), which includes the Assigned Security Engineer (ASE) and Data Protection Officer (DPO) who come together to make and a risk-based decision if the system/application/service should be accredited for use in a production environment. Essentially, this the formal opinion from cybersecurity and privacy representatives on the level of risk posed to ACME, based on the results of IAP.

If risks are deemed to be unacceptable and a viable solution is not able to be implemented, the risk decision is deferred to the Executive Risk Committee (ERC), which includes the Chief Information Security Officer (CISO), Chief Risk Officer (CRO) and Chief Privacy Officer (CPO). The ERC will determine the appropriate next steps for the system/application/service under review.

- Contingency plan
- Ensure that appropriate personnel are available to assist with testing.
- Implement steps to remediate identified vulnerabilities and configuration issues in a timely manner.
- Ensure project team follows appropriate change control procedures.

Project Manager (PM)

PMs are responsible for the following activities associated with IAP:

- Include CSD and the DPO on project kick-off meetings.
- Involve CSD and the DPO early on in the SDLC/PDLC process to allow for ample time to conduct IAP.
- Liaise between the BPO, asset custodians and CSD to ensure SPTP documentation exists to perform IAP activities.

Asset Custodians

Asset custodians (e.g., system administrators) are responsible for the following activities associated with IAP:

- Implement controls to ensure systems, applications and services comply with ACME's policies and standards.
- Develop Standardized Operating Procedures (SOPs) for their area of responsibility.
- Monitor system integrity, protection levels, and security-related events.
- Follow up on detected security anomalies associated with systems, applications and services under their control.
- Assist in IAP activities, as directed.

IAP's Phased Approach To Testing

IAP phases are based on NIST 800-37, *Risk Management Framework (RMF) for Information Systems & Organizations*.[9] These contains six (6) distinct phases:

1. Categorize
2. Select
3. Implement
4. Assess
5. Authorize
6. Monitor

These phases contain the actionable steps required to ensure that throughout the life of the system, application or service, security and privacy principles are appropriately identified and implemented to reduce risk.

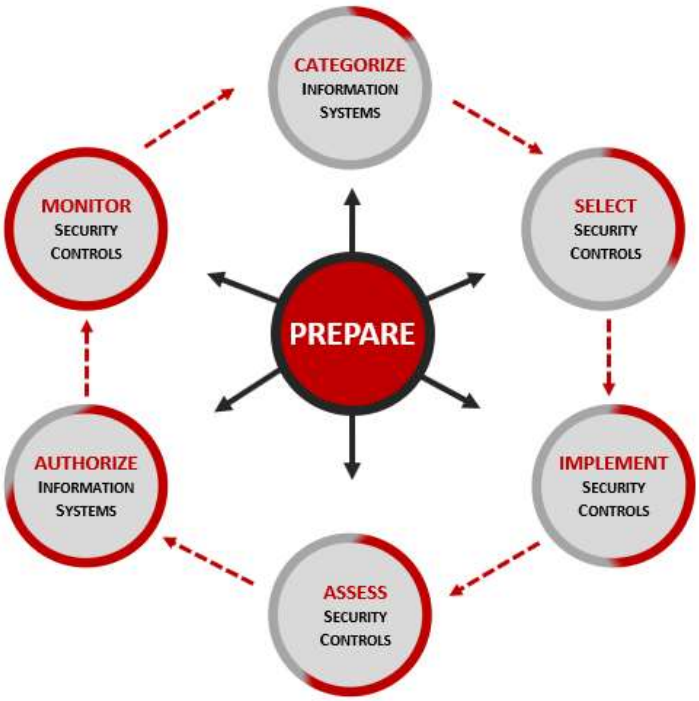


Figure 8. NIST 800-37 "Risk Management Framework".

IAP Phase 1: Categorize

The tasks associated with the Categorize phase help govern ACME risk management processes by determining the adverse impact to organizational operations and assets, individuals and other organizations with respect to the loss of confidentiality, integrity, availability and safety of ACME systems, applications and services. See Appendix B for specific tasks associated with the Categorize phase.

IAP Phase 2: Select

The tasks associated with the Select phase help select, tailor, and document the controls necessary to protect the system, application or service commensurate with risk to ACME operations and assets, individuals and other organizations. See Appendix C for specific tasks associated with the Select phase.

IAP Phase 3: Implement

The tasks associated with the Implement phase help define the controls in the security and privacy plans for system, application or service to create a baseline configuration with the specific details of the control implementation. See Appendix D for specific tasks associated with the Implement phase.

[9] National Institute of Standards and Technology - http://csrc.nist.gov/publications/PubsSPs.html

IAP Phase 4: Assess

The tasks associated with the Assess phase help determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system, application or service. See Appendix E for specific tasks associated with the Assess phase.

IAP Phase 5: Authorize

The tasks associated with the Authorize phase help provide organizational accountability by requiring a senior management official to determine if the security, privacy, and supply chain risk to ACME operations and assets, individuals or other organizations based on the operation of a system, application or service, is acceptable. See Appendix F for specific tasks associated with Authorize phase.

IAP Phase 6: Monitor

The tasks associated with the Monitor phase help maintain an ongoing situational awareness about the security and privacy posture of the system, application or service in support of risk management decisions. See Appendix G for specific tasks associated with the Monitor phase.

IAP's Integration of System & Project Management Phases

In reference to IAP operations, the lifespan of the system, application and service is based on SDLC/PDLC phases from NIST 800-64, which is necessary to cover the operations and eventual disposal of assets and data. This is important to account for, since traditional project management methodologies (e.g., PMBOK) end once "go live" is achieved, which can create a long-term gap in oversight throughout the usable lifecycle of the system, application or service. These five (5) NIST-based SDLC/PDLC phases include: [10]

- Initiate
- Design, Build & Acquire
- Implement & Assess
- Operate & Maintain
- Dispose

As depicted in the graphic below, these SDLC/PDLC phases provide governance oversight across the lifespan of the asset and are flexible enough to account for:

- Cybersecurity & privacy involvement;
- Agile development cycles;
- Traditional project management phases;[11]
- Major revisions;
- End of Life (EOL) decommissioning and disposal.

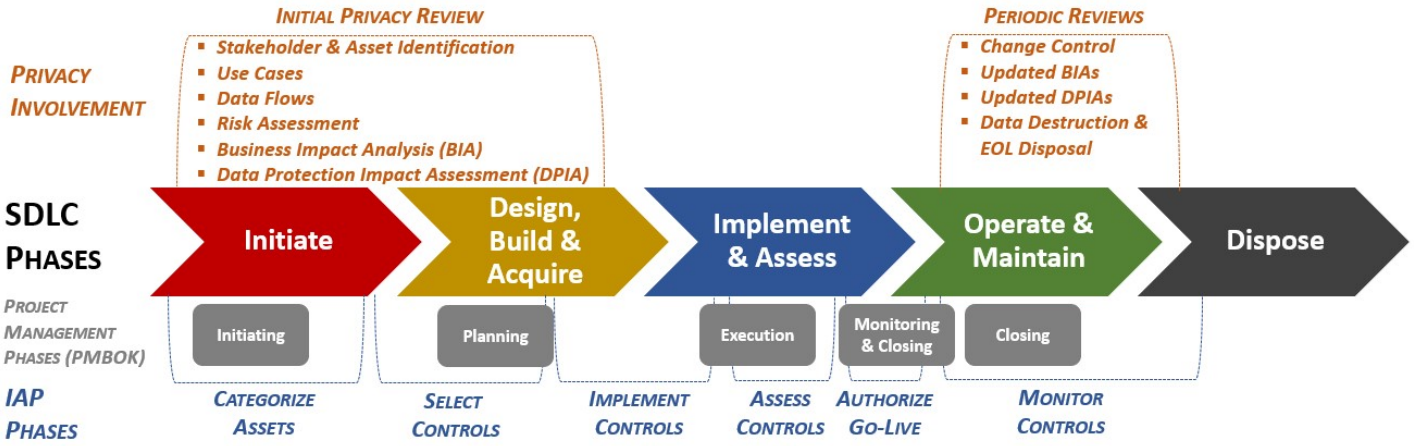


Figure 9: SDLC & IAP interaction.

[10] NIST SP 800-64 rev2 - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf
[11] Project Management Body of Knowledge (PMBOK) - https://www.pmi.org/pmbok-guide-standards

SDLC/PDLC Phase: Initiate

During this first phase of the SDLC/PDLC, cybersecurity and privacy considerations are key to diligent and early integration, thereby ensuring that threats, requirements, and potential constraints in functionality and integration are considered. At this point, cybersecurity and privacy are looked at more in terms of business risks.

Key activities in this SDLC/PDLC phase include:

- Tasks associated with the Categorize phase (see Appendix B for specific tasks associated with the Categorize phase);
- Identifying key cybersecurity and privacy roles.
- Identifying sources of project requirements, such as relevant statutory, regulatory and contractual obligations,
- Ensuring all key stakeholders have a common understanding, including cybersecurity and privacy implications, considerations, and requirements.
- Outlining initial thoughts on key milestones including timeframes.
- A determination of the acquisition strategy to be used throughout the remainder of the development process.
- A system concept review that verifies that the concept is viable, complete, achievable, and in line with organizational mission objectives and budgetary constraints.
- A performance specification review that ensures that the initial system design has addressed all currently identified specified security requirements.
- An Enterprise Architecture (EA) alignment that harmonizes IT vision, standards, and business requirements, as well as cybersecurity and alignment with current and imminent capabilities.
- A financial review that balances the cost implications associated with risk management.

To assist in further research, the matrix below provides a mapping of relevant industry publications to corresponding SDLC/PDLC activities during this phase:

SDLC/PDLC Phase Activity	Supporting Publications
Initiate security planning	NIST SP 800-64 NIST SP 800-100 NIST SP 800-37 NIST SP 800-53 ISO 15288
Categorizing systems	NIST SP 800-60 FIPS 199
Business Impact Assessment (BIA)	NIST SP 800-34
Data Protection Impact Assessment (DPIA)	NIST SP 800-37 IAPP DPIA Template[12]
Ensure secure system development processes	NIST SP 800-64 NIST SP 800-16

SDLC/PDLC Phase: Design, Build & Acquire

During this phase, the solution is designed, built and tested. This may include the acquisition and integration of third-party tools. This phase also includes conducting Proof of Concept (POC) evaluations and the procurement of technologies.

Key activities in this SDLC/PDLC phase include:

- Tasks associated with the Select phase (see Appendix C for specific tasks associated with the Select phase).
- Tasks associated with the Implement phase (see Appendix D for specific tasks associated with the Implement phase).
- An architecture/design review that evaluates the planned system design and potential integration with other systems as well as incorporation of shared services and common cybersecurity and privacy controls, such as authentication, disaster recovery, intrusion detection, or incident reporting.
- A performance review that evaluates whether the system is delivering, or capable of delivering, to the documented expectation of the owner and whether the system behaves in a predictable manner if it is subjected to improper use (e.g., the ability of the system to maintain availability and data integrity at the expected extreme resource loads).
- A functional review that ensures functional requirements identified are sufficiently detailed and are testable.
- Mid-project status & financial review is important to detect major shifts in planned level of effort to ensure cost-benefit ratios are monitored and effective decisions are continued.

[12] International Association of Privacy Professionals (IAPP) – DPIA Template - https://iapp.org/resources/article/template-for-data-protection-impact-assessment-dpia/

DETERMINING THE APPROPRIATE LEVEL OF ASSURANCE

Assets and services are categorized by two primary attributes: (a) the potential impact they pose from misuse and (b) the data classification level of the data processed, stored or transmitted by the asset or process. These two attributes combine to establish a basis for controls that should be assigned to that system or asset. *This basis is called an Assurance Level (AL)*.

BASELINE SECURITY CATEGORIZATION – BASIC OR ENHANCED ASSURANCE

This is straightforward where the data sensitivity rating represents the highest data classification of the data processed, stored or transmitted by the asset or process.

Where the data sensitivity intersect with Safety & Criticality (SC) levels, it is considered the Assurance Levels (AL). The AL represents the "level of effort" that is needed to properly ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of the asset or process. *It is important to note that SCs and data sensitivity ratings are independent characteristics.*

IAP Categorization Matrix		Data Sensitivity			
		Restricted	Confidential	Internal Use	Public
Safety & Criticality	SC-1 Mission Critical	ENHANCED	ENHANCED	ENHANCED	ENHANCED
	SC-2 Business Critical	ENHANCED	ENHANCED	BASIC	BASIC
	SC-3 Non-Critical	ENHANCED	BASIC	BASIC	BASIC

Figure 10: IAP categorization matrix.

BASIC ASSURANCE

Basic establishes the minimum level of control that would be "reasonably-expected" and is defined as industry-recognized secure practices (e.g., PCI DSS, NIST 800-53, ISO 27002, etc.). For security controls in Basic assurance projects or initiatives, the expectation for cybersecurity and privacy controls include:

- Controls are appropriately-scoped to address all applicable statutory, regulatory and contractual requirements;
- Technologies and processes are in-place with the expectation that no misconfigurations exist; and
- Flaw remediation processes correct any discovered flaws in a timely manner.

ENHANCED ASSURANCE

Enhanced establishes a more secure level of control that exceed minimum requirements and is defined as exceeding industry-recognized secure practices (e.g., DLP, FIM, DAM, etc.). These requirements are often "situationally required" per a statutory, regulatory or contractual obligation that is specific to a type of data or under a specific circumstance (e.g., personal data, cardholder data, electronic health protected information, etc.) where the expectation for cybersecurity and privacy controls include:

- Building upon Basic assurance requirements;
- Implementing robust preventative, detective and responsive capabilities exist that are commensurate with the value of the project to ACME; and
- Stakeholders perform a greater role in maintaining situational awareness to ensure controls are properly executed and governed.

Determining Mandatory and Discretionary Technology Controls

What sets the Basic and Enhanced requirements apart comes down to the technology controls in place, where Enhanced will have more protection in place than Basic. The expectation is that Basic contains "reasonably-expected protections" that would withstand scrutiny by an outside auditor or regulator, based on following industry-recognized practices to design, build and maintain secure systems, applications and services. In terms of "basic security," this consists of having antimalware protections, protecting sensitive data, maintain systems and reviewing security logs (see the chart below for more details).

Technology Controls By Assurance Level

When it is necessary to increase security requirements, additional controls will be needed. These Discretionary controls go above and beyond Mandatory controls to meet specific data protection needs that would withstand scrutiny by an outside auditor or regulator (see the chart below for specific examples of enhanced controls). The assignment of Enhanced controls is often required to meet a statutory, regulatory or contractual obligation (e.g., PCI DSS, EU GDPR, NIST 800-171, etc.).

The chart below is intended to provide reasonable guidance for expectations to keep systems, applications and services secure. The specifics of technology controls are determined by the technology platform, since certain technologies are not possible to be installed on all technology platforms.

Assurance Level	BASIC	ENHANCED
Level of Effort	Meets industry-recognized secure practices	Greater than basic industry-recognized secure practices
MANDATORY Technology Controls	▪ Antimalware (host-based) ▪ Encryption in transit (e.g., SSL/TLS, SFTP, SSH, etc.) ▪ Log collection (forwarded to centralized log collector) ▪ Patch management ▪ Vulnerability scanning ▪ Identity & Access Management (IAM)	▪ Antimalware (host-based) ▪ Configuration management (automated) ▪ Encryption at rest (e.g., file, folder, table or whole drive) ▪ Encryption in transit (e.g., SSL/TLS, SFTP, SSH, etc.) ▪ File Integrity Monitoring (**FIM**) ▪ Host Intrusion Prevention System (**HIPS**) ▪ Log collection (forwarded to **SIEM**) ▪ Mobile Device Management (**MDM**) ▪ Multi-Factor Authentication (**MFA**) ▪ Network Intrusion Detection / Protection (**NIDS** / **NIPS**) ▪ Next Generation Firewall (**NGF**) ▪ Patch management
DISCRETIONARY Technology Controls	▪ Configuration management (automated) ▪ Encryption at rest (e.g., file, folder, table or whole drive) ▪ Host Intrusion Prevention System (**HIPS**) ▪ Mobile Device Management (**MDM**) ▪ Multi-Factor Authentication (**MFA**) ▪ Network Intrusion Detection / Protection (**NIDS** / **NIPS**) ▪ Next Generation Firewall (**NGF**) ▪ Privileged Identity & Account Management (**PIAM**) ▪ Security Incident Event Manager (**SIEM**)	▪ Database encryption ▪ Database Access Management (**DAM**) ▪ Data Loss Prevention (**DLP**) ▪ Dynamic / Static Application Security Testing (**DAST** / **SAST**) ▪ Network Access Control (**NAC**) ▪ Penetration test ▪ Privileged Identity & Account Management (**PIAM**) ▪ Session recording ▪ Web Application Firewall (**WAF**)

Figure 11: Basic vs. Enhanced control expectations.

There will be cases where the Assurance Level may require a set of controls, but cybersecurity, privacy, technology or business teams feel additional controls are needed to address a specific risk. This is where discretionary controls come into play. Discretionary controls are at the discretion of stakeholders to implement that go above and beyond Mandatory controls.

Enhanced controls are "situationally required" and must be selected and implemented based on applicable statutory, regulatory or contractual requirements. In the absence of any such requirements, ACME may treat these controls or enhancements as discretionary technology controls.

IDENTIFYING CYBERSECURITY & PRIVACY CONTROLS - MINIMUM SECURITY REQUIREMENTS (MSR)

ACME leverages the Secure Controls Framework (SCF)[13] for its IAP controls, since it is the most scalable and efficient manner to organize cybersecurity and privacy controls. The SCF addresses over 100 statutory, regulatory and contractual frameworks, which allows for an efficient method to organize multiple sets of requirements into a single checklist of controls for each system/application/service that undergoes IAP. This checklist of controls constitutes the Minimum Security Requirements (MSR).

The SCF is a free resource for businesses, so all stakeholders in the IAP process, including external parties, can download and use the SCF. This allows the IAP process to utilize consistent terminology and controls nomenclature.

The overall process to identify the appropriate cybersecurity and privacy controls for IAP follows these steps:

1. Identify all applicable statutory, regulatory and contractual obligations.
2. Filter the SCF so only those applicable controls are shown.
3. Assign those applicable controls to stakeholders to ensure all requirements are properly addressed.

Reference Appendix H for the process to select appropriate cybersecurity and privacy controls.

ORGANIZATION CONTROLS BY FUNCTION

There are five (5) main categories of controls used during IAP activities:

- Identify
- Protect
- Detect
- Respond
- Recover

These categories align with the NIST Cybersecurity Framework (NIST CSF) approach to organize controls by function.

Figure 12: NIST Cybersecurity Framework functions.

IDENTIFYING CONTROLS

These controls are foundational for effective cybersecurity. Understanding the business context, resources that support critical functions, and the related cybersecurity risks enable ACME to focus its efforts and resources to properly secure its network.

Controls in this category focus on helping ACME understand the following:

- Business context;
- Resources that support critical functions; and
- Related cybersecurity risks.

PROTECTIVE CONTROLS

These controls focus on implementing the appropriate safeguards to ensure the safe functionality of systems, applications and services. These activities are performed consistent with ACME's risk strategy and support the ability to limit or contain the impact of a potential cybersecurity event.

Controls in this category focus on helping ACME understand the following:

- How user accounts are being managed;
- What the maintenance plan is to keep the system patched and secure;
- Change control processes;

[13] Secure Controls Framework (SCF) – https://www.securecontrolsframework.com

IAP is expected to be conducted as part of the SDLC/PDLC process for new systems, applications and services prior to its "go live" date, as well as existing critical systems at least every three (3) years or when a significant change made.

IAP TIMELINES

Due to the unique nature of each system/application/service undergoing IAP, providing a "cookie cutter" timeline will be inherently inaccurate. For this reason, it is necessary for CSD to be included as close to the project kick-off, as possible. The ability to assess the requirements will dictate the level of involvement of CSD throughout the SDLC/PDLC process.

CSD will create a system/application/service-specific timeline for IAP activities in a Security & Privacy Testing Plan (SPTP) document.

EXPECTED DELIVERABLES

There are several deliverables in the IAP process. The three (3) main deliverables from CSD to the involved parties for a system/project are the Security & Privacy Testing Plan (SPTP), Project Risk Register (PRR) and the Security & Privacy Assessment Report (SPAR).

SECURITY & PRIVACY TESTING PLAN (SPTP)

The SPTP will cover the following pertinent information that stakeholders need to be aware of:

- Scope of IAP for this specific assessment;
- Proposed timeline of activities and CSD deliverables;
- List of documentation artifacts CSD requires from stakeholders to conduct IAP, including due dates;
- Test objectives;
- Procedures that CSD will follow to perform testing; and
- Expected tools/technologies that will be used by CSD during testing.

After each component has been tested and corresponding results have been documented, an informal out-brief will take place between CSD and the applicable asset custodian, as well as the asset owner and project manager. Conducting out-briefs is an informal process since it is generally an ongoing process throughout the IAP.

Disclosure of the findings, especially any critical findings, provides the opportunity for immediate corrective action. Corrective actions can be implemented and, in most cases, should be implemented before the formal SPAR is written.

PROJECT RISK REGISTER (PRR)

CSD will maintain a PRR in the form of a Plan of Action & Milestones (POA&M) that serves as a "living document" to identify and track findings to ensure remediation actions are both assigned to the appropriate stakeholder and verified when completed.

SECURITY & PRIVACY ASSESSMENT REPORT (SPAR)

CSD developed a report format that includes results for each component tested, comments about additional information discovered during testing, statements about risk, and overall findings. Based on the nature of the SPAR, this document also serves as a Data Protection Impact Assessment (DPIA).

The assessor from CSD will sign off on the findings from IAP, certifying that the system/application/service does or does not meet the Minimum Security Requirements (MSR). In addition to the Operational Risk Committee (ORC), the Business Process Owner (BPO), Project Manager (PM) and other key stakeholders will receive a copy of the final SPAR.

TEST OBJECTIVES

CSD will use the test objectives to determine if a system, in its operational environment, and with the required security controls in place, satisfies Minimum Security Requirements (MSR). The expectation is that the test objectives map back to ACME's applicable policies, standards and compliance obligations.

Performing Security Testing

CSD personnel will perform IAP in accordance with the test procedures provided in the SPTP. System administrators or other technical personnel should be available at the time of testing to witness and execute necessary test procedures. In some cases, multiple technical personnel may be required to execute the test (e.g., CSD may need a Windows server administration to assist in testing controls on a Microsoft Windows Server as well as a SQL database administrator for database testing).

Prior to executing the IAP Plan, the IAP team will work with stakeholders to ensure the following:

- Components scheduled for testing are operational.
- Required system personnel are available to assist with the IAP process.

Depending on the type of test objective, CSD will gather results based on one or all of the following testing methods:

- Technical Review. Observe via hands-on execution, the system to verify security controls such as password complexity rules, warning banners, and password-protected screen savers.
- Interviews. Interview system/project personnel to identify information such as how passwords are distributed, what ports are required for the system/project to function, or how application logs are handled.
- Documentation Review. Examine system documentation such as rules of behavior, SSP, and contingency plans.

IAP Workflow Overview – Inputs, Actions & Deliverables

The workflow of IAP activities requires inputs from stakeholders. Without proper input, required actions and deliverables can be delayed, which will negatively impact the overall project timeline.

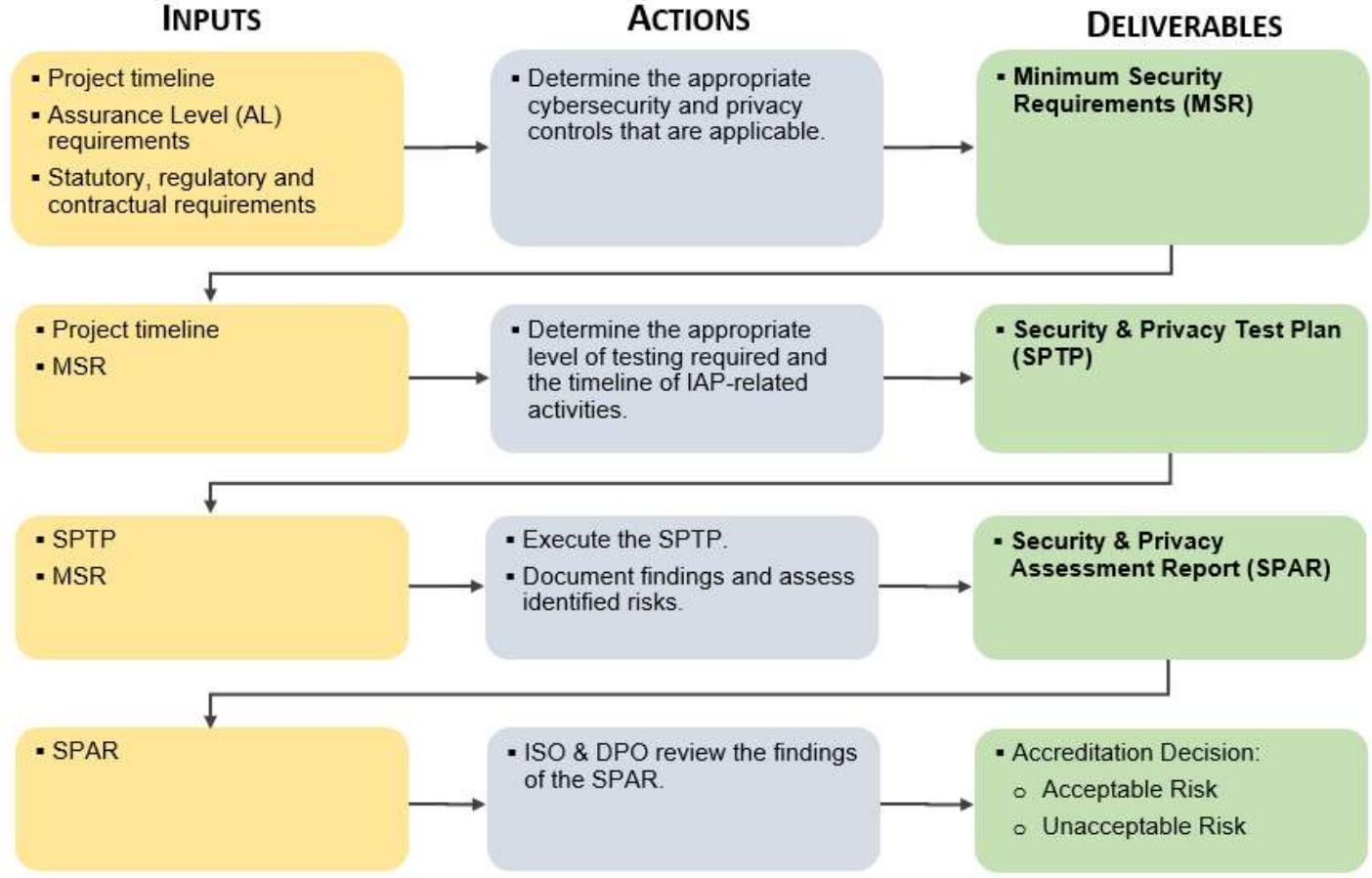


Figure 13: Workflow inputs and deliverable.

APPENDIX A - TASKS BY PHASE - PREPARE

The purpose of the Prepare phase is to carry out essential activities at the organization, mission and business process, and system levels of the enterprise to help prepare the organization to manage its security and privacy.

These tasks come directly from NIST Special Publication 800-37 revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.[14] The steps listed below represent "industry recognized best practices" for conducting activities associated with this phase.

NOTE: Tasks P-1 through P-7 are "organization level" tasks and are excluded from the scope of performing IAP activities at the system, application or service level.

P-8: MISSION OR BUSINESS FOCUS

Task: Identify the missions, business functions, and mission/business processes that the system is intended to support.

Expected Deliverable(s):

- List of business functions/processes that the system will directly or indirectly support

Task Guidance: ACME's mission and business functions influence the design and development of the processes that are created to carry out those missions and business functions. The prioritization of these functions drives investment strategies and funding decisions, and therefore, affects the development of the enterprise architecture and the associated security and privacy architectures. Information is elicited from stakeholders to acquire a more thorough understanding of the missions, business functions, and mission/business processes of the organization from a system security and privacy perspective

Potential Input(s):

- Organizational mission statement
- Organizational policies
- Mission/business process information
- System stakeholder information
- Cybersecurity Framework profiles

P-9: SYSTEM STAKEHOLDERS

Task: Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.

Expected Deliverable(s):

- List of system stakeholders

Task Guidance: Stakeholders include individuals, organizations, or representatives that have an interest in the system throughout the system life cycle—for design, development, implementation, delivery, operation, and sustainment of the system. It also includes all aspects of the supply chain. Stakeholders may reside in the same organization or they may reside in different organizations in situations when there is a common interest by those organizations in the system. Communication among stakeholders is important throughout the SDLC/PDLC to ensure that security and privacy requirements are satisfied, concerns and issues are addressed expeditiously, and risk management processes are carried out effectively

Potential Input(s):

- Organizational mission statement
- Mission or business objectives
- Missions, business functions, and mission/business processes that the system will support
- Other mission/business process information
- Organizational security and privacy policies and procedures
- Organizational charts

[14] NIST SP 800-37 rev2 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

APPENDIX F - TASKS BY PHASE - AUTHORIZE

The purpose of the Authorize phase is to provide organizational accountability by requiring a senior management official to determine if the security, privacy, and supply chain risk to organizational operations and assets, individuals or other organizations based on the operation of a system or the use of common controls, is acceptable.

These tasks come directly from NIST Special Publication 800-37 revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.[19] The steps listed below represent "industry recognized best practices" for conducting activities associated with this phase.

R-1: AUTHORIZATION PACKAGE

Task: Assemble the authorization package and submit the package to the authorizing official for an authorization decision.

Expected Deliverable(s):

- Authorization package (with an executive summary), which may be generated from a security or privacy management tool for submission to the authorizing official.

Task Guidance: The information in the authorization package is used by authorizing officials to make informed, risk-based decisions. Authorization packages include:

- security and privacy plans;
- Security and privacy assessment reports;
- POA&M; and
- An executive summary.

Additional information can be included in the authorization package at the request of the authorizing official. Organizations maintain version and change control as the information in the authorization package is updated. Providing timely updates to the plans, assessment reports, and a POA&M on an ongoing basis supports the concept of near real-time risk management and ongoing authorization, and can be used for reauthorization actions, if required.

When controls are implemented by an external provider through contracts, interagency agreements, lines of business arrangements, licensing agreements, or supply chain arrangements, the organization ensures that the information needed to make risk-based decisions is made available by the provider. The senior manager for privacy reviews the authorization package for systems that process personal data to ensure compliance with applicable privacy requirements and to manage privacy risks, prior to authorizing officials making risk determination and acceptance decisions.

The authorization package may be provided to the authorizing official in hard copy or electronically or may be generated using an automated security/privacy management and reporting tool. Organizations can use automated support tools in preparing and managing the content of the authorization package. Such tools provide an effective vehicle for maintaining and updating information for authorizing officials regarding the ongoing security and privacy posture of systems within the organization. When a system is under ongoing authorization, the authorization package is presented to the authorizing official via automated reports to provide information in the most efficient and timely manner possible. Information to be presented to the authorizing official in assessment reports is generated in the format and with the frequency determined by the organization using information from the cybersecurity and privacy continuous monitoring programs. The assessment reports presented to the authorizing official include information about implemented system-specific, hybrid, and common controls. The authorization documents are updated at an organization-defined frequency using automated or manual processes in accordance with the risk management objectives of the organization.

Potential Input(s):

- security and privacy plans; security and privacy assessment reports
- POA&M
- Supporting assessment evidence or other documentation, as required

R-2: RISK ANALYSIS & DETERMINATION

Task: Analyze and determine the risk from the operation or use of the system or the provision of common controls.

Expected Deliverable(s):

- Risk determination

[19] NIST SP 800-37 rev2 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

APPENDIX H – CYBERSECURITY & PRIVACY CONTROL SELECTION

ACME leverages the Secure Controls Framework (SCF)[21] as for its IAP controls, since it is the most scalable and efficient manner to organize cybersecurity and privacy controls. The SCF addresses over 100 statutory, regulatory and contractual frameworks, so it allows for an efficient method to organize multiple sets of requirements into a single checklist of controls for each system/application/service that undergoes IAP. This checklist of controls constitutes the Minimum Security Requirements (MSR).

The SCF is a free resource for businesses, so all stakeholders in the IAP process, including external parties, can download and use the SCF. This allows the IAP process to utilize consistent terminology and controls nomenclature.

The overall process to identify the appropriate cybersecurity and privacy controls for IAP follows these steps:

STEP 1: DOWNLOAD THE LATEST VERSION OF THE SECURE CONTROLS FRAMEWORK (SCF)

Download the latest version of the SCF from the following site: https://www.securecontrolsframework.com/download-scf

Note: The SCF will asked for log in credentials to download the SCF. If you do not already have a log in, you will need to create a free account on the website. There is no cost to download the SCF and the sign-up process only takes a few moments.

STEP 2: IDENTIFY ALL APPLICABLE REQUIREMENTS

In order to ensure the system/application/service is meeting its MSR, it is necessary to first identify all applicable statutory, regulatory and contractual obligations that must be addressed.

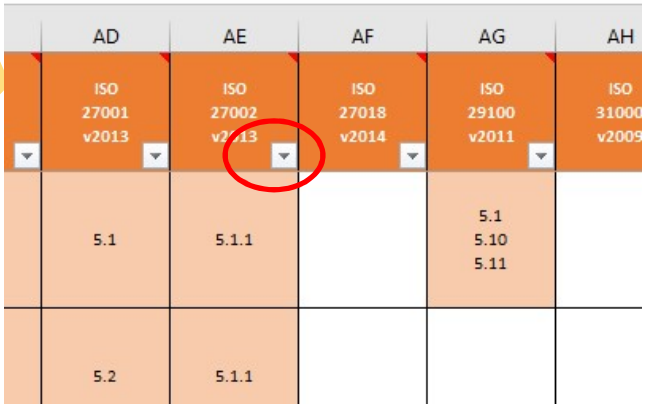
A. The Business Process Owner (BPO) is expected to maintain this list of requirements.
B. If the BPO does not have a complete listing, the following roles within ACME should be able to piece together what those applicable statutory, regulatory and contractual requirements will be:
    i. Legal department (should be able to identify privacy-related requirements)
    ii. Procurement department (should be able to identify contracts that call out unique cybersecurity and privacy requirements that need to be accounted for)
    iii. Cybersecurity department (should be able to identify "best practices" requirements, based on known requirements that guide the management of the cybersecurity program)

Note: It is the BPO's responsibility to identify, document and maintain compliance with all applicable statutory, regulatory and contractual obligations.

STEP 3: FILTER OUT NON-APPLICABLE REQUIREMENTS

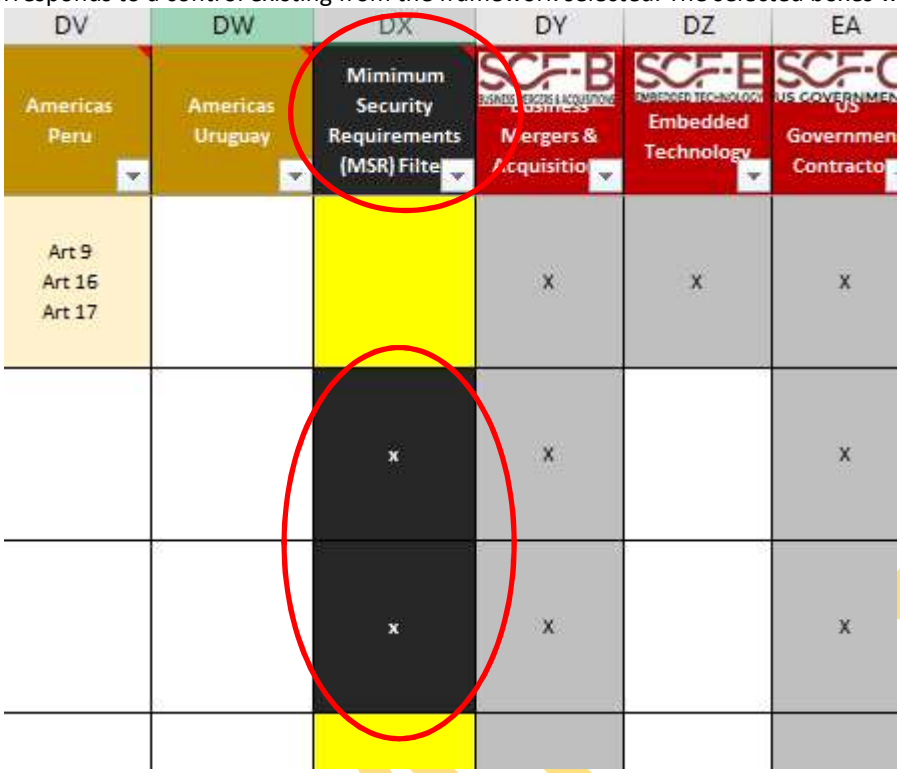
This step requires a basic understanding of using Microsoft Excel (or a compatible spreadsheet application).

A. From your previous work to identify applicable statutory, regulatory and contractual obligations, identify those columns within the Excel spreadsheet.
B. Select your first framework (e.g., ISO 27002) and use the filter function to only show those controls that apply to that framework.

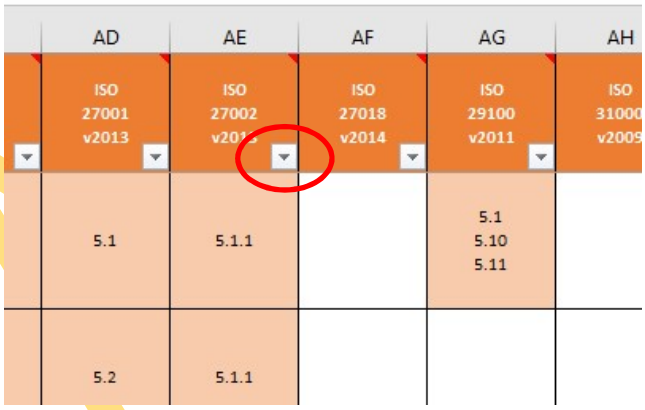


[21] Secure Controls Framework (SCF) – https://www.securecontrolsframework.com

C. In the column labelled "**Minimum Security Requirements (MSR) Filter**" place an "x" (or other character) in each of box in that column that corresponds to a control existing from the framework selected. The selected boxes will turn black.



D. Uncheck the filter on the first framework selected.



E.

F. Repeat steps B, C & D with each of the requirements. This will end up with the "CONTROL FILTER" column listing all of the applicable controls necessary to address the security of your system/application/service.

G. You can delete the controls that do not have an "x" in the "**Minimum Security Requirements (MSR) Filter**" column to help ensure consistency with the control set.

You now have a set of Minimum Security Requirements (MSR) for your system/application/service that are unique to your applicable statutory, regulatory and contractual requirements.

STEP 4: ASSIGN CONTROLS TO STAKEHOLDERS

From the previous step, you've identified your MSR. Now it is time to ensure each of the controls is properly assigned to the correct stakeholder. This involves a process of identifying the appropriate individual/team that is responsible for the execution of the specific controls (e.g., Network administrator is assigned all network-related controls).

Note: It is the BPO's responsibility to assign controls and oversee that the system/application/service is being properly maintained to be both secure and compliant.