SECURE CONTROLS FRAMEWORK

SCF CDPAS

CYBERSECURITY & DATA PROTECTION ASSESSMENT STANDARDS

Contributors:

Tom Cornelius
Andy Kuykendall
Robert E. Johnson, III
David Driggers
Kim Owen
Michael Brooks
Sully Perella
Peter Sternkopf
Sean Hermanny
Bill Corbitt
Cat Hammond
Derek Thomas
Adam German
Kirk Anderegg

Version 2024.1

This publication is available free of charge from: https://securecontrolsframework.com/content/cdpas.pdf

Table of Contents

FOREWORD

The Secure Control Framework Council (SCF Council) established a cohesive, consistent set of standards for performing cybersecurity and data protection-related Third Party Assessment, Attestation and Certification Services (3PAAC Services). By following the Cybersecurity & Data Protection Assessment Standards (CDPAS) approach, cybersecurity and data protection practitioners can improve the currently disjointed approach used to perform assessments of cybersecurity and/or data protection controls.

The CDPAS is a "standard" that normalizes third-party assessment practices. Per NIST, a standard is *"a document, established by consensus and approved by a recognized body, which provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context."* [1]

In compliance-related matters, it is important to note that words have specific meanings. The CDPAS focuses on third-party assessments, not internal or external audits. The terms "audit" and "assessment" are not interchangeable, since each has a unique meaning:

- Assessment: The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for an information system or organization.[2]
- Audit: The independent examination of records and activities to ensure compliance with established controls, policy and operational procedures and to recommend any indicated changes in controls, policy, or procedures.[3]

In addition to performing an assessment, 3PAAC Services embody the concepts of attestation and certification:

- Attestation: The issue of a statement, based on a decision, that fulfillment of specified requirements has been demonstrated.[4]
- Certification: The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness.[5]

As part of 3PAAC Services, a Third-Party Assessment Organization (3PAO) is expected to:

1. Conduct an assessment of applicable cybersecurity and/or data protection controls within an assessment boundary;
2. Provide an attestation based on the findings from the controls assessment in a Report on Conformity (ROC); and
3. Finalize the process by authorizing the issue of a certification, if sufficient conformity is achieved.

INTENDED AUDIENCE

The intended audience of the CDPAS is those parties encompassing the "assessment ecosystem," which includes:

- Organization Seeking Assessment (OSA);
- 3PAOs;
- Assessors; and
- External Service Providers (ESP):
  - Consultants;
  - Cloud Service Providers (CSP);
  - Managed Service Providers (MSP); and
  - Managed Security Services Providers (MSSP).

PURPOSE

The CDPAS exists to provide performance standards for cybersecurity and data protection-related 3PAAC Services.

[1] *NIST Glossary for Standard - https://csrc.nist.gov/glossary/term/standard*
[2] *NIST Glossary for Assessment - https://csrc.nist.gov/glossary/term/assessment*
[3] *NIST Glossary for Audit - https://csrc.nist.gov/glossary/term/audit*
[4] *NIST Glossary for Attestation - https://csrc.nist.gov/glossary/term/attestation*
[5] *NIST Glossary for Certification - https://csrc.nist.gov/glossary/term/certification*

INTENT

The CDPAS is not “one-size-fits-all.” Instead, the guidance throughout this document should be adopted and tailored to the unique size, resources and risk circumstances of each OSA and 3PAO.

The CDPAS can be modified, or augmented, with OSA-specific requirements, policies, or other compliance obligations due to statutory, regulatory and/or contractual requirements. This publication empowers OSAs to develop cybersecurity and data protection assessment strategies tailored to their specific mission, business needs, threats and operational environments.

PROHIBITIONS

The following usages of this content are strictly prohibited:

1. Use without proper attribution to the SCF Council;
2. Training Artificial Intelligence (AI) technologies; and/or
3. Use as part of an AI dataset or any other AI-related activities.

LIABILITY LIMITATIONS

THIS CONTENT IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE CONTENT OR THE USE OR OTHER DEALINGS IN THE CONTENT.

Submit comments on this publication to: comments@securecontrolsframework.com

TERMINOLOGY & ACRONYMS

The SCF Council recognizes two (2) primary sources for authoritative definitions for cybersecurity and data protection terminology:

1. The National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Cybersecurity Terms*, is the approved reference document used to define cybersecurity-related terminology;[6] and
2. NIST Glossary.[7]

From the context of applying a standard to 3PAAC Services, it is important to clarify mandatory versus optional criteria:[8]

- The terms "*SHALL*" and "*SHALL NOT*" indicate requirements:
  - To be followed strictly in order to conform; and
  - From which no deviation is permitted.
- The terms "*SHOULD*" and "*SHOULD NOT*" indicate that:
  - Among several possibilities one (1) is recommended as particularly suitable, without mentioning or excluding others;
  - A certain course of action is preferred, but not necessarily required; or
  - A certain possibility, or course of action, is discouraged, but not prohibited.
- The terms "MAY" and "NEED NOT" indicate a course of action permissible within reasonable limits.
- The terms "*CAN*" and "*CANNOT*" indicate:
  - A possibility and capability; or
  - The absence of that possibility or capability.

TERMINOLOGY STANDARDIZATION

Within the cybersecurity profession, the term "control" can be applied to a variety of contexts and can serve multiple purposes. When used in the CDPAS context, a control is a mechanism (e.g., a safeguard or countermeasure) designed to address protection needs specified by security requirements.

- Controls are:
  - The power to make decisions about how something is managed or how something is done;
  - The ability to direct the actions of someone or something;
  - An action, method or law that limits; and/or
  - A device or mechanism used to regulate or guide the operation of a machine, apparatus or system.
- Requirements are statements that translate, or express, a need and its associated constraints and conditions.

Additional clarification for assessment-relevant terminology:

- Assessment Boundary. The scope of an organization's control implementation to which assessment of objects is applied:
  - An assessment may involve multiple assessment boundaries; and
  - Assessment boundary may be defined as the People, Processes, Technologies, Data and/or Facilities (PPTDF) that comprise:
    - The entire organization;
    - A specific contract, project or initiative;
    - A specific Business Unit (BU) within an organization; or
    - A specific country, or geographic region, of the organization's business operations.
- Assessment Object. The item (e.g., specifications, mechanisms, activities, activities, individuals) upon which an assessment method is applied during an assessment.
- Conformity Assessment. A demonstration that specified requirements are fulfilled.
- Control Inheritance: Security control inheritance is a situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed,

[6] *NIST IR 7298 - https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf*
[7] *NIST Glossary - https://csrc.nist.gov/glossary*
[8] *NIST SP 800-63A - https://pages.nist.gov/800-63-3/sp800-63a.html*

authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. [9]

- Material Control. When a deficiency, or absence, of a specific control poses a material impact, that control is designated as a material control. See Appendix A: Material Controls for examples of material controls. A material control is such a fundamental cybersecurity and/or data protection control that:
  - It is not capable of having compensating controls; and
  - Its absence, or failure, exposes an organization to such a degree that it could have a material impact.
- Material Risk. When an identified risk that poses a material impact, that is a material risk.
  - A material risk is a quantitative or qualitative scenario where the exposure to danger, harm or loss has a material impact (e.g., significant financial impact, potential class action lawsuit, death related to product usage, etc.); and
  - A material risk should be identified and documented in an organization's "risk catalog" that chronicles the organization's relevant and plausible risks.
- Material Threat. When an identified threat poses a material impact, that is a material threat.
  - A material threat is a vector that causes damage or danger that has a material impact (e.g., poorly governed Artificial Intelligence (AI) initiatives, nation state hacking operations, dysfunctional internal management practices, etc.); and
  - A material threat should be identified and documented in an organization's "threat catalog" that chronicles the organization's relevant and plausible threats.
- Material Incident. When an incident poses a material impact, that is a material incident.
  - A material incident is an occurrence that does or has the potential to:
    - Jeopardize the Confidentiality, Integrity, Availability and/or Safety (CIAS) of a system, application, service or the data that it processes, stores and/or transmits with a material impact on the organization; and/or
    - Constitute a violation, or imminent threat of violation, of an organization's policies, standards, procedures or acceptable use practices that has a material impact (e.g., malware on sensitive and/or regulated systems, emergent AI actions, illegal conduct, business interruption, etc.).
  - Reasonably foreseeable material incidents should be documented in an organization's Incident Response Plan (IRP) that chronicles the organization's relevant and plausible incidents, so there are appropriate practices to identify, respond to and recover from such incidents.
- Material Weakness. A material weakness is a deficiency, or a combination of deficiencies, in an organization's cybersecurity and/or data protection controls (across its supply chain) where it is probable that reasonable threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance that the organization can adhere to its stated risk tolerance.
  - When there is an existing deficiency (e.g., control deficiency) that poses a material impact, that is a material weakness (e.g., inability to maintain access control, lack of situational awareness to enable the timely identification and response to incidents, etc.).
  - A material weakness will be identified as part of a gap assessment, audit or other form of assessment as a finding due to one (1), or more, control deficiencies. A material weakness should be documented in an organization's Plan of Action & Milestones (POA&M), risk register, or similar tracking mechanism for remediation purposes.
- Reciprocity. Reciprocity is an agreement among participating organizations to accept each other's: [10]
  - Security assessments to reuse system resources; and/or
  - Assessed security posture to share information.
- Risk. A risk is:
  - A situation where someone, or something valued, is exposed to danger, harm or loss (noun); or
  - To expose someone or something valued to danger, harm or loss (verb).
- Risk Appetite: The types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value. [11]
- Risk Tolerance: The level of risk an entity is willing to assume in order to achieve a desired result. [12]
- Risk Threshold: Values used to establish concrete decision points and operational control limits to trigger management

[9] *NIST Glossary for Security Control Inheritance - https://csrc.nist.gov/glossary/term/security_control_inheritance*
[10] *NIST Glossary for Reciprocity - https://csrc.nist.gov/glossary/term/reciprocity*
[11] *NIST Glossary for Risk Appetite - https://csrc.nist.gov/glossary/term/risk_appetite*
[12] *NIST Glossary for Risk Tolerance - https://csrc.nist.gov/glossary/term/risk_tolerance*

action and response escalation.[13]

- Threat. A threat:
  - Is a person, or thing, likely to cause damage or danger (noun); or
  - Indicates impending damage or danger (verb).

ACRONYMS

The following acronyms are used throughout the CDPAS:

Acronym	Term	Definition
1PD	First Party Declaration	1PDs are self-attestations (e.g., internal assessments).
3PA	Third-Party Attestation	3PA are attestations made by an independent third-party, generally in the performance of an assessment or audit.
3PAAC	Third-Party Assessment, Attestation and Certification Services	Assessment, attestation and certification services performed by a third-party organization.
3PAO	Third-Party Assessment Organization	A company that performs assessment, attestation and certification services.
AAT	Artificial Intelligence and Autonomous Technologies	Tools that are advanced enough to act with limited human involvement through Artificial Intelligence (AI), Machine Learning (ML) or similar autonomous technologies.
AO	Assessment Objective	AOs are objective statements that establish the desired outcome for the assessment for a specific control. There may be multiple AOs associated with a control.
APIT	Automated Point In Time	APIT assessments utilize automation to augment a traditional assessment methodology, where AAT is used to compare the desired state of conformity versus the current state via machine-readable configurations and/or assessment evidence: ▪ Relevant to a specific point in time (time at which the control was evaluated); ▪ In situations where technology cannot evaluate evidence, evidence is manually reviewed; and ▪ The combined output of automated and manual reviews of artifacts is used to derive a finding.
ATE	Assessment Technical Expert	ATE are assessment team members who have the necessary subject matters expertise to conduct a specific part of an assessment. ATE report to the ATL.
ATL	Assessment Team Lead	An ATL is an individual assigned by the 3PAO to lead its assessment team in the conduct of 3PAAC Services.
AEHR	Automated Evidence with Human Assessment	AEHR assessments are used for ongoing, continuous control assessments: ▪ AAT continuously evaluates controls by comparing the desired state of conformity versus the current state through machine-readable configurations and/or assessment evidence; and ▪ Recurring human reviews: ○ Evaluate the legitimacy of the results from automated control assessments; and ○ Validate the automated evidence review process to derive a finding.
CIAS	Confidentiality, Integrity, Availability and/or Safety	CIAS is an evolution of the "CIA Triad" concept that defines the purpose of security controls. It adds the component of Safety.
COI	Conflict of Interest	COI involves situations in which a personal interest, or relationship, conflicts with the faithful performance of an official duty.
CPE	Continuing Professional Education	CPE describes the ongoing process of improving skills and competencies through formal or informal educational activities.

[13] *NIST Glossary for Thresholds - https://csrc.nist.gov/glossary/term/thresholds*

DSR	Discretionary Security Requirements	DSR are discretionary cybersecurity and/or data protection controls that address voluntary industry practices or internal requirements. DSR are primarily internally influenced, based on the organization's respective industry and risk tolerance.
ERL	Evidence Request List	ERLs establish a finite list of supporting evidence used in an assessment: ▪ Prior to the start of the assessment, an ERL is provided by the 3PAO to the OSA. ▪ The ERL's standardized evidence expectations allow OSAs to have sufficient time to accumulate reasonable evidence to determine the adequacy of control design and operation.
ESP	External Service Provider	An independent, third-party organization that provides services, technologies, facilities and/or people. ESPs include but are not limited to: ▪ Consulting / professional services; ▪ Software development; ▪ Staff augmentation; and ▪ Technology support (e.g., Managed Services Provider (MSP)).
MCR	Minimum Compliance Requirements	MCR are minimum requirements that must be addressed to comply with applicable laws, regulations and contracts. MCR are primarily externally-influenced, based on industry, government, state and local regulations.
MPIT	Manual Point In Time	MPIT assessments are a traditional assessment methodology: ▪ Relevant to a specific point in time (time at which the control was evaluated); and ▪ Relies on the manual review of artifacts to derive a finding.
MLC	Maturity Level Criteria	MLC are specific to each maturity level to define reasonable staffing, technologies and processes to implement the desired level of maturity.
MSA	Master Services Agreement	MSAs are comprehensive contracts between two parties that establish terms and conditions of current and future transactions.
OSA	Organization Seeking Assessment	A company, entity or business unit seeking the external assessment.
PbD	Privacy by Design	Data privacy through the design and governance of processes and technologies. PbD prioritizes data protection as a core business requirement, rather than a technical feature.
RASCI	Responsible, Accountable, Supportive, Consulted & Informed	Refers to a RASCI matrix that defines responsibilities associated with individuals or teams: ▪ Responsible - entity directly responsible for performing a task (e.g., control/process operator); ▪ Accountable - entity overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ Supportive - entity(ies) under the coordination of the Responsible person for support in performing the task; ▪ Consulted - entity(ies) not directly involved in task execution but were consulted for subject matter expertise; and ▪ Informed - entity(ies) not involved in task execution but are informed when the task is completed.
ROC	Report on Conformity	A formalized report that issues an assessment conformity designation. The ROC summarizes the assessment findings and justification for the conformity designation.
SbD	Secure by Design	Processes and technologies are designed and built in a way that protects against reasonable threats. SbD prioritizes cybersecurity as a core business requirement, rather than treating it as a technical feature.
SOW	Statement of Work	SOWs are contracts that cover the work management aspects of a project (e.g., scope, timeline, cost, responsibilities, etc.).

CYBERSECURITY & DATA PROTECTION ASSESSMENT STANDARDS (CDPAS)

STANDARD 1: PROFESSIONAL DUTY OF CARE

Assessors must exercise due diligence and due care by using their skills and knowledge to reach informed, objective decisions when conducting Third-Party Assessment, Attestation & Certification Services (3PAAC Services).

Justification: Assessors and Third-Party Assessment Organizations (3PAOs) operate in a position of trust and authority. Therefore, assessors and 3PAOs must exercise due diligence and due care in the conduct of their business interactions and representation of professionalism in business interactions.

Guidance: There is a professional obligation for cybersecurity and/or data privacy practitioners to provide reasonable services and skills to their clients. 3PAOs and assessors are expected to be familiar with the industry norms associated with client 3PAAC Service engagements, due to the specialized knowledge that may be required as part of the assessment.

STANDARD 1.1: ETHICAL CONDUCT

Assessors must:

1. Act ethically, professionally and legally towards clients, employers, colleagues and society; and
2. Adhere to ethical principles and values in personal and professional endeavors, specifically being honest, forthright and trustworthy.

Justification: Assessors operate from a position of trust and authority. Therefore, assessors are expected to conduct themselves professionally. Unprofessional conduct can harm the 3PAO and the Organization Seeking Assessment (OSA).

Guidance: Organizations providing 3PAAC Services are reasonably expected to have formalized standards of conduct (e.g., rules of behavior) that their employees and contractors are contractually obligated to adhere to. Those documented standards of conduct can help define an assessor's formal role and responsibilities. Violations of those standards of conduct are expected to be addressed through Human Resources (HR)-related enforcement mechanisms that includes personnel sanctions. HR enforcement actions are expected to reflect the severity of the conduct violation.

STANDARD 1.2: INDEPENDENCE

Assessors must maintain objectivity and be free to exercise professional judgment.

Justification: Assessors operate from a position of trust and authority. Therefore, assessors must operate independently and exercise professional judgment without bias or influence. Without assessor independence:

- *The integrity of the assessment should be considered compromised; and*
- *Any final report or related observations should be dismissed as untrustworthy, requiring a re-assessment by a different 3PAO.*

Guidance: Ensuring assessor independence may be achieved through:

- *Avoiding Conflicts of Interest (COI);*
- *Sound hiring practices; and*
- *Top-down evaluations to uncover dysfunctional management practices.*

STANDARD 1.3: SUBJECT MATTER COMPETENCY

Assessors must:

1. Have documented evidence of relevant job experience and relevant training to demonstrate proficiency in performing assessment duties; and
2. Annually, complete at least twenty (20) hours of Continuing Professional Education (CPE) training in topics relevant to the skills and situational awareness necessary to be an effective assessor.

Justification: It is reasonable to expect an assessor to be a demonstrable Subject Matter Expert (SME) in cybersecurity and/or data protection practices. Being able to demonstrate this will be through relevant, ongoing skill development:

- *Industry-recognized cybersecurity and/or data privacy certifications;*
- *Industry involvement (e.g., conference panels); and*
- *Other training opportunities (e.g., online or in-person training events).*

Guidance: It is possible to complete the annual CPE requirements concurrently with other professional certifications. While it is impossible to have expertise in every highly technical subcategory of the cybersecurity profession, it is reasonable to expect that an assessment team will bring in Assessment Technical Experts (ATE), with subject matters expertise to conduct their specific part of an assessment, as necessary. 3PAOs should leverage NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, for guidance on specialized technical assessments, including:[14]

- *Application security testing and examination; and*
- *Remote access testing.*

The US Department of Defense Manual (DODM) 8140.03, Cybersecurity Workforce Qualification and Management Program, contains a listing of industry certifications, based on position category and seniority for the role of a Secure Control Assessor.[15]

- *Entry-level assessor;*
- *Intermediate-level assessor; and*
- *Senior-level assessor.*

In addition to practical, hands-on experience, this DODM guidance should be used by 3PAOs to establish a baseline level of subject matter competency necessary to perform 3PAAC Services:

- *Entry and intermediate-level assessor:*
  - *An undergraduate (Bachelor of Science) degree fulfills the educational requirement if it is:*
    - *From an:*
      - *Accreditation Board for Engineering and Technology (ABET) accredited; or*
      - *Centers of Academic Excellence (CAE) designated institution*
    - *In the one of the following degrees:*
      - *Information Technology (IT)*
      - *Cybersecurity;*
      - *Data Science;*
      - *Information Systems; or*
      - *Computer Science (CS);*

  and/or

  - *One (1) of the following certifications:*
    - *CGRC/CAP - ISACA Certified in Governance, Risk, and Compliance (formerly known as CAP);*
    - *GSEC - GIAC Security Essentials Certification;*
    - *CASP+ - CompTIA Advanced Security Practitioner plus;*
    - *Cloud+ - CompTIA Cloud plus;*
    - *PenTest+ - CompTIA Penetration Tester plus; and/or*
    - *Security+ - CompTIA Security plus.*
- *Senior-level assessor:*
  - *An undergraduate degree fulfills the educational requirement if it is:*
    - *From an:*
      - *Accreditation Board for Engineering and Technology (ABET) accredited; or*
      - *Centers of Academic Excellence (CAE) designated institution*
    - *In the one of the following degrees:*
      - *Information Technology (IT)*
      - *Cybersecurity;*
      - *Data Science;*
      - *Information Systems; or*
      - *Computer Science (CS);*

  and/or

  - *One (1) of the following certifications:*

[14] *NIST SP 800-115 - https://csrc.nist.gov/pubs/sp/800/115/final*
[15] *DoDM 8140.03 - https://dodcio.defense.gov/Portals/0/Documents/Library/DoDM-8140-03.pdf*

- *CISM - ISACA Certified Information Security Manager;*
- *CISA - ISACA Certified Information Systems Auditor;*
- *CISSP - ISC2 Certified Information Systems Security Professional;*
- *CISSP-ISSEP - ISC2 CISSP - Information Systems Security Engineering Professional;*
- *GCSA - GIAC Cloud Security Automation;*
- *GSLC - GIAC Security Leadership Certification;*
- *GSNA - GIAC Systems and Network Auditor;*
- *CySA+ - CompTIA Cybersecurity Analyst plus;*
- *C)ISSO - Certified Information Systems Security Officer;*
- *C)PTE - Certified Penetration Testing Engineer; and/or*
- *FITSP-A - Federal IT Security Professional-Auditor.*

STANDARD 1.4: CONFLICT OF INTEREST (COI) AVOIDANCE

Assessors must avoid actual and/or perceived COI. COI includes involvement in the design, or implementation, of any of the OSA's cybersecurity and/or data protection controls, which are reasonably expected, or intended, to be included in the scope of the assessment:

1. An assessor is prohibited from conducting 3PAAC Services if the assessor made a material impact on the OSA's cybersecurity and data protection program; and
2. Materiality impact is defined as:
    a. Material Impact - Within the past five (5) years, the assessor made a significant impact on the OSA's cybersecurity and/or data protection program, where the assessor performed a broad scope of work with a strategic and/or operational impact on the OSA's cybersecurity and/or data protection controls; and
    b. Non-Material Impact - Within the past two (2) years, the assessor made no greater than a minor impact on the OSA's cybersecurity and/or data protection program, where the assessor performed a limited scope of work with minimal impact on tactical-focused cybersecurity and/or data protection controls.

Justification: Assessors operate from a position of trust and authority. Therefore, the integrity of an assessor must be sufficiently independent of the OSA and maintain the ability to conclude on the design and operational quality of the controls assessed without bias from prior knowledge of the OSA's cybersecurity and privacy control structure. An actual or perceived COI devalues an assessor's integrity. In a worst-case scenario, when there is an actual COI, the assessment results could be considered fraud if the assessor benefits from the activity.

Guidance: Avoiding COI may be achieved through:

- *Being aware of what constitutes a material and non-material impact; and*
- *Due diligence practices for assessment team participation reviews.*

STANDARD 2: SECURE PRACTICES

3PAOs must identify potential assessment-related threats and implement ways to minimize and/or mitigate those associated risks.

Justification: Assessors and 3PAOs must be capable of protecting data at a level equivalent to the assessed environment. This requires the assessors and 3PAOs to proactively identify relevant threats and implement appropriate cybersecurity and/or data protection controls to minimize risk to the 3PAO and OSA.

Guidance: The 3PAO is expected to define and implement pertinent cybersecurity and/or data protection controls required by applicable laws, regulations, contractual obligations and industry norms.

STANDARD 2.1: SECURITY & PRIVACY BY DESIGN

3PAOs must implement Secure by Design (SbD) and Privacy by Design (PbD) principles for governing:

1. Administrative processes;
2. Technology selection and architectural decisions;
3. Physical security practices; and

4. The protection of sensitive and/or regulated data throughout the information lifecycle.

Justification: Cybersecurity and data protection practices need to be "baked in" as compared to "bolted on" a 3PAO's day-to-day practices. This is the concept of cybersecurity and data protection practices being consciously "designed and implemented" to ensure secure and compliant practices are operationalized across system and information lifecycles.

Guidance: The Secure Controls Framework (SCF) has Cybersecurity & Data Privacy by Design (C|P) Principles that 3PAOs can leverage.[16] The term "sensitive data" includes, but is not limited to:

- *Personal Data (PD):*
  - *Full name;*
  - *Date of birth;*
  - *Email address;*
  - *Phone number;*
  - *IP address;*
  - *Place of birth; and*
  - *Employment information.*
  - *Non-precise geographical data (e.g., ZIP code, city, state, country, etc.).*
- *Sensitive Personal Data (sPD):*
  - *Government-issued ID information (e.g., driver's license, passport, Social Security number (SSN), etc.);*
  - *Information that allows account access:*
    - *Account log-in, financial account, debit card or credit card number in combination with:*
    - *Any required security or access code, password or credentials allowing access.*
  - *Precise geolocation data;*
  - *Race or ethnicity;*
  - *Citizenship or immigration status;*
  - *Religious or philosophical beliefs;*
  - *Trade union membership;*
  - *Genetic data;*
  - *Biometric data;*
  - *Health-related data;*
  - *Data concerning a person's sex life or sexual orientation;*
  - *Contents of a data subject's communications (e.g., email and/or text messages) unless the data processor is the intended recipient of the communication;*
  - *Attorney-Client Privilege Information (ACPI); and*
  - *Cardholder Data (CHD).*
- *Intellectual Property (IP):*
  - *Patents;*
  - *Trade secrets;*
  - *Trademarks; and*
  - *Copyrights.*
- *Regulated data:*
  - *Controlled Unclassified Information (CUI);*
  - *Federal Contract Information (FCI);*
  - *Export-Controlled Data (ITAR / EAR);*
  - *Protected Health Information (PHI);*
  - *Student Educational Records (FERPA); and*
  - *Critical Infrastructure Information (CII).*

STANDARD 2.2: STATEMENT OF WORK (SOW)

3PAOs must formalize an agreement detailing the scope, nature and extent of the assessment that includes the following:

1. The type of assessment to be performed, inclusive of control testing procedures;
2. The assessment boundary;
3. The timeline for completing each stage of work, inclusive of review and report finalization details; and

[16] *SCF C|P Principles - https://securecontrolsframework.com/domains-principles/*

4. Where remediation and reassessment are necessary, the reassessment stage.

Justification: A formal contract is reasonably expected to detail the nature of the work and milestones.

Guidance: 3PAOs are expected to have formal onboarding processes for an OSA. This may include multiple types of agreements, in addition to a SOW:

- *Master Services Agreement (MSA);*
- *Non-Disclosure Agreements (NDAs); and*
- *Change Orders.*

STANDARD 2.3: ASSESSMENT-SPECIFIC DATA PROTECTION IMPACT ASSESSMENT (DPIA)

3PAOs must perform a Data Protection Impact Assessment (DPIA) to cover the types of sensitive and/or regulated data that is reasonably expected to be stored, processed and/or transmitted throughout the lifecycle of the assessment.

Justification: A DPIA is designed to systematically analyze, identify and mitigate data protection risks associated with a project or initiative. A DPIA:

- *Can be used for more than data protection considerations; and*
- *Applies to multiple types of sensitive and/or regulated data.*

Guidance: Assessments should be considered discrete projects with unique data protection requirements. To understand data handling requirements, a DPIA should be performed prior to initiating any 3PAAC Services.

STANDARD 2.4: INTELLECTUAL PROPERTY (IP) PROTECTIONS

3PAOs must take all reasonable precautions to protect the confidentiality of all OSA Intellectual Property (IP) the assessment team is exposed to during the assessment lifecycle.

Justification: Assessors and 3PAOs operate from a position of trust and authority. Therefore, assessors and 3PAOs are expected to protect IP with all reasonable technical, administrative and physical controls necessary.

Guidance: The 3PAO should implement a process to identify IP types that the assessment team will reasonably be exposed to. Ideally, specific systems/applications/networks containing sensitive information should be documented for awareness by the assessment team.

STANDARD 2.5: PROTECTION OF ASSESSMENT INFORMATION

3PAOs must implement reasonable technical, administrative and physical controls to protect the confidentiality, integrity and availability of assessment information throughout the lifecycle of the assessment.

Justification: Assessors and 3PAOs operate from a position of trust and authority. Therefore, assessors and 3PAOs are expected to protect assessment-related data with all reasonable technical, administrative and physical controls necessary for the entire lifecycle of the assessment data.

Guidance: The 3PAO is expected to govern its cybersecurity and/or data protection controls to protect assessment-related information. At a minimum, these reasonable controls should adhere to the applicable laws, regulations, contractual obligations and industry norms for cybersecurity and data protection protections.

3PAOs should leverage NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, for guidance on security assessment related:[17]

- *Data handling:*
  - *Data collection;*
  - *Data storage;*
  - *Data transmission; and*

[17] *NIST SP 800-115 - https://csrc.nist.gov/pubs/sp/800/115/final*

- *Data destruction; and*
- *Post-testing activities:*
  - *Mitigating recommendations;*
  - *Reporting; and*
  - *Remediation/mitigation.*

STANDARD 2.6: USE OF ASSESSMENT INFORMATION

3PAOs are prohibited from using information obtained during an assessment for any purpose not:

1. Explicitly authorized by the OSA; and
2. Included in the MSA or SOW.

Justification: Assessors and 3PAOs operate from a position of trust and authority. Therefore, assessors and 3PAOs are expected to use the collected information only for the assessment's stated purpose(s).

Guidance: The MSA/SOW and DPIA should clearly define permissible uses of assessment information, including any limitations on data sharing and requirements for data anonymization. Explicit clauses should prohibit using data for purposes outside the agreed scope.

STANDARD 2.7: DISPOSAL OF ASSESSMENT INFORMATION

3PAOs must:

1. Satisfy statutory, regulatory and/or contractual obligations for data retention;
2. Adhere to a formal data retention schedule; and
3. Securely dispose of assessment information, once the minimum retention period is achieved.

Justification: 3PAOs operate from a position of trust and authority. Therefore, 3PAOs are expected to securely dispose of assessment-related data once the data retention period is met, as agreed to in the SOW and/or MSA.

Guidance: For assessments not involving sensitive and/or regulated data, or an OSA with specific retention requirements, it is reasonable for a 3PAO to maintain an OSA's assessment data for no less than three (3) years. For regulated OSAs, suggestions are as follows:

- *Health Insurance Portability and Accountability Act (HIPAA) requires Covered Entities (CEs) and Business Associates (BAs) to retain certain documents for a minimum of six (6) years;*
- *Accounting and assessment firms generally follow the Institute of Internal Auditors (IIA) and US-based tax authority guidance of seven (7) years; and*
- *The proposed rule for Cybersecurity Maturity Model Certification (CMMC) requires CMMC Third-Party Assessment Organizations (C3PAOs) to retain assessment-related information for a minimum of ten (10) years.*

Based on the DPIA and contractual obligations as part of the assessment, the 3PAO may have unique retention requirements for assessment findings. Each assessment must have a discrete and secure storage location, with the capability to manually, or automatically, purge assessment information once the data retention period is met.

STANDARD 3: DUE DILIGENCE - OSAS

OSA must:

1. Identify, document and remediate risks in accordance with the OSA's documented risk management practices;
2. Perform due diligence activities in preparation for an assessment;
3. Document these activities as part of the OSA's assessment planning process; and
4. Demonstrate evidence of assessment readiness to a 3PAO for 3PAAC Services.

Justification: The OSA has a fiduciary duty to its shareholders. Being unprepared to engage with a 3PAO for 3PAAC Services is fiscally irresponsible, since 3PAAC Services are costly and the likelihood of a successful assessment without evidence of due diligence is remote.

Guidance: OSAs can use ISO 27005[18] or NIST SP 800-37[19] for guidance on implementing and maintaining its risk management practices.

OSAs should treat assessments as discrete projects. This proper resourcing and governance can help an OSA perform and document due diligence activities.

The NIST Risk Management Framework (RMF) defines the lifecycle of cybersecurity & data protection controls.[20] The RMF consists of seven (7) unique phases that covers the lifecycle of controls governance:

1. *Prepare. Essential activities to prepare the OSA to manage cybersecurity and privacy risks;*
2. *Categorize. Categorize systems, applications, services and data based on an impact analysis;*
3. *Select. Select appropriate cybersecurity and data protection controls to protect* PPTDF *based on risk assessments;*
4. *Implement. Implement the cybersecurity and data protection controls and document how those controls are deployed;*
5. *Assess. Assess to determine if the cybersecurity and data protection controls are in place, operating as intended, and producing the desired results;*
6. *Authorize. A senior OSA official (e.g., manager, director, officer, etc.) makes a risk-based decision to authorize the system, application, service or project to operate in a production environment; and*
7. *Monitor. Continuously monitor:*
    a. *Cybersecurity and data protection control implementation; and*
    b. *Evolving risks and threats.*

In the context of 3PAAC Services, OSAs should expect a 3PAO to ask reasonable questions pertaining to the following governance topics:

- *How the OSA's performs due diligence and due care activities for cybersecurity and data protection obligations;*
- *How the OSA's systems/processes/services/data are categorized;*
- *The reasoning for the OSA's cybersecurity & data protection controls that were selected;*
- *How the OSA's cybersecurity & data protection controls were implemented;*
- *The method the OSA used to assess cybersecurity & data protection controls, prior to systems/services/applications going into production; and*
- *The OSA's ongoing monitoring practices to determine:*
    - *Cybersecurity & data protection control effectiveness; and*
    - *Awareness of evolving risks and threats.*

STANDARD 3.1: ADHERENCE TO DATA PROTECTION REQUIREMENTS

OSA must adhere to all applicable statutory, regulatory and/or contractual obligations to protect sensitive and/or regulated data during 3PAAC Services.

Justification: Providing access to specific systems, applications, services and/or data may not be authorized, due to existing data protection practice requirements (e.g., privacy notice, data sharing agreements, etc.).

Guidance: OSAs should perform a DPIA to identify the types of data processed and their sensitivity levels and help systematically identify, analyze and mitigate data protection risks associated with 3PAAC Services. The DPIA should be performed before initiating any 3PAAC Services to understand potential limitations on assessor access to systems, applications, services and/or data.

STANDARD 3.2: ASSESSMENT BOUNDARY DEMARCATION

OSAs must:

1. Establish the scope of the assessment by defining the assessment boundary demarcation as:
    a. Organization-wide;
    b. A specific contract, project or initiative;
    c. A specific Business Unit (BU) within an organization; or

[18] *ISO 27005 - https://www.iso.org/standard/80585.html*
[19] *NIST SP 800-37 - https://csrc.nist.gov/pubs/sp/800/37/r2/final*
[20] *NIST RMF - https://csrc.nist.gov/projects/risk-management/about-rmf*

d. A specific country, or geographic region, of the organization's business operations; and

2. If applicable, identify relevant third-parties that make up the assessment boundary.

Justification: The OSA is ultimately responsible for conducting the due diligence to define the assessment boundary demarcation. This fundamental step influences the SOW for 3PAAC Services.

Guidance: To define the demarcation of the assessment boundary:

- *For an organization-wide scope, it is defined by a discrete:*
  - *Taxpayer Identification Number (TIN);*
  - *Employer Identification Number (EIN);*
  - *Value Added Tax (VAT);*
  - *Dun & Bradstreet Data Universal Numbering System (DUNS); or*
  - *If applicable, a Commercial And Government Entity (CAGE) Code.*
- *For a contract, project, product or initiative, it is defined by:*
  - *Sufficient detail to describe the scope of the assessment boundary:*
    - *People;*
    - *Processes;*
    - *Technologies;*
    - *Data; and*
    - *Facilities;*
  - *Contract number and/or the name of the project or initiative; and*
  - *If applicable, a CAGE Code that is associated with the contract.*
- *For a BU, country or geographic region, it is defined by:*
  - *Sufficient detail to describe the scope of the assessment boundary:*
    - *People;*
    - *Processes;*
    - *Technologies;*
    - *Data; and*
    - *Facilities;*
  - *OSA-designated name for the BU, country(ies) or geographic region; and*
  - *If applicable, a CAGE Code that is associated with the BU.*

STANDARD 3.3: GRAPHICAL REPRESENTATION OF ASSESSMENT BOUNDARY

OSAs must generate a graphical representation of the assessment boundary to ensure control applicability is appropriately determined for systems, applications, services and third-parties that:

1. Reflects the current architecture of the network environment(s);
2. Clearly represents network access points on the perimeter of the network(s);
3. Documents all sensitive and/or regulated data flows; and
4. Contains sufficient detail to assess the applicable cybersecurity and/or data protection controls.

Justification: Graphically representing the assessment boundary helps:

- *Prevent miscommunication among stakeholders by providing a clear visual delineation of which systems, data and processes are included within the scope; and*
- *Ensure comprehensive coverage by reducing errors in scoping and including all relevant elements during the assessment.*

Guidance: A graphical representation of the assessment boundary can be in the form of a network diagram.

STANDARD 3.4: STAKEHOLDER IDENTIFICATION

OSAs must clearly define applicable internal and third-party assessment stakeholders.

Justification: Identifying the applicable internal and external stakeholders is crucial to any assessment-related due diligence. Developing a trust relationship with key stakeholders is also essential for a successful assessment.

Guidance: Stakeholder identification can be achieved through documenting a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix:

- *Responsible - entity directly responsible for performing a task (e.g., control/process operator);*
- *Accountable - entity overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner);*
- *Supportive - entity(ies) under the coordination of the Responsible person for support in performing the task;*
- *Consulted - entity(ies) not directly involved in task execution but were consulted for subject matter expertise; and*
- *Informed - entity(ies) not involved in task execution but are informed when the task is completed.*

STANDARD 3.5: CONTROL RECIPROCITY

For control reciprocity:

1. The sole authority to determine control reciprocity is the:
    a. Certification scheme owner; or
    b. Applicable Accreditation Body (AB); and
2. If a control reciprocity exists:
    a. OSAs must identify the specific controls it seeks reciprocity for; and
    b. Applicable controls identified for reciprocity must share the same assessment boundary(ies).

Justification: Control reciprocity decisions involve an analysis to determine applicability, which is solely up to the discretion of an authoritative body to make the determination. OSA, assessor and/or 3PAO opinions do not matter in control reciprocity decisions, since they are non-authoritative.

Guidance: For properly scoped and applicable controls, 3PAOs are required to accept the reciprocity decision from the authoritative body.

Control reciprocity decisions are rarely straightforward, due to the nature of crosswalk mapping between different frameworks. Clarification should be sought from the relevant authoritative body for answers to specific reciprocity questions.

Example 1: Cybersecurity Maturity Model Certification (CMMC)

- *An OSA with a current and valid CMMC Level 2 certification would be able to demonstrate conformity with:*
    - *Controlled Unclassified Information (CUI) controls in NIST SP 800-171 R2; and*
    - *Federal Contract Information (FCI) controls in FAR 52.204-21 and NIST SP 800-171 R2.*
- *While the OSA would be able to demonstrate compliance with CUI and FCI controls, it would not be able to demonstrate conformity with broader compliance obligations for:*
    - *DFARS 252.204-7012 (e.g., incident reporting requirements); and/or*
    - *Non-Federal Organization (NFO) controls from NIST SP 800-171 R2.*

Example 2: FedRAMP

- *A current and valid FedRAMP certification would allow an OSA to demonstrate conformity with applicable NIST SP 800-53 in the FedRAMP Cloud Service Provider (CSP) environment.*
- *The OSA would not be able to use that same FedRAMP certification to demonstrate conformity with applicable NIST SP 800-53 controls outside of the FedRAMP CSP environment.*

Example 3: ISO/IEC 27001

- *A current and valid ISO/IEC 27001:2022 certification would allow an OSA to demonstrate conformity with applicable ISO/IEC 27001:2022 controls within the scope of the ISO/IEC 27001:2022 certification.*
- *The OSA would not be able to use that same ISO/IEC 27001:2022 certification to demonstrate conformity with controls outside of the scope of the ISO/IEC 27001:2022 certification.*

STANDARD 3.6: CONTROL INHERITANCE

To claim control inheritance:

1. From the External Services Provider (ESP) the OSA is seeking control inheritance, OSAs must obtain evidence in the form of a:
    a. First-Party Declaration (1PD); or
    b. Third-Party Attestation (3PA);
2. OSAs must identify the specific controls it seeks control inheritance for;
3. Applicable controls identified for control inheritance must share the same assessment boundary(ies); and
4. The ESP's service(s) claiming control inheritance must be documented in:
    a. A contract between the OSA and ESP; and
    b. A RASCI matrix, or similar form of customer responsibility matrix, that clearly identifies applicable roles and responsibilities associated with inherited controls.

Justification: It is reasonable to assume that OSAs will have external support and/or services, which requires the evaluation of inherited controls.

Guidance: It is at the 3PAO's discretion to perform limited or in-depth control testing to validate control inheritance.

Example 1: Service Organization Control (SOC) 2 Type 2

- *An OSA could leverage an ESP's Service Organization Control (SOC) 2 Type 2 report to address physical security of data center assets.*
- *The OSA would not be able to leverage that same SOC 2 Type 2 report for the OSA's on-premises physical security.*

Example 2: Cybersecurity Maturity Model Certification (CMMC)

- *An OSA with a current and valid CMMC Level 2 certification would be able to demonstrate conformity with:*
    - *Controlled Unclassified Information (CUI) controls in NIST SP 800-171 R2; and*
    - *Federal Contract Information (FCI) controls in FAR 52.204-21 and NIST SP 800-171 R2.*
- *While the OSA would be able to demonstrate compliance with CUI and FCI controls, it would not be able to demonstrate conformity with broader compliance obligations for:*
    - *DFARS 252.204-7012 (e.g., incident reporting requirements); and/or*
    - *Non-Federal Organization (NFO) controls from NIST SP 800-171 R2.*

STANDARD 3.7: DEFINED CYBERSECURITY AND/OR DATA PRIVACY CONTROLS

OSAs must define applicable cybersecurity and/or data protection controls for the assessment.

Justification: The OSA is ultimately responsible for conducting the due diligence to define the applicable cybersecurity and/or data protection controls for the assessment. This fundamental step influences SOW for 3PAAC Services.

Guidance: The SCF's Integrated Controls Management (ICM) Model provides guidance on how to properly define applicable controls.[21] The ICM focuses on the need to understand and clarify the difference between "compliant" versus "secure" since the distinction is necessary to have coherent risk management discussions. To assist in this process, an organization's applicable controls are categorized according to "must have" vs "nice to have" requirements:

- *Minimum Compliance Requirements (MCR) are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts. MCR are primarily externally-influenced, based on industry, government, state and local regulations. MCR should never imply adequacy for secure practices and data protection, since they are merely compliance-related.*
- *Discretionary Security Requirements (DSR) are tied to the organization's risk appetite since DSR are "above and beyond" MCR, where the organization self-identifies additional cybersecurity and/or data protection controls to address voluntary industry practices or internal requirements, such as findings from internal audits or risk assessments. DSR are primarily internally-influenced, based on the organization's respective industry and risk tolerance. While MCR establish the foundational floor that must be adhered to, DSR are where organizations often achieve improved efficiency, automation and enhanced security.*

[21] *Integrated Controls Management (ICM) Model - https://securecontrolsframework.com/integrated-controls-management/*

The combination of MCR and DSR equate to an organization's Minimum Security Requirements (MSR), which define the "must have" and "nice to have" requirements for PPTDF in one control set. It describes the Minimum Viable Product (MVP) technical and business requirements from a cybersecurity and data protection perspective. In short, the MSR can be considered an organization's IT General Controls (ITGC), which establishes the basic controls that must be applied to systems, applications, services, processes and data throughout the enterprise. ITGC provide the foundation of assurance for an organization's decision makers. ITGC enables an organization's governance function to define how technologies are designed, implemented and operated.

STANDARD 3.8: DEFINED RISK TOLERANCE

OSAs must define their organizational risk tolerance as follows:

1. Low;
2. Moderate;
3. High;
4. Severe; or
5. Extreme.

Justification: Defined risk tolerance provides criteria to assess an OSA's risk management practices. An organization's risk tolerance is influenced by several factors that includes, but is not limited to:

- *Statutory, regulatory and contractual compliance obligations (including adherence to privacy principles for ethical data protection practices);*
- *Organization-specific threats (natural and manmade);*
- *Reasonably expected industry practices;*
- *Pressure from competition; and*
- *Executive management decisions (e.g., Board of Directors).*

Guidance: See Appendix B: Risk Terminology Normalization for context and examples for determining the appropriate risk tolerance for an organization.

STANDARD 3.9: DEFINED MATURITY LEVEL

OSAs must define the current and targeted level of maturity of its cybersecurity and/or data protection program as one (1) of the following six (6) designations:

1. Level 0 - Not Performed;
2. Level 1 - Performed Informally;
3. Level 2 - Planned & Tracked;
4. Level 3 - Well-Defined;
5. Level 4 - Quantitatively-Controlled; or
6. Level 5 - Continuously Improving; and

Justification: The intended usage of maturity is meant to provide relevant context, as it pertains to control implementation and operations. Different evaluation criteria would be reasonably expected for each level of maturity.

Guidance: The CDPAS leverages the maturity levels from the SCF's Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM):[22]

- ***LEVEL 0 MATURITY - NOT PERFORMED*** *This level of maturity is defined as "non-existence practices," where the control is not being performed:*
  - *Practices are non-existent, where a reasonable person would conclude the control is not being performed.*
  - *Evidence of due care and due diligence do not exist to demonstrate compliance with applicable statutory, regulatory and/or contractual obligations.*
- ***LEVEL 1 MATURITY - PERFORMED INFORMALLY*** *This level of maturity is defined as "ad hoc practices," where the control is being performed, but lacks completeness & consistency:*
  - *Practices are "ad hoc" where the intent of a control is not met due to a lack consistency and formality.*

[22] *SCF Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM) - https://securecontrolsframework.com/capability-maturity-model/*

- *When the control is met, it lacks consistency and formality (e.g., rudimentary practices are performed informally).*
- *A reasonable person would conclude the control is not consistently performed in a structured manner.*
- *Performance depends on the specific knowledge and effort of the individual performing the task(s), where the performance of these practices is not proactively governed.*
- *Limited evidence of due care and due diligence exists, where it would be difficult to legitimately disprove a claim of negligence for how cybersecurity/privacy controls are implemented and maintained.*

- ***LEVEL 2 MATURITY - PLANNED & TRACKED*** *Practices are "requirements-driven" where the intent of control is met in some circumstances, but not standardized across the assessment boundary:*
  - *Practices are "requirements-driven" (e.g., specified by a law, regulation or contractual obligation) and are tailored to meet those specific compliance obligations (e.g., evidence of due diligence).*
  - *Performance of a control is planned and tracked according to specified procedures and work products conform to prescribed standards (e.g., evidence of due care).*
  - *Controls are implemented in some, but not all applicable circumstances/environments (e.g., specific enclaves, facilities or locations).*
  - *A reasonable person could conclude controls are "compliance-focused" to narrowly meet a specific obligation, since the control(s):*
    - *Are localized to specific systems, applications and/or services; and*
    - *Are not standardized across the authorization boundary.*
  - *Sufficient evidence of due care and due diligence exists to demonstrate compliance with specific statutory, regulatory and/or contractual obligations.*
- ***LEVEL 3 MATURITY - WELL DEFINED*** *This level of maturity is defined as "standardized practices," where the control implementation is well-defined and standardized across the assessment boundary:*
  - *From the perspective of the CDPAS, Level 3 maturity practices are standardized across the Assessment Boundary, where this could be across:*
    - *The entire organization;*
    - *A specific contract, project or initiative;*
    - *A specific Business Unit (BU) within an organization; or*
    - *A specific country, or geographic region, of the organization's business operations.*
  - *Controls are implemented in all applicable circumstances/environments (deviations are documented and justified).*
  - *Performance of a control is according to specified well-defined and standardized procedures.*
  - *Control execution is planned and managed using an enterprise-wide, standardized methodology.*
  - *Sufficient evidence of due care and due diligence exists to demonstrate compliance with specific statutory, regulatory and/or contractual obligations.*
- ***LEVEL 4 MATURITY - QUANTITATIVELY CONTROLLED*** *This level of maturity is defined as "metrics-driven practices," where in addition to being well-defined and standardized control implementation across the assessment boundary, there are detailed metrics to enable governance oversight:*
  - *Practices are "metrics-driven" and provide sufficient management insight (based on a quantitative understanding of process capabilities) to predict optimal performance, ensure continued operations and identify areas for improvement.*
  - *Practices build upon established Level 3 maturity criteria and have detailed metrics to enable governance oversight.*
  - *Detailed measures of performance are collected and analyzed. This leads to a quantitative understanding of process capability and an improved ability to predict performance.*
  - *Performance is objectively managed and the quality of work products is quantitatively known.*
- ***LEVEL 5 MATURITY - CONTINUOUSLY IMPROVING*** *This level of maturity is defined as "world-class practices," where control implementation is not only well-defined and standardized across the organization (with detailed metrics), processes are continuously improving:*
  - *Practices are "world-class" capabilities that leverage predictive analysis.*
  - *Practices build upon established Level 4 maturity criteria and are time-sensitive to support operational efficiency, which likely includes automated actions through machine learning or Artificial Intelligence (AI).*
  - *Quantitative performance goals (targets) for process effectiveness and efficiency are established, based on the business goals of the organization.*
  - *Process improvements are implemented according to "continuous improvement" practices to affect process changes.*

STANDARD 3.10: DEFINED MATERIALITY THRESHOLD

OSAs must define the criteria for materiality, as it pertains to its cybersecurity and data protection program.

Justification: The intended usage of materiality is meant to provide relevant context, regarding risk thresholds. Materiality designations are intended to act as a "guard rail" for risk management decisions. A material weakness crosses an organization's risk threshold by making an actual difference to the organization, where systems, applications, services, personnel, the organization and/or third-parties are, or may be, exposed to an unacceptable level of risk.

Guidance: A financial benchmark is commonly used to determine materiality. From a financial impact perspective, for an item to be considered material, the control deficiency, risk, threat or incident (singular or a combination) generally must meet one, or more, of the following criteria where the potential financial impact is measured as:[23]

- *≥ 5% of pre-tax income*
- *≥ 0.5% of total assets*
- *≥ 1% of total equity (shareholder value); and/or*
- *≥ 0.5% of total revenue.*

The SCF Council defines the materiality threshold for an organization's cybersecurity and data protection program as, "A deficiency, or a combination of deficiencies, in an organization's cybersecurity and/or data protection controls (across its supply chain) where it is probable that reasonable threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance that the organization can adhere to its stated risk tolerance." [24]

STANDARD 3.11: MATERIAL RISK DESIGNATION

OSAs must:

1. Identify risks from its risk catalog that have the potential to pose a material impact; and
2. Designate those identified risks as material risks.

Justification: The intended usage of materiality is meant to provide relevant context, regarding risk thresholds. A material risk crosses an organization's risk threshold by making an actual difference to the organization, where systems, applications, services, personnel, the organization and/or third-parties are, or may be, exposed to an unacceptable level of risk.

Guidance: See Appendix B: Risk Terminology Normalization for context on risk management concepts. A risk is:

- *Where someone or something valued is exposed to danger, harm or loss (noun); or*
- *To expose someone or something valued to danger, harm or loss (verb).*

When there is an identified risk that poses a material impact, that is a material risk:

- *A material risk is a quantitative or qualitative scenario where the exposure to danger, harm or loss has a material impact (e.g., potential class action lawsuit, death related to product usage, etc.); and*
- *A material risk should be identified and documented in an organization's "risk catalog" that chronicles the organization's relevant and plausible risks.*

STANDARD 3.12: MATERIAL THREAT DESIGNATION

OSAs must:

1. Identify threats from its threat catalog that have the potential to pose a material impact; and
2. Designate those identified risks as material threats.

Justification: The intended usage of materiality is meant to provide relevant context, regarding risk thresholds. A material threat crosses an organization's risk threshold by making an actual difference to the organization, where systems, applications, services, personnel, the organization and/or third-parties are, or may be, exposed to an unacceptable level of risk.

[23] *Norwegian Research Council - https://snf.no/media/yemnkmbh/a51_00.pdf*
[24] *SCF Cybersecurity Materiality - https://securecontrolsframework.com/cybersecurity-materiality/*

Guidance: A threat:

- *Is a person or thing likely to cause damage or danger (noun); or*
- *Indicates impending damage or danger (verb).*

When there is an identified threat that poses a material impact, that is a material threat:

- *A material threat is a vector that causes damage or danger that has a material impact (e.g., poorly governed Artificial Intelligence (AI) initiatives, nation state hacking operations, dysfunctional internal management practices, etc.); and*
- *A material threat should be identified and documented in an organization's "threat catalog" that chronicles the organization's relevant and plausible threats.*

STANDARD 3.13: MATERIAL INCIDENT DESIGNATION

OSAs must:

1. Identify reasonable incidents that have the potential to pose a material impact; and
2. Designate those identified risks as material incidents.

Justification: The intended usage of materiality is meant to provide relevant context, regarding risk thresholds. A material incident crosses an organization's risk threshold by making an actual difference to the organization, where systems, applications, services, personnel, the organization and/or third-parties are, or may be, exposed to an unacceptable level of risk.

Guidance: An incident is an occurrence that actually or potentially:

- *Jeopardizes the Confidentiality, Integrity, Availability or Safety (CIAS) of a system, application, service or the data that it processes, stores and/or transmits; and/or*
- *Constitutes a violation or imminent threat of violating an organization's policies, procedures or acceptable use practices.*

When there is an incident that poses a material impact, that is a material incident:

- *A material incident is an occurrence that does or has the potential to:*
  - *Affect the CIAS of systems, applications, services or data; or*
  - *Violate organizational practices that have a material impact (e.g., malware on sensitive and/or regulated systems, emergent AI actions, illegal conduct, business interruption, etc.); and*
- *Reasonably foreseeable material incidents should be documented in an organization's Incident Response Plan (IRP) that chronicles the organization's relevant and plausible incidents, so there are appropriate processes to identify, respond to and recover from such incidents.*

STANDARD 3.14: INTERNAL ASSESSMENT

To demonstrate evidence of assessment readiness for 3PAAC Services to a 3PAO, OSAs must:

1. Perform at least one (1) internal cybersecurity and/or data protection controls assessment in preparation for an external assessment by a 3PAO; and
2. Document the internal assessment(s) as part of the OSA's assessment preparation process.

Justification: Performing internal assessments to demonstrate readiness for 3PAAC Services is a due diligence activity. The OSA has a fiduciary duty to its shareholders. Being unprepared to engage with a 3PAO for 3PAAC Services is fiscally irresponsible, since 3PAAC Services are costly and the likelihood of a successful assessment without evidence of due diligence is remote.

Guidance: OSAs should perform and document internal assessments with the same level of rigor and reasonable interpretation of controls expected from a 3PAO.

STANDARD 4: DUE DILIGENCE - ASSESSORS & 3PAOS

3PAOs must:

1. Perform due diligence activities in preparation for an assessment;
2. Document these activities as part of the 3PAO's assessment planning process; and
3. Include the justification for accepting the OSA's readiness for 3PAAC Services.

Justification: Due diligence is simply taking reasonable steps to avoid harm. Therefore, 3PAOs must perform due diligence activities for all assessments.

Guidance: Treating assessments as discrete projects can help a 3PAO perform and document due diligence activities, since many activities are commonly expected for engagements.

STANDARD 4.1: FORMALIZED ASSESSMENT PLAN

3PAOs must:

1. Formalize OSA-specific assessment plans; and
2. Designate an Assessment Team Lead (ATL) with assigned responsibilities to conduct 3PAO Services.

Justification: It is a reasonable expectation for 3PAOs to present a formalized assessment plan to the OSA.

Guidance: Treating assessments as discrete projects can help a 3PAO perform and document due diligence activities, since these activities are commonly expected for assessment engagements. Adequately formulating the plan includes formal documentation of fieldwork steps that reasonably support execution of the 3PAO's assessment methodology from fieldwork initiation to completion, including report development, peer review and issuance.

3PAOs should leverage NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, for guidance on security assessment execution:[25]

- *Security assessment planning:*
  - *Developing a security assessment policy;*
  - *Prioritizing and scheduling assessments;*
  - *Selecting and customizing techniques;*
  - *Assessment logistics:*
    - *Assessor selection and skills;*
    - *Location selection; and*
    - *Technical tools and resources selection;*
  - *Assessment plan develop; and*
  - *Legal considerations;*
- *Security assessment execution:*
  - *Coordination;*
  - *Assessing;*
  - *Analysis; and*
  - *Data handling:*
    - *Data collection;*
    - *Data storage;*
    - *Data transmission; and*
    - *Data destruction; and*
- *Post-testing activities:*
  - *Mitigating recommendations;*
  - *Reporting; and*
  - *Remediation/mitigation.*

DODM 8140.03 should be used for competence criteria for the role of an ATL. Based on the position category and seniority for the role, the ATL is expected to be an "senior-level assessor" with the following qualifications:[26]

[25] *NIST SP 800-115 - https://csrc.nist.gov/pubs/sp/800/115/final*
[26] *DoDM 8140.03 - https://dodcio.defense.gov/Portals/0/Documents/Library/DoDM-8140-03.pdf*

- *An undergraduate degree:*
  - *From an:*
    - *Accreditation Board for Engineering and Technology (ABET) accredited; or*
    - *Centers of Academic Excellence (CAE) designated institution; and*
  - *In the one of the following degrees:*
    - *Information Technology (IT)*
    - *Cybersecurity;*
    - *Data Science;*
    - *Information Systems; or*
    - *Computer Science (CS);*

and/or

- *One (1) of the following certifications:*
  - *CISM - ISACA Certified Information Security Manager;*
  - *CISA - ISACA Certified Information Systems Auditor;*
  - *CISSP - ISC2 Certified Information Systems Security Professional;*
  - *CISSP-ISSEP - ISC2 CISSP - Information Systems Security Engineering Professional;*
  - *GCSA - GIAC Cloud Security Automation;*
  - *GSLC - GIAC Security Leadership Certification;*
  - *GSNA - GIAC Systems and Network Auditor;*
  - *CySA+ - CompTIA Cybersecurity Analyst plus;*
  - *C)ISSO - Certified Information Systems Security Officer;*
  - *C)PTE - Certified Penetration Testing Engineer; and/or*
  - *FITSP-A - Federal IT Security Professional-Auditor.*

STANDARD 4.2: DEFINED ASSESSMENT BOUNDARIES

3PAOs must:

1. Validate the scope of the assessment by defining assessment boundaries; and
2. Limit assessor activities to the defined assessment boundary.

Justification: Assessors and 3PAOs operate from a position of trust and authority. Therefore, assessors must recognize the boundary and restrict assessment activities to systems, applications, services, personnel and third parties within that defined boundary.

Guidance: The Unified Scoping Guide (USG) provides a methodology to assist 3PAOs with: [27]

- *Validating control boundaries; and*
- *Defining the scope of the sensitive and/or regulated data where it is stored, transmitted and/or processed.*

STANDARD 4.3: VALIDATE CONTROL APPLICABILITY

3PAOs must ensure applicable cybersecurity and/or data protection controls to be assessed are:

1. Applicable to the scope of the SOW; and
2. Validated by the OSA.

Justification: OSAs must have documented evidence to justify the assessment scope to the 3PAO. As part of due diligence activities, 3PAOs need to know the specific cybersecurity and/or data protection controls that will make up the assessment, confined within the assessment boundary(ies).

Guidance: Documentation of an OSA's controls by the assessor on behalf of, or in conjunction with, the OSA would not be considered a COI. For the purposes of completing the assessment, this clarification of applicable controls would not constitute "control design or implementation" services.

[27] *Unified Scoping Guide (USG) - https://unified-scoping-guide.com*

STANDARD 4.4: DEFINED EVIDENCE REQUEST LIST (ERL)

Based on the defined cybersecurity and/or data protection controls, the assessor must provide the OSA with an Evidence Request List (ERL) that defines the SOW-specific artifacts necessary to perform 3PAAC Services. For evidence:

1. The OSA must provide evidence artifacts of a level of detail, accuracy and formatting to satisfy assessment rigor criteria; and
2. The 3PAO may request additional evidence artifacts, or clarification of OSA-submitted ERL artifacts, as necessary to perform 3PAAC Services.

Justification: Assessors and 3PAOs operate from a position of trust and authority. Therefore, minimizing "scope creep" that can increase the duration, cost and personnel commitments associated with an assessment is essential. As part of due diligence activities, assessors and 3PAOs are expected to:

- *Define an authoritative ERL; and*
- *Before the start of the assessment, provide any artifact requests to the OSA.*

An ERL provides assessment-specific artifacts where:

- *It establishes a minimum level of reasonable evidence necessary for the 3PAO to conduct 3PAAC Services;*
- *The intent is for ERLs to establish a finite list of supporting evidence used in an assessment; and*
- *Prior to the start of the assessment, an ERL will be provided by the 3PAO to the OSA.*

Guidance: The SCF provides ERL that assessors and 3PAOs can use. The ERL is part of the SCF download.[28] The ERL represents the minimum level of reasonable evidence requests.

STANDARD 4.5: EXPLICIT AUTHORIZATION FOR TESTING

Prior to performing assessment-related control testing activities, 3PAOs must obtain written authorization from the OSA in the form of a:

1. Signed contract;
2. MSA;
3. SOW; and/or
4. Change order.

Justification: Obtaining explicit authorization minimizes liability to assessors and 3PAOs. The assumption is that an OSA's network is highly integrated with dependencies that can affect the ability of the organization to perform its business operations. Therefore, 3PAOs must receive written authorization to perform specific assessment-related control testing activities.

Guidance: Any control testing activities should be viewed similarly to precautions taken by a third-party to perform a vulnerability assessment or penetrating testing engagement.

STANDARD 4.6: FIRST-PARTY DECLARATIONS (1PD) - CONTROL INHERITANCE

Assessors must review available 1PD artifacts to understand possible dependencies and control inheritance, if applicable and/or available. 1PDs must:

1. Originate from internal audits and/or assessments by:
    a. The OSA; and/or
    b. ESP that impact the OSA's assessment boundary;
2. If applicable, document the ESP's service(s) the OSA is claiming control inheritance in:
    a. A contract between the OSA and ESP; and
    b. A RASCI matrix, or similar form of customer responsibility matrix, that clearly identifies applicable roles and responsibilities associated with inherited controls;
3. Contain sufficient detail to determine the applicability of inherited cybersecurity and/or data protection controls;
4. Specify the specific controls being inherited;
5. Validate that controls identified for inheritance share the same assessment boundary(ies);
6. Reflect the current architecture of the OSA's network infrastructure; and
7. Have been generated within the past twelve (12) months.

[28] *SCF Evidence Request List (ERL) - https://securecontrolsframework.com/scf-download*

Justification: It is a reasonable assumption that an OSA will have third-party dependencies. The OSA may provide self-attestations from supporting organizations to demonstrate control implementation. 1PD may address significant control inheritance (e.g., third-party control responsibility, service providers' security certifications, etc.), but this evidence requires some form of validation by the 3PAO.

Most assessments can be considered "black box" endeavors, where the assessor has no previous information on the environment being assessed. However, some assessments are "gray box" or "white box" assessments where the assessor is expected to work off previous evidence.

Guidance: It is at the 3PAO's discretion to perform limited or in-depth control testing to validate control inheritance.

STANDARD 4.7: THIRD-PARTY ATTESTATIONS (3PA) - CONTROL INHERITANCE & RECIPROCITY

Assessors must review available 3PA artifacts to understand possible dependencies and control inheritance, if applicable and/or available. 3PA must:

1. Be from a reputable third-party with subject matter expertise in the topic being attested to;
2. If applicable, document the ESP's service(s) the OSA is claiming control inheritance in:
    a. A contract between the OSA and ESP; and
    b. A RASCI matrix, or similar form of customer responsibility matrix, that clearly identifies applicable roles and responsibilities associated with inherited controls;
3. Contain sufficient detail to determine the applicability of inherited cybersecurity and/or data protection controls;
4. Specify the specific controls:
    a. Being inherited; and/or
    b. Claiming reciprocity;
5. Validate that controls identified for inheritance and/or reciprocity share the same assessment boundary(ies);
6. Reflect the current architecture of the OSA's network infrastructure; and
7. Have been generated within the past twelve (12) months.

Justification: It is a reasonable assumption that an OSA will have third-party dependencies. The OSA may be provided with third-party attestations (e.g., SOC 2, ISO 27001, CMMC, etc.) to demonstrate control implementation. 3PA may address significant control inheritance (e.g., third-party control responsibility, service providers' security certifications, etc.), but this evidence requires some form of validation by the 3PAO.

Guidance: For properly scoped and applicable controls:

- *3PAOs are required to accept the reciprocity decision from the authoritative body; and*
- *It is at the 3PAO's discretion to perform limited or in-depth control testing to validate control inheritance.*

STANDARD 4.8: STAKEHOLDER VALIDATION

Assessors must validate the applicability of pertinent assessment stakeholders, based on the OSA's provided:

1. Assessment boundary demarcation;
2. Graphical representation of assessment boundary(ies);
3. RASCI matrix;
4. Defined cybersecurity and/or data protection controls; and
5. When applicable:
    a. 1PD and/or
    b. 3PA.

Justification: Identified stakeholders provide justification for the defined assessment boundary. If the identified stakeholders do not support the assessment boundary, there is an indication that:

- *The scope of the assessment may be incorrect;*
- *The defined cybersecurity and/or data protection controls are incorrect; and/or*
- *The identified stakeholders are incorrect.*

Guidance: Stakeholder identification can be achieved by documenting a RASCI matrix.

STANDARD 5: DUE CARE - OSAS

OSAs must perform due care activities when executing:

1. Control design;
2. Control implementation; and
3. Continued operation.

Justification: Due care is the conduct a reasonable person with appropriate skills and experience, would exercise in a similar situation. Therefore, OSAs are expected to operate by a standard of care that others in the industry would reasonably follow.

Guidance: Treating assessments as discrete projects can help an OSA perform and document due care activities. This requires proactive governance on behalf of the OSA.

STANDARD 5.1: PROACTIVE GOVERNANCE

OSAs must assign an employee with sufficient authority and subject matter expertise to proactively govern the OSA's cybersecurity and data protection program(s).

Justification: Proactive governance is the opposite of reactive governance, where an issue or problem is addressed after it becomes a crisis. OSAs are expected to govern its cybersecurity and data protection program proactively.

Guidance: It is possible for one role to oversee both cybersecurity and data protection efforts. However, common roles associated with hierarchical authority for the cybersecurity and data protection programs include:

- *From a cybersecurity perspective for cybersecurity-related leadership:*
  - *Chief Information Security Officer (CISO); and*
  - *Director of Cybersecurity, or a comparable position.*
- *From a data protection perspective for data privacy-related leadership:*
  - *Chief Privacy Officer (CPO).*

Proactive governance is a continuous process of risk and threat identification, analysis and remediation. In addition, it also includes proactively updating policies, standards and procedures in response to emerging threats or regulatory changes.

OSAs should leverage NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, for guidance on:[29]

- *Review techniques:*
  - *Documentation review;*
  - *Log review;*
  - *Ruleset review;*
  - *System configuration review;*
  - *Network sniffing and;*
  - *File integrity checking; and*
- *Target identification and analysis techniques:*
  - *Network discovery;*
  - *Network port and service identification;*
  - *Vulnerability scanning; and*
  - *Wireless scanning.*

STANDARD 5.2: NON-CONFORMITY OVERSIGHT

OSAs must document, assess and implement remediation actions to address instances of non-conformity, where deficiencies with:

1. Material controls are remediated without delay; and
2. Non-material controls are remediated according to the:
   a. Risk associated with the non-conforming control; and

[29] *NIST SP 800-115 - https://csrc.nist.gov/pubs/sp/800/115/final*

b. OSA's established vulnerability management and/or change management practices.

Justification: A formal methodology is necessary to provide non-conformity oversight.

Guidance: As part of proactive governance, it is expected that OSAs will encounter instances of non-conformity due to business and technology-related changes or limitations. This ongoing process of evolving cybersecurity and/or data protection practices to meet changes in business and technology requires proactive governance suitable of withstanding scrutiny by an independent third-party. Formal oversight of non-conformities is necessary to systematically identify, track and remediate gaps in cybersecurity and/or data protection controls. For example, establishing a corrective action plan with timelines and responsibilities helps ensure that identified issues are addressed promptly and effectively.

STANDARD 5.3: ANNUAL AFFIRMATION

OSAs must:

1. Internally perform an annual assessment that validates:
    a. The assessment boundary(ies) for issued certifications;
    b. POA&M items are proactively managed to remediate identified deficiencies; and
    c. Implemented changes are not material to the assessment boundary(ies); and
2. Affirm the status of its cybersecurity and data protection controls continues to support its conformity designation for applicable certifications.

Justification: Annual affirmations:

- *Ensure OSAs conduct periodic checks; and*
- *Verify that unaccounted for material changes have not occurred.*

Guidance: The organization official making the annual affirmation should be the senior individual responsible for the organization's compliance requirements. This individual should:

- *Be assigned the role of monitoring compliance with applicable requirements; and*
- *Have the technical competence to understand how compliance can be objectively demonstrated.*

Per Standard 9, material and non-material changes are defined as:

- *Material Change. A material change to the OSA's cybersecurity and/or data protection program is where the OSA performed a broad scope of significant changes to the OSA's cybersecurity and/or data protection controls.*
- *Non-Material Change. A non-material change to the OSA's cybersecurity and/or data protection program is where the OSA performed a limited scope of minor changes to the OSA's cybersecurity and/or data protection controls.*

The content of the affirmation should include the following information:

- *Name, title, and contact information for the individual performing the affirmation; and*
- *An affirmation statement attesting that the OSA has implemented and continues to maintain all applicable cybersecurity and/or data protection controls relevant to PPTDF within the relevant assessment boundary.*

STANDARD 6: DUE CARE - ASSESSORS & 3PAOS

3PAOs must perform due care activities in the execution of assessment activities.

Justification: Due care is the conduct a reasonable person with appropriate skills and experience would exercise in a similar situation. Therefore, assessors and 3PAOs are expected to operate by a standard of care that others in the industry would reasonably follow.

Guidance: Treating assessments as discrete projects can help a 3PAO perform and document due care activities. This requires proactive governance on behalf of the 3PAO.

STANDARD 6.1: ASSESSMENT METHODS

Assessors must:

1. Utilize an assessment method in accordance with the SOW; and
2. Specify one (1) of the following assessment methods:
    a. Manual Point In Time (MPIT). MPIT is a traditional assessment methodology that:
        i. Is relevant to a specific point in time (time at which the controls were evaluated); and
        ii. Relies on the manual review of artifacts to derive a finding;
    b. Automated Point In Time (APIT). APIT utilizes automation to augment a traditional assessment methodology, where Artificial Intelligence and Autonomous Technologies (AAT) are used to compare the desired state of conformity versus the current state via machine-readable configurations and/or assessment evidence:
        i. Is relevant to a specific point in time (time at which the controls were evaluated);
        ii. In situations where technology cannot evaluate evidence, evidence is manually reviewed; and
        iii. The combined output of automated and manual reviews of artifacts is used to derive a finding; or
    c. Automated Evidence with Human Review (AEHR). AEHR is used for ongoing, continuous control assessments:
        i. AAT continuously evaluates controls by comparing the desired state of conformity versus the current state through machine-readable configurations and/or assessment evidence; and
        ii. Recurring human reviews:
            1. Evaluate the legitimacy of the results from automated control assessments; and
            2. Validate the automated evidence review process to derive a finding.

Justification: The SOW is expected to capture the assessment method, since that establishes the context for expected assessor involvement and related costs. The adoption of automation technologies for 3PAAC Services must be addressed to:

- *Adjust to evolving technologies available to 3PAOs; and*
- *Avoid improper assumptions about control evaluation practices.*

Guidance: It is acceptable for a 3PAO to offer a single assessment method (e.g., MPIT). However, 3PAOs are expected to have procedures developed for each assessment method offered as part of its 3PAAC Services.

APIT and AEHR may leverage Artificial Intelligence and/or Machine Learning (AI/ML) technologies. In the case of AI/ML being used, 3PAOs must be prepared to demonstrate sufficient evidence of due diligence and due care to justify the integrity of the findings and overall assessment results (e.g., evidence of validating results, test cases, etc.).

See Appendix C: Assessment Rigor for more details on how assessment methods relate to assessment rigor. At a minimum:

- *Standard rigor should be used for MPIT assessments;*
- *Enhanced rigor should be used for APIT assessments; and*
- *Comprehensive rigor should be used for AEHR assessments.*

STANDARD 6.2: ASSESSMENT RIGOR

Assessors must perform the assessment at a level of rigor in accordance with the SOW. There are three (3) levels of rigor:

1. Level 1 Rigor: STANDARD. Standard rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether the applicable controls are:
    a. Implemented; and
    b. Free of obvious errors.
2. Level 2 Rigor: ENHANCED. Enhanced rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether:
    a. The applicable controls are:
        i. Implemented; and
        ii. Free of obvious/apparent errors; and
    b. There are increased grounds for confidence that the applicable controls are:
        i. Implemented correctly; and
        ii. Operating as intended.
3. Level 3 Rigor: COMPREHENSIVE. Comprehensive rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining:
    a. Whether the applicable controls are:

i. Implemented; and
ii. Free of obvious/apparent errors;

b. Whether there are further increased grounds for confidence that the applicable controls are:
   i. Implemented correctly; and
   ii. Operating as intended on an ongoing and consistent basis; and
c. There is support for continuous improvement in the effectiveness of the applicable controls.

Justification: It is essential to establish the expectation for the level of rigor to be performed by the assessment team. The SOW is expected to capture the level of rigor, since that establishes the context for expected assessor involvement and related costs. At a minimum:

- *Standard rigor should be used for MPIT assessments;*
- *Enhanced rigor should be used for APIT assessments; and*
- *Comprehensive rigor should be used for AEHR assessments.*

Guidance: See Appendix C: Assessment Rigor for more details on assessment rigor. 3PAOs are expected to have assessment plans developed for each level of rigor. In addition, the 3PAO is expected to develop clear criteria for determining the level of rigor (Standard, Enhanced, Comprehensive) based on the OSA's needs, risk appetite and risk profile. OSAs are responsible for selecting the most appropriate level of rigor to address their unique assessment requirements.

STANDARD 6.3: ASSESSING BASED ON CONTROL APPLICABILITY

Assessors must limit their evidence examination, interviews and testing activities based on the applicability of the assessed cybersecurity and/or data protection controls. A single cybersecurity and/or data protection control primarily applies to only one (1) of the following functions:

1. People;
2. Processes;
3. Technologies;
4. Data; and/or
5. Facilities.

Justification: Control scoping does not mean all controls apply uniformly to every asset, individual or facility. There is a common misconception that if something is "in scope" then every control will be applicable across the entire assessment boundary. This is an incorrect assumption, since the nature of a control is primarily administrative, technical or physical. This means specific controls may not apply to all assets, processes, people and locations.

Guidance: Control scoping is not the same thing as control applicability, since it is technically infeasible to apply all controls uniformly, based on control applicability:

- *Controls are primarily administrative, technical and/or physical. This means that there may be controls that are not applicable.*
- *It is possible for a control to apply across more than a single function. However, in most cases, controls apply to a single function.*

The recommended solution is to create some form of a matrix that can apply the appropriate controls to the correct PPTDF to help identify the proper scope for the implementation of controls:

- ***People** - Control directly applies to humans (e.g., training, background checks, non-disclosure agreements, etc.).*
- ***Processes** - Control directly applies to administrative work performed (e.g., processes, procedures, administrative documentation, etc.).*
- ***Technologies** - Control directly applies to systems, applications and services (e.g., secure baseline configurations, patching, etc.).*
- ***Data** - Control directly applies to data protection (e.g., encrypting sensitive and/or regulated data, applying metatags, etc.).*
- ***Facilities** - Control directly applies to infrastructure assets (e.g., physical access, HVAC systems, visitor control, etc.).*

Example 1: Network firewall

- *A network firewall is a technology asset where specific other controls would be applicable, such as Multi-Factor Authentication (MFA), access control, secure baseline configurations and patch management.*
- *A network firewall is a device. Therefore, a network firewall is not capable of undergoing end user training, completing a Non-Disclosure Agreement (NDA) or conducting incident response exercises.*

Example 2: User awareness training

- *User awareness training focuses on personnel, such as employees and applicable third parties, who will interact with the organization's systems and data. NDAs, threat intelligence awareness and acceptable use notifications apply to individuals.*
- *An individual is not a device. Therefore, an individual is not capable of having a secure baseline configuration applied, be scanned by a vulnerability assessment tool, or have missing patches installed.*

Example 3: Incident Response Plan (IRP)

- *An IRP is a documented process that guides incident response operations.*
- *An IRP is not an individual or technology. Therefore, an IRP cannot sign an NDA, have MFA or be patched.*

STANDARD 6.4: ASSESSMENT OBJECTIVES (AOS)

Assessors must evaluate controls by utilizing Assessment Objectives (AOs), when AOs are available.

Justification: AOs are objective statements that establish the desired outcome for the assessment for a specific control. There may be multiple AOs associated with a control.

Guidance: AOs provide objective criteria that each must be satisfied to legitimately determine whether the control is implemented and operating as intended. The SCF has a catalog of AOs that 3PAOs can use, including:

- *SCF baseline;*
- *NIST SP 800-53A R5;*
- *NIST SP 800-171A;*
- *NIST SP 800-171A R3; and*
- *NIST SP 800-172A.*

STANDARD 6.5: CONTROL DESIGNATION

Assessors must designate a status to assessed controls as follows:

1. There are four (4) possible designations:
    a. Satisfactory;
    b. Deficient;
    c. Alternative Control; or
    d. Not Applicable (N/A); and
2. Where AOs are available, for a control to be designated as Satisfactory, each of the control's applicable AOs must be designated as:
    a. Satisfactory;
    b. Alternative Control; or
    c. N/A; and
3. If all of the following conditions exist, a control designated as Deficient may be re-evaluated during the course of the assessment and for up to ten (10) business days following the active assessment period:
    a. Additional evidence:
        i. Is available to demonstrate the control is satisfied; and
        ii. Cannot change, or limit the effectiveness of, other requirements that have previously been scored Satisfactory; and
    b. The Report on Conformity (ROC) has not been delivered to the OSA.

Justification: The assessed status of controls needs a standardized status designation. A standardized methodology to describe the assessed status of a control is necessary to maintain the integrity of the assessment process.

Guidance: In the context of control designations, as designation of:

- *Satisfactory is positive, where the criteria are met;*
- *Deficient is negative, where the criteria are not met;*
- *Alternative Control is neutral, where another control, or controls, is/are designated as sufficiently reducing the risk(s) associated with the control; and*
- *N/A is neutral, where the control, or AO, does not apply.*

STANDARD 6.6: OBJECTIVITY THROUGH REASONABLE INTERPRETATION

Assessors must maintain objectivity through the following:

1. Reasonable interpretation of:
    a. Controls; and
    b. When available, AOs; and
2. Analysis of relevant evidence from:
    a. Examinations;
    b. Interviews; and/or
    c. Testing.

Justification: Assessors operate from a position of trust and authority. Therefore, assessors must utilize objectivity through reasonable interpretation of both AOs and evidence. Objectivity and reasonableness are cornerstone expectations for any professional. The testing of controls determines the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the applicable AOs.

Guidance: If a control doesn't meet the intent of the design, there is no need to test its effectiveness. Assessors should leverage NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, for guidance on:[30]

- *Review techniques:*
    - *Documentation review;*
    - *Log review;*
    - *Ruleset review;*
    - *System configuration review;*
    - *Network sniffing and;*
    - *File integrity checking; and*
- *Target identification and analysis techniques:*
    - *Network discovery;*
    - *Network port and service identification;*
    - *Vulnerability scanning; and*
    - *Wireless scanning.*

Appendix D: Adequate Security provides context about determining "reasonableness" in the context of evaluating cybersecurity and/or data protection controls. For a 3PAO to maintain reasonable interpretation by its assessment team, it is expected to:

- *Implement sound hiring practices to attract and retain quality individuals;*
- *Ensure assessors receive continuing education that is specific to assessment-related activities to maintain situational awareness of leading industry practices; and*
- *Perform After Action Reviews (AARs) with an OSA to identify possible conflicts where reasonable interpretation was not followed.*

STANDARD 6.7: ADEQUATE SAMPLING

For reasonable evidence of conformity:

1. Assessors must obtain an adequate sampling of applicable evidence to make a reasonable determination of conformity; and
2. The sampling must represent the period of operation relevant to the assessment.

[30] *NIST SP 800-115 - https://csrc.nist.gov/pubs/sp/800/115/final*

Justification: Assessors are expected to use one (1), or more, of these sampling methods to help ensure that the assessment results are representative of the overall environment, providing a reliable basis for evaluating control effectiveness:

- *Simple random sampling;*
- *Stratified sampling;*
- *Systemic sampling; and/or*
- *Cluster sampling.*

Guidance: Simple random sampling is preferred for performing Standard and Enhanced assessments. This involves randomly selecting a subset of people, processes, technologies, data sets and facilities to evaluate cybersecurity and/or data protection controls.

Appendix D: Adequate Security provides context about determining adequacy. The assessor establishes adequate evidence to support a conclusion of sufficient operation for the period as follows:

- *Adequate evidence is defined by reasonable, not absolute assurance principles; and*
- *Adequacy is determined by the assessor for each control included in the scope boundary.*

Adequate evidence of conformity would suggest multiple samples are selected across the previous twelve (12)-month period of operation in which the samples would be available and in the same format for a randomized period of dates selected by the assessor, validating the evidence (e.g., log file) was present and generated for that period (e.g., asset created the log event).

STANDARD 6.8: ASSESSMENT TOOLS & AUTOMATION

3PAOs must implement assessment-related mechanisms to:

1. Improve accuracy; and
2. Reduce human error.

Justification: Traditional, manual assessment methodologies are inefficient and error-prone. 3PAOs should incorporate automated mechanisms (e.g., a Governance, Risk & Compliance (GRC) solution) or advanced assessment tools (e.g., Artificial Intelligence and Autonomous Technologies (AAT)) to:

- *Increase the efficiency of the assessment process; and*
- *Reduce:*
  - *Human error; and*
  - *The ability of an assessor to skew data.*

Guidance: Relying on hand-written notes or ad hoc spreadsheets is something that 3PAOs should strive to avoid. The use of Governance, Risk & Compliance (GRC) platforms with specific control assessment functions should be considered a minimal expectation for an assessment tool utilized by 3PAO for 3PAAC Services.

STANDARD 7: QUALITY CONTROL

3PAOs must systematically examine and evaluate assessment processes, procedures, activities and deliverables to ensure compliance with established quality standards and requirements.

Justification: An assessment's results can have positive, negative or neutral consequences for the OSA. Therefore, quality control by the 3PAO is crucial to ensure the assessment results accurately reflect the actual state of cybersecurity and/or data protection controls. This requires internal quality control processes by the 3PAO.

Guidance: The 3PAO is expected to adhere to a relevant Quality Management System (QMS), as defined by industry-recognized practices (e.g., ISO 9001, ISO 17020, etc.).

STANDARD 7.1: ASSESSMENT FINDINGS

To ensure the ability of a reasonable individual, having a similar amount of knowledge and experience, to arrive at the same conclusion(s), 3PAOs must:

1. Document assessment findings;
2. Objectively confirm the validity of the assessment team's conclusions; and
3. If applicable, submit assessment results to the appropriate:
    a. Accreditation Body (AB); or
    b. Governing body.

Justification: Assessment teams may be made up of both employees of a 3PAO and independent contractors. Due to this possible transitory nature of individual assessors, assessment findings must be documented in a manner that a reasonable individual, with similar qualifications and experience, could evaluate the same facts and circumstances and arrive at the same conclusion as the original assessor.

Guidance: The documentation of assessment findings to ensure reasonableness is expected to be included in the 3PAO's quality control processes. The documentation of assessment findings should include but is not limited to:

- *Detailed descriptions of the findings and their impact on the OSA's cybersecurity posture;*
- *Evidence supporting each finding, such as logs, screenshots, or interview notes; and*
- *Recommendations for remediation and timelines for implementing corrective actions.*

Assessors may provide initial findings to the OSA as "end of day" or "end of period" out briefing to give the OSA situational awareness on the status of the assessment.

3PAOs should leverage NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, for guidance on security assessment related:[31]

- *Mitigating recommendations;*
- *Reporting; and*
- *Remediation/mitigation.*

STANDARD 7.2: OBJECTIVE PEER REVIEW

Assessors must obtain an objective peer review of all assessment-related findings before presenting findings to the OSA.

Justification: Objectivity is essential when documenting assessment findings. Reviewing the findings by a qualified, competent individual not part of the assessment team is crucial to produce a quality assessment report. Internal peer reviews ensure objectivity by having assessment findings evaluated by someone independent of the assessment process. This practice helps identify potential biases or errors and ensures that findings are based on evidence and aligned with established criteria.

Guidance: Peer reviews by people other than the assessment team are expected to be part of the 3PAO's quality control processes. Peer reviews can be from an internal or third-party resource.

STANDARD 8: CONFORMITY DESIGNATION

3PAOs must summarize assessment results with a conformity designation. Only one (1) of the following four (4) possible conformity designations may be used:

1. STRICTLY CONFORMS. The designation of Strictly Conforms is a positive outcome. Strictly Conforms indicates:
    a. The OSA can demonstrate Strict Conformity with its selected cybersecurity and/or data protection controls, where one hundred percent (100%) of the assessed controls have reasonable evidence to conclude:
        i. The controls are met and operational;
        ii. Any control designated as Not Applicable (N/A) is validated as such by the assessor; and/or
        iii. Where applicable, compensating controls are validated by the assessor as being:
            1. Applicable;
            2. Reasonable; and

[31] *NIST SP 800-115 - https://csrc.nist.gov/pubs/sp/800/115/final*

3. Implemented and operating properly; and

b. Assessed controls provide reasonable assurance that the OSA's cybersecurity and data protection program provides adequate security, where it:
   i. Adheres to a defined and documented risk tolerance;
   ii. Mitigates material cybersecurity and/or data protection risks;
   iii. Is designed to detect and protect against material cybersecurity and/or data protection threats; and
   iv. Is prepared to respond to material incidents.

2. CONFORMS. The designation of Conforms is a positive outcome. Conforms indicates:
   a. The OSA can demonstrate conformity with its selected cybersecurity and/or data protection controls, where at least eighty percent (80%) of the assessed controls have reasonable evidence to conclude:
      i. The controls are met and operational;
      ii. Any control designated as N/A is validated as such by the assessor; and/or
      iii. Where applicable, compensating controls are validated by the assessor as being:
         1. Applicable;
         2. Reasonable; and
         3. Implemented and operating properly;
   b. Any assessed control deficiency is not material to the OSA's cybersecurity and data protection program; and
   c. Assessed controls provide reasonable assurance that the OSA's cybersecurity and data protection program provides adequate security, where it:
      i. Adheres to a defined and documented risk tolerance;
      ii. Mitigates material cybersecurity and/or data protection risks;
      iii. Is designed to detect and protect against material cybersecurity and/or data protection threats; and
      iv. Is prepared to respond to material incidents.

3. SIGNIFICANT DEFICIENCY. The designation of Significant Deficiency is a negative outcome. Significant Deficiency indicates:
   a. The OSA can demonstrate limited conformity with its selected cybersecurity and/or data protection controls due to a systemic problem within the OSA's cybersecurity and data protection program, where:
      i. At least seventy percent (70%), but less than eighty percent (80%), of the assessed controls have reasonable evidence to conclude:
         1. The controls are met and operational;
         2. Any control designated as N/A is validated as such by the assessor; and/or
         3. Where applicable, compensating controls are validated by the assessor as being:
            a. Applicable;
            b. Reasonable; and
            c. Implemented and operating properly;
   b. Any assessed control deficiency is not material to the OSA's cybersecurity and data protection program;
   c. Assessed controls do not provide reasonable assurance that the OSA's cybersecurity and data protection program provides adequate security, where it:
      i. Adheres to a defined and documented risk tolerance;
      ii. Mitigates material cybersecurity and/or data protection risks;
      iii. Is designed to detect and protect against material cybersecurity and/or data protection threats; and
      iv. Is prepared to respond to material incidents; and
   d. The OSA's cybersecurity and data protection program:
      i. Has systemic problems inherent in the overall function of a team, department, project, application, service and/or vendor rather than a specific, isolated factor; and
      ii. Requires implementing limited changes to personnel, technology and/or practices to correct the design and implementation of deficient cybersecurity and/or data protection controls.

4. MATERIAL WEAKNESS. The designation of Material Weakness is a negative outcome. Material Weakness indicates:
   a. The OSA cannot demonstrate conformity with its selected cybersecurity and/or data protection controls due to deficiencies that make it probable that reasonably expected threats will not be promptly detected or prevented, where:
      i. One (1), or more, material controls is/are deficient; and/or
      ii. Less than seventy percent (70%) of the assessed controls have reasonable evidence to conclude:
         1. The controls are met and operational;
         2. Any control designated as N/A is validated by the assessor and confirmed as such; and/or
         3. Where applicable, compensating controls are validated by the assessor as being:

a. Applicable;
b. Reasonable; and
c. Implemented and operating properly;

b. Assessed controls do not provide reasonable assurance that the OSA's cybersecurity and data protection program adequately:
    i. Adheres to a defined and documented risk tolerance;
    ii. Mitigates material cybersecurity and/or data protection risks; and/or
    iii. Possesses the capability to:
        1. Detect and protect against material cybersecurity and/or data protection threats; and/or
        2. Respond to material incidents; and
c. The OSA's cybersecurity and data protection program:
    i. Cannot perform its stated mission; and
    ii. Drastic changes to people, processes and/or technologies are required to remediate the deficiencies.

Justification: A systemic weakness across existing assessment methodologies is the lack of a standardized assessment conformity designation. Assessment conformity designations are supported by Standard 6.5 (Control Designation) and are used to summarize the overall assessment.

Guidance: See Appendix D: Adequate Security for more details on defining adequate security. The assessment conformity designation is intended for the OSA's executive leadership team to clearly and unambiguously provide a "pass or fail score" to the assessment. The use of the terminology in this standard is recognized throughout the industry, so it avoids reinventing the concept.

An OSA cannot have a Strictly Conforms, Conformity or Significant Deficiency designation with a Material Weakness determination in one (1), or multiple, domain(s)/family(ies) of cybersecurity and/or data protection controls included in the assessment boundary.

STANDARD 8.1: REPORT ON CONFORMITY (ROC)

3PAOs must produce a written Report on Conformity (ROC) that uses persuasive, reasonable evidence to defend the assessment conformity designation.

Justification: The assessment results must be documented in a professional format capable of defending the assessment conformity designation.

Guidance: The format of a ROC is not standardized in the industry and would be up to a governing body, or 3PAO, to define its specific needs. A ROC should include, but is not limited to the following elements:

- *Disclosure of the level of rigor selected for 3PAAC Services (see Appendix C for details on Assessment Rigor);*
- *A summary of the assessment scope and objectives;*
- *Detailed findings and evidence supporting each determination;*
- *An executive summary highlighting the overall conformity status (e.g., Strictly Conforms, Conforms, Significant Deficiency, Material Weakness);*
- *Recommendations for remediation where deficiencies are identified; and*
- *A section for the OSA to respond to findings or submit challenges.*

This format ensures that the ROC is comprehensive and provides all necessary information for stakeholders to understand the assessment results.

3PAOs are expected to link persuasive, reasonable evidence to the applicable level of rigor and available evidence.

STANDARD 8.2: ASSESSMENT FINDING CHALLENGES

3PAOs must have a formal process to:

1. Intake, review and respond to an OSA's challenges regarding assessment findings, as defined in the:
    a. MSA; and/or
    b. SOW; and
2. Settle challenges through:
    a. Direct negotiation;
    b. If applicable, the applicable Accreditation Body (AB);
    c. Arbitration; or
    d. The applicable legal venue, as defined in the:
        i. MSA; and/or
        ii. SOW.

Justification: 3PAOs and OSAs have the right to disagree. However, the ROC reflects the point-in-time observations of the 3PAO's assessment team. These assessment findings affect the assessment conformity designation issued by the 3PAO. Therefore, 3PAOs must be prepared to handle challenges to assessment findings professionally and responsively. It is reasonable to expect that assessment conformity designation, particularly those identifying a Significant Deficiency or Material Weakness, may lead to disputes or challenges from the OSA. A formalized process for handling these challenges is necessary to maintain the integrity of the assessment and ensure that all concerns are addressed in a fair and transparent manner. This process should include clear guidelines for submitting challenges, timelines for review, criteria for evaluating challenges and procedures for resolution.

Guidance: The 3PAO must ensure the SOW and other documentation it uses as part of its 3PAAC Services covers the processes around challenging assessment findings. This may require legal arbitration for points of contention that cannot be settled solely by the 3PAO and OSA.

To help eliminate unexpected results, assessors may provide initial findings to the OSA as "end of day" or "end of period" out briefing to give the OSA situational awareness on the status of the assessment.

STANDARD 9: MAINTAINING CONFORMITY

OSAs must seek re-assessment when there is a material change to the assets and/or processes that make up the assessment boundary. Changes are defined as:

1. Material Change. A material change to the OSA's cybersecurity and/or data protection program is where the OSA performed a broad scope of significant changes to the OSA's cybersecurity and/or data protection controls.
2. Non-Material Change. A non-material change to the OSA's cybersecurity and/or data protection program is where the OSA performed a limited scope of minor changes to the OSA's cybersecurity and/or data protection controls.

Justification: A 3PAO-issued attestation and/or certification is voided when material changes affect the assessment boundary, since the basis for the attestation and/or certification is no longer applicable.

Guidance: The timeline for remediation should be agreed upon between the 3PAO and the OSA, since the timeline is dependent upon the risk appetite of the organization. However, unless justified by a legitimate business, or technical, reason no POA&M item should be older than one-hundred eighty (180) days. Items older than that should be considered deficient.

- *Assessor has the ability to re-evaluate controls during the course of the assessment and for up to ten (10) business days following the active assessment period.*
- *A "plan to address" a deficiency does not suffice as evidence to support control conformity. The plan to remediate a deficiency must be implemented and operational.*

An OSA's material changes to any certified environment should be coordinated with the 3PAO that performed the most recent assessment. That 3PAO should be contracted to conduct 3PAAC Services to validate, or re-issue, an attestation and/or certification.

- *Material changes have a strategic and/or operational impact on the OSA's cybersecurity and/or data protection capabilities; and*
- *Non-material changes have a tactical-focused impact on the OSA's cybersecurity and/or data protection capabilities.*

STANDARD 9.1: PLAN OF ACTION & MILESTONES (POA&M)

OSAs must document control deficiencies in a Plan of Action & Milestones (POA&M), or similar form of control deficiency tracking mechanism, at a minimum identifies the following:

1. Deficient control(s);
2. A description of the control deficiency(ies);
3. Affected people, processes, technologies, data and/or facilities;
4. Designated Point of Contact (POC) for remediation efforts;
5. Remediation plan (e.g., milestones, resources needed, etc.);
6. Scheduled remediation date; and
7. Date remediation was completed.

Justification: A formal methodology is necessary to document identified tasks, responsibilities and milestones associated with control deficiencies. It provides a clear roadmap for addressing weaknesses, assigns responsibilities and sets deadlines for completion, ensuring accountability and timely resolution.

Guidance: The timeline for remediation should be agreed upon between the 3PAO and the OSA, since the timeline is dependent upon the risk appetite of the organization. However, unless justified by a legitimate business, or technical, reason no POA&M item should be older than one-hundred eighty (180) days. Items older than that should be considered deficient.

- *Assessor has the ability to re-evaluate controls during the course of the assessment and for up to ten (10) business days following the active assessment period.*
- *A "plan to address" a deficiency does not suffice as evidence to support control conformity. The plan to remediate a deficiency must be implemented and operational.*

A POA&M is a "living document" that can exist in a manner that works best for the OSA, ranging from a simple Excel spreadsheet that serves as a risk register or it can be a dedicated module in a GRC technology platform. POA&Ms:

- *Identify tasks that need to be accomplished;*
- *Provides details on resources required to achieve the elements of the plan;*
- *Target milestones to meeting the tasks; and*
- *Track remediation efforts and dates for those milestones.*

STANDARD 9.2: CHANGES AFFECTING THE ASSESSMENT BOUNDARY

A 3PAO-issued attestation and/or certification is invalidated following any material change to the assets and/or processes that make up the OSA's assessment boundary.

Justification: A 3PAO-issued attestation and/or certification is voided when material changes affect the assessment boundary. Only through a reassessment of the changes can a certification be maintained. Reassessing the environment after any material change is crucial because such changes can significantly alter the risk landscape and the effectiveness of existing controls.

Guidance: Proper change management practices must consider the implications of making proposed changes. Therefore, material changes should be coordinated with a 3PAO, where an internal audit should be performed once the changes are implemented and then followed by a 3PAO to conduct 3PAAC Services to validate, or re-issue, an attestation and/or certification.

For example, if a company implements a new data management system or undergoes a significant restructuring, these changes could introduce new vulnerabilities or affect the applicability of current controls. To maintain the validity of an attestation, or certification, a reassessment ensures that all controls remain effective and that the organization continues to meet its cybersecurity and data protection obligations.

STANDARD 9.3: REASSESSMENTS DUE TO MATERIAL CHANGE

As part of a reassessment due to material change, assessors:

1. Must:
    a. Conduct 3PAAC Services consistent with the original assessment's rigor on the assets and/or processes affected by a material change; and
    b. Limit the scope of the reassessment to the assets and/or processes that changed; and
2. May rely on the findings from the most recent, current assessment for unaffected assets and/or processes.

Justification: Engaging a 3PAO to perform a limited assessment for material changes is intended to make 3PAAC Services sustainable from a cost and labor perspective. Conducting a targeted reassessment after material changes ensures that the assessment scope is focused on areas impacted by the changes, optimizing the use of resources and minimizing costs.

Guidance: Per Standard 9, material and non-material changes are defined as:

- *Material Change. A material change to the OSA's cybersecurity and/or data protection program is where the OSA performed a broad scope of significant changes to the OSA's cybersecurity and/or data protection controls.*
- *Non-Material Change. A non-material change to the OSA's cybersecurity and/or data protection program is where the OSA performed a limited scope of minor changes to the OSA's cybersecurity and/or data protection controls.*

A new assessment is required if there are significant architectural or boundary changes to the previous assessment scope. Examples include, but are not limited to:

- *Expansions of networks;*
- *Mergers and Acquisitions (M&A) activities;*
- *Operational changes within assessment boundary(ies) such as new or changed:*
    - *Technology platforms (e.g., OS migration from Windows to Linux);*
    - *ESP integrations; and/or*
    - *Facilities.*

To effectively coordinate reassessments, an OSA should:

- *Conduct pre-change consultation. The OSA should consult with the 3PAO before implementing significant changes to understand potential impacts;*
- *Conduct an internal audit. Once changes are implemented, the OSA should conduct an internal audit to identify any immediate issues or risks introduced by the changes; and*
- *Engage a 3PAO to schedule a reassessment. Based on the internal audit findings, the OSA should engage the 3PAO to perform a targeted reassessment that focuses solely on the affected areas.*

APPENDICES

APPENDIX A: MATERIAL CONTROLS

When a deficiency, or absence, of a specific control poses a material impact, that control is designated as a material control:

- A material control is such a fundamental cybersecurity and/or data protection control that it is not capable of having compensating controls; and
- The absence, or failure, of a material control exposes the organization to such a degree that it could lead to a material impact.

MATERIALITY THRESHOLDS

The SCF Council defines the materiality threshold for an organization's cybersecurity and data protection program as, *"A deficiency, or a combination of deficiencies, in an organization's cybersecurity and/or data protection controls (across its supply chain) where it is probable that reasonable threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance that the organization can adhere to its stated risk tolerance."* [32]

A financial benchmark is commonly used to determine materiality. As an example, from a financial impact perspective, for an item to be considered material, the control deficiency, risk, threat or incident (singular or a combination) should meet one, or more, of the following criteria where the potential financial impact is measured as:[33]

- ≥ 5% of pre-tax income
- ≥ 0.5% of total assets
- ≥ 1% of total equity (shareholder value); and/or
- ≥ 0.5% of total revenue.

KEY CONTROLS

Material controls should be considered key controls. There are many definitions for what a key control means, but it is commonly used within Sarbanes Oxley (SOX) compliance referring to controls that are crucial for maintaining the integrity of an organization's IT General Controls (ITGC). These key controls are designed to mitigate a risk or prevent fraud, where if one (1), or more, key controls fail, it may be difficult to detect or fix problems with other controls.

For organizations that use the term key control as part of their ITGC, it is possible to leverage the SCF's catalog of material controls and perform a crosswalk mapping to see if its key controls match up with possible material controls.

SCF-DESIGNATED MATERIAL CONTROLS

The following are examples of cybersecurity and/or data protection controls that would reasonably be considered material controls to an organization:

SCF Domain	Domain Principle	SCF Control	SCF #	Materiality Justification
Cybersecurity & Data Protection Governance	Execute a documented, risk-based program that supports business objectives while encompassing appropriate cybersecurity and privacy	Cybersecurity & Data Protection Governance Program	GOV-01	OSA does not facilitate the implementation of cybersecurity & data protection governance controls.

[32] *SCF Cybersecurity Materiality - https://securecontrolsframework.com/cybersecurity-materiality/*
[33] *Norwegian Research Council - https://snf.no/media/yemnkmbh/a51_00.pdf*

	principles that address applicable statutory, regulatory and contractual obligations.	Publishing Cybersecurity & Data Protection Documentation	GOV-02	OSA does not establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.
		Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	OSA does not assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.
		Forced Technology Transfer (FTT)	GOV-12	OSA does not avoid and/or constrain the forced exfiltration of sensitive/regulated information (e.g., Intellectual Property (IP)) to the host government for purposes of market access or market management practices.
		State-Sponsored Espionage	GOV-13	OSA does not constrain the host government's ability to leverage the organization's technology assets for economic or political espionage and/or cyberwarfare activities.
Artificial & Autonomous Technologies	Ensure trustworthy and resilient Artificial Intelligence (AI) and autonomous technologies to achieve a beneficial impact by informing, advising or simplifying tasks, while minimizing emergent properties or unintended consequences.	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	OSA does not ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.
		Trustworthy AI & Autonomous Technologies	AAT-01.2	OSA does not ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) are designed to be reliable, safe, fair, secure, resilient, transparent, explainable and data protection-enhanced to minimize emergent properties or unintended consequences.
		AI & Autonomous Technologies Risk Management Decisions	AAT-07	OSA does not leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.
		AI & Autonomous Technologies Likelihood & Impact Risk Analysis	AAT-07.2	OSA does not define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts.
		Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	OSA does not implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related testing, identification of incidents and information sharing.

		AI TEVV Trustworthiness Assessment	AAT-10.1	OSA does not evaluate Artificial Intelligence (AI) and Autonomous Technologies (AAT) for trustworthy behavior and operation including security, anonymization and disaggregation of captured and stored data for approved purposes.
		AI TEVV Safety Demonstration	AAT-10.4	OSA does not demonstrate the Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed are safe, residual risk does not exceed the organization's risk tolerance and can fail safely, particularly if made to operate beyond its knowledge limits.
		AI TEVV Results Evaluation	AAT-10.10	OSA does not evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) to determine the viability of the proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT).
		AI & Autonomous Technologies Intellectual Property Infringement Protections	AAT-12	OSA does not prevent third-party Intellectual Property (IP) rights infringement by Artificial Intelligence (AI) and Autonomous Technologies (AAT).
		Data Source Identification	AAT-12.1	OSA does not identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).
		Data Source Integrity	AAT-12.2	OSA does not protect the integrity of source data to prevent accidental contamination or malicious corruption (e.g., data poisoning) that could compromise the performance of Artificial Intelligence and Autonomous Technologies (AAT).
		AI & Autonomous Technologies Knowledge Limits	AAT-14.2	OSA does not identify and document knowledge limits of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to provide sufficient information to assist relevant stakeholder decision making.
		AI & Autonomous Technologies Viability Decisions	AAT-15	OSA does not define the criteria as to whether Artificial Intelligence (AI) and Autonomous Technologies (AAT) achieved intended purposes and stated objectives to determine whether its development or deployment should proceed.
		Responsibility To Supersede, Deactivate and/or Disengage AI & Autonomous Technologies	AAT-15.2	OSA does not define the criteria and responsible party(ies) for superseding, disengaging or deactivating Artificial Intelligence (AI) and Autonomous Technologies (AAT) that demonstrate performance or outcomes inconsistent with intended use.
		AI & Autonomous Technologies Performance Changes	AAT-16.6	OSA does not evaluate performance improvements or declines with domain experts and relevant stakeholders to define context-relevant risks and trustworthiness issues.

		AI & Autonomous Technologies Harm Prevention	AAT-17	OSA does not proactively prevent harm by regularly identifying and tracking existing, unanticipated and emergent Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.
		AI & Autonomous Technologies Human Subject Protections	AAT-17.1	OSA does not protect human subjects from harm.
		AI & Autonomous Technologies Risk Response	AAT-18.1	OSA does not prioritize, respond to and remediate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks based on assessments and other analytical output.
Asset Management	Manage all technology assets from purchase through disposition, both physical and virtual, to ensure secured use, regardless of the asset's location	Asset Governance	AST-01	OSA does not facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.
		Asset Inventories	AST-02	OSA does not perform inventories of technology assets that: ▪ Accurately reflects the current systems, applications and services in use; ▪ Identifies authorized software products, including business justification details; ▪ Is at the level of granularity deemed necessary for tracking and reporting; ▪ Includes organization-defined information deemed necessary to achieve effective property accountability; and ▪ Is available for review and audit by designated organizational personnel.
		Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	OSA does not maintain network architecture diagrams that: ▪ Contain sufficient detail to assess the security of the network's architecture; ▪ Reflect the current architecture of the network environment; and ▪ Document all sensitive/regulated data flows.
		Secure Disposal, Destruction or Re-Use of Equipment	AST-09	OSA does not securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.
		Use of Personal Devices	AST-12	OSA does not restrict the possession and usage of personally-owned technology devices within organization-controlled facilities.

		Bring Your Own Device (BYOD) Usage	AST-16	OSA does not implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.
Business Continuity & Disaster Recovery	Maintain a resilient capability to sustain business-critical functions while successfully responding to and recovering from incidents through well-documented and exercised processes.	Business Continuity Management System (BCMS)	BCD-01	OSA does not facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).
		Data Backups	BCD-11	OSA does not create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
		AI & Autonomous Technologies Incidents	BCD-16	OSA does not handle failures or incidents with Artificial Intelligence (AI) and Autonomous Technologies (AAT) deemed to be high-risk.
Change Management	Manage change in a sustainable and ongoing manner that involves active participation from both technology and business stakeholders to ensure that only authorized changes occur.	Change Management Program	CHG-01	OSA does not facilitate the implementation of a change management program.
		Prohibition Of Changes	CHG-02.1	OSA does not prohibit unauthorized changes, unless organization-approved change requests are received.
Cloud Security	Govern cloud instances as an extension of on-premise technologies with equal or greater security protections than the organization's own internal cybersecurity and privacy controls.	Cloud Services	CLD-01	OSA does not facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.
		Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	OSA does not control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.
Compliance	Oversee the execution of cybersecurity and privacy controls to ensure appropriate evidence required due care and due diligence exists to meet compliance with applicable statutory, regulatory and contractual obligations.	Statutory, Regulatory & Contractual Compliance	CPL-01	OSA does not facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.
		Compliance Scope	CPL-01.2	OSA does not document and validate the scope of cybersecurity and/or data protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.

		Cybersecurity & Data Protection Controls Oversight	CPL-02	OSA does not provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.
		Cybersecurity & Data Protection Assessments	CPL-03	OSA does not ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate cybersecurity & data protection policies, standards and other applicable requirements.
		Government Surveillance	CPL-06	OSA does not constrain the host government from having unrestricted and non-monitored access to the organization's systems, applications and services that could potentially violate other applicable statutory, regulatory and/or contractual obligations.
Configuration Management	Enforce secure configurations for systems, applications and services according to vendor-recommended and industry-recognized secure practices.	System Hardening Through Baseline Configurations	CFG-02	OSA does not develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.
		Least Functionality	CFG-03	OSA does not configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.
		User-Installed Software	CFG-05	OSA does not restrict the ability of non-privileged users to install unauthorized software.
Continuous Monitoring	Maintain situational awareness of security-related events through the centralized collection and analysis of event logs from systems, applications and services.	Continuous Monitoring	MON-01	OSA does not facilitate the implementation of enterprise-wide monitoring controls.
		Reviews & Updates	MON-01.8	OSA does not review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.
		Centralized Collection of Security Event Logs	MON-02	OSA does not utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.
		Content of Event Logs	MON-03	OSA does not configure systems to produce event logs that contain sufficient information to, at a minimum: ▪ Establish what type of event occurred; ▪ When (date and time) the event occurred; ▪ Where the event occurred;

				▪ The source of the event; ▪ The outcome (success or failure) of the event; and ▪ The identity of any user/subject associated with the event.
		Audit Trails	MON-03.2	OSA does not link system access to individual users or service accounts.
		Time Stamps	MON-07	OSA does not configure systems to use an authoritative time source to generate time stamps for event logs.
		Protection of Event Logs	MON-08	OSA does not protect event logs and audit tools from unauthorized access, modification and deletion.
		Event Log Retention	MON-10	OSA does not retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.
		Anomalous Behavior	MON-16	OSA does not detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.
Cryptographic Protections	Utilize appropriate cryptographic solutions and industry-recognized key management practices to protect the confidentiality and integrity of sensitive/regulated data both at rest and in transit.	Use of Cryptographic Controls	CRY-01	OSA does not facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.
		Transmission Confidentiality	CRY-03	Cryptographic mechanisms do not exist that would protect the confidentiality of data being transmitted.
		Transmission Integrity	CRY-04	Cryptographic mechanisms do not exist that would protect the integrity of data being transmitted.
		Encrypting Data At Rest	CRY-05	Cryptographic mechanisms do not exist that would prevent unauthorized disclosure of data at rest.

		Cryptographic Key Management	CRY-09	OSA does not facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.
Data Classification & Handling	Enforce a standardized data classification methodology to objectively determine the sensitivity and criticality of all data and technology assets so that proper handling and disposal requirements can be followed.	Data Protection	DCH-01	OSA does not facilitate the implementation of data protection controls.
		Data Stewardship	DCH-01.1	OSA does not ensure data stewardship is assigned, documented and communicated.
		Data & Asset Classification	DCH-02	OSA does not ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.
		Disclosure of Information	DCH-03.1	OSA does not restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.
		Physical Media Disposal	DCH-08	OSA does not securely dispose of media when it is no longer required, using formal procedures.
		System Media Sanitization	DCH-09	OSA does not sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.
		Limitations on Use	DCH-10.1	OSA does not restrict the use and distribution of sensitive/regulated data.
		Removable Media Security	DCH-12	OSA does not restrict removable media in accordance with data handling and acceptable usage parameters.
		Protecting Sensitive Data on External Systems	DCH-13.3	OSA does not ensure that the requirements for the protection of sensitive information processed, stored or transmitted on external systems, are implemented in accordance with applicable statutory, regulatory and contractual obligations.

		Publicly Accessible Content	DCH-15	OSA does not control publicly-accessible content.
		Information Disposal	DCH-21	OSA does not securely dispose of, destroy or erase information.
		Information Location	DCH-24	OSA does not identify and document the location of information and the specific system components on which the information resides.
		Transfer of Sensitive and/or Regulated Data	DCH-25	OSA does not restrict and govern the transfer of sensitive and/or regulated data to third-countries or international organizations.
		Data Localization	DCH-26	OSA does not constrain the impact of "digital sovereignty laws," that require localized data within the host country, where data and processes may be subjected to arbitrary enforcement actions that potentially violate other applicable statutory, regulatory and/or contractual obligations.
Embedded Technology	Provide additional scrutiny to reduce the risks associated with embedded technology, based on the potential damages posed from malicious use of the technology.	Embedded Technology Security Program	EMB-01	OSA does not facilitate the implementation of embedded technology controls.
Endpoint Security	Harden endpoint devices to protect against reasonable threats to those devices and the data those devices store, transmit and process.	Endpoint Security	END-01	OSA does not facilitate the implementation of endpoint security controls.
		Malicious Code Protection (Anti-Malware)	END-04	OSA does not utilize antimalware technologies to detect and eradicate malicious code.
		Phishing & Spam Protection	END-08	OSA does not utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.
Human Resources Security	Execute sound hiring practices and ongoing personnel management to cultivate a cybersecurity and privacy-minded workforce.	Human Resources Security Management	HRS-01	OSA does not facilitate the implementation of personnel security controls.

		Users With Elevated Privileges	HRS-02.1	OSA does not ensure that every user accessing a system that processes, stores, or transmits sensitive information is cleared and regularly trained to handle the information in question.
		Defined Roles & Responsibilities	HRS-03	OSA does not define cybersecurity roles & responsibilities for all personnel.
		Personnel Screening	HRS-04	OSA does not manage personnel security risk by screening individuals prior to authorizing access.
		Terms of Employment	HRS-05	OSA does not require all employees and contractors to apply cybersecurity and/or data protection principles in their daily work.
		Rules of Behavior	HRS-05.1	OSA does not define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.
		Use of Communications Technology	HRS-05.3	OSA does not establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.
		Access Agreements	HRS-06	OSA does not require internal and third-party users to sign appropriate access agreements prior to being granted access.
		Confidentiality Agreements	HRS-06.1	OSA does not require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.
		Third-Party Personnel Security	HRS-10	OSA does not govern third-party personnel by reviewing and monitoring third-party cybersecurity and/or data protection roles and responsibilities.
Identification & Authentication	Enforce the concept of "least privilege" consistently across all systems, applications and services for individual, group and service accounts	Identity & Access Management (IAM)	IAC-01	OSA does not facilitate the implementation of identification and access management controls.

	through a documented and standardized Identity and Access Management (IAM) capability.	User & Service Account Inventories	IAC-01.3	Automated mechanisms do not exist that would maintain a current list of authorized users and service accounts.
		User Provisioning & De-Provisioning	IAC-07	OSA does not utilize a formal user registration and de-registration process that governs the assignment of access rights.
		Change of Roles & Duties	IAC-07.1	OSA does not revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.
		Termination of Employment	IAC-07.2	OSA does not revoke user access rights in a timely manner, upon termination of employment or contract.
		Authenticator Management	IAC-10	OSA does not securely manage authenticators for users and devices.
		Protection of Authenticators	IAC-10.5	OSA does not protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.
		No Embedded Unencrypted Static Authenticators	IAC-10.6	OSA does not ensure that unencrypted, static authenticators are not embedded in applications, scripts or stored on function keys.
		Default Authenticators	IAC-10.8	OSA does not ensure default authenticators are changed as part of account creation or system installation.
		Account Management	IAC-15	OSA does not proactively govern account management of individual, group, system, service, application, guest and temporary accounts.
		Disable Inactive Accounts	IAC-15.3	Automated mechanisms do not exist that would disable inactive accounts after an organization-defined time period.

		Restrictions on Shared Groups/Accounts	IAC-15.5	OSA does not authorize the use of shared/group accounts only under certain organization-defined conditions.
		Account Disabling for High Risk Individuals	IAC-15.6	OSA does not disable accounts immediately upon notification for users posing a significant risk to the organization.
		System Account Reviews	IAC-15.7	OSA does not review all system accounts and disable any account that cannot be associated with a business process and owner.
		Privileged Account Management (PAM)	IAC-16	OSA does not restrict and control privileged access rights for users and services.
		Privileged Account Inventories	IAC-16.1	OSA does not inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational management.
		Periodic Review of Account Privileges	IAC-17	OSA does not periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.
		User Responsibilities for Account Management	IAC-18	OSA does not compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards, certificates, etc.).
		Credential Sharing	IAC-19	OSA does not prevent the sharing of generic IDs, passwords or other generic authentication methods.
		Access Enforcement	IAC-20	OSA does not enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."
		Access To Sensitive/Regulated Data	IAC-20.1	OSA does not limit access to sensitive/regulated data to only those individuals whose job requires such access.

		Database Access	IAC-20.2	OSA does not restrict access to databases containing sensitive/regulated data to only necessary services or those individuals whose job requires such access.
		Least Privilege	IAC-21	OSA does not utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.
		Privileged Accounts	IAC-21.3	OSA does not restrict the assignment of privileged accounts to management-approved personnel and/or roles.
		Identity Proofing (Identity Verification)	IAC-28	OSA does not verify the identity of a user before issuing authenticators or modifying access permissions.
		Management Approval For New or Changed Accounts	IAC-28.1	OSA does not ensure management approvals are required for new accounts or changes in permissions to existing accounts.
Incident Response	Maintain a viable incident response capability that trains personnel on how to recognize and report suspicious activities so that trained incident responders can take the appropriate steps to handle incidents, in accordance with a documented Incident Response Plan (IRP).	Incident Handling	IRO-02	OSA does not cover: ▪ Preparation; ▪ Automated detection or intake of incident reports; ▪ Analysis; ▪ Containment; ▪ Eradication; and ▪ Recovery.
Information Assurance	Execute an impartial assessment process to validate the existence and functionality of appropriate cybersecurity and privacy controls, prior to a system, application or service being used in a production environment.	Information Assurance (IA) Operations	IAO-01	OSA does not facilitate the implementation of cybersecurity and/or data protection assessment and authorization controls.
		Assessments	IAO-02	OSA does not formally assess the cybersecurity and/or data protection controls in systems, applications and services through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.

		Threat Analysis & Flaw Remediation During Development	IAO-04	OSA does not require system developers and integrators to create and execute a Security Test and Evaluation (ST&E) plan to identify and remediate flaws during development.
		Security Authorization	IAO-07	OSA does not ensure systems, projects and services are officially authorized prior to "go live" in a production environment.
Maintenance	Proactively maintain technology assets, according to current vendor recommendations for configurations and updates, including those supported or hosted by third-parties.	Controlled Maintenance	MNT-02	OSA does not conduct controlled maintenance activities throughout the lifecycle of the system, application or service.
Mobile Device Management	Implement measures to restrict mobile device connectivity with critical infrastructure and sensitive/regulated data that limit the attack surface and potential data exposure from mobile device usage.	Centralized Management Of Mobile Devices	MDM-01	OSA does not implement and govern Mobile Device Management (MDM) controls.
Network Security	Architect and implement a secure and resilient defense-in-depth methodology that enforces the concept of “least functionality” through restricting network access to systems, applications and services.	Network Security Controls (NSC)	NET-01	OSA does not develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).
		Boundary Protection	NET-03	OSA does not monitor and control communications at the external network boundary and at key internal boundaries within the network.
		Data Flow Enforcement - Access Control Lists (ACLs)	NET-04	OSA does not implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.
		Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	OSA does not configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).
		Network Segmentation (macrosegementation)	NET-06	OSA does not ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.
		Sensitive/Regulated Data Enclave (Secure Zone)	NET-06.3	OSA does not implement segmentation controls to restrict inbound and outbound connectivity for sensitive/regulated data enclaves (secure zones).

		Domain Name Service (DNS) Resolution	NET-10	OSA does not ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name/address resolution.
		Electronic Messaging	NET-13	OSA does not protect the confidentiality, integrity and availability of electronic messaging communications.
		Remote Access	NET-14	OSA does not define, control and review organization-approved, secure remote access methods.
		Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	OSA does not define secure telecommuting practices and govern remote access to systems and data for remote workers.
		Email Content Protections	NET-20	OSA does not implement an email filtering security service to detect malicious attachments in emails and prevent users from accessing them.
Physical & Environmental Security	Protect physical environments through layers of physical security and environmental controls that work together to protect both physical and digital assets from theft and damage.	Physical Access Control	PES-03	Physical access control mechanisms do not exist that would enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).
		Physical Security of Offices, Rooms & Facilities	PES-04	OSA does not identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.
		Working in Secure Areas	PES-04.1	Physical security mechanisms do not exist that would allow only authorized personnel access to secure areas.
		Restrict Unescorted Access	PES-06.3	Physical access control mechanisms do not exist that would restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.
Data Privacy	Align data privacy practices with industry-recognized privacy principles to implement appropriate administrative, technical and	Data Privacy Program	PRI-01	OSA does not facilitate the implementation and operation of data privacy controls.

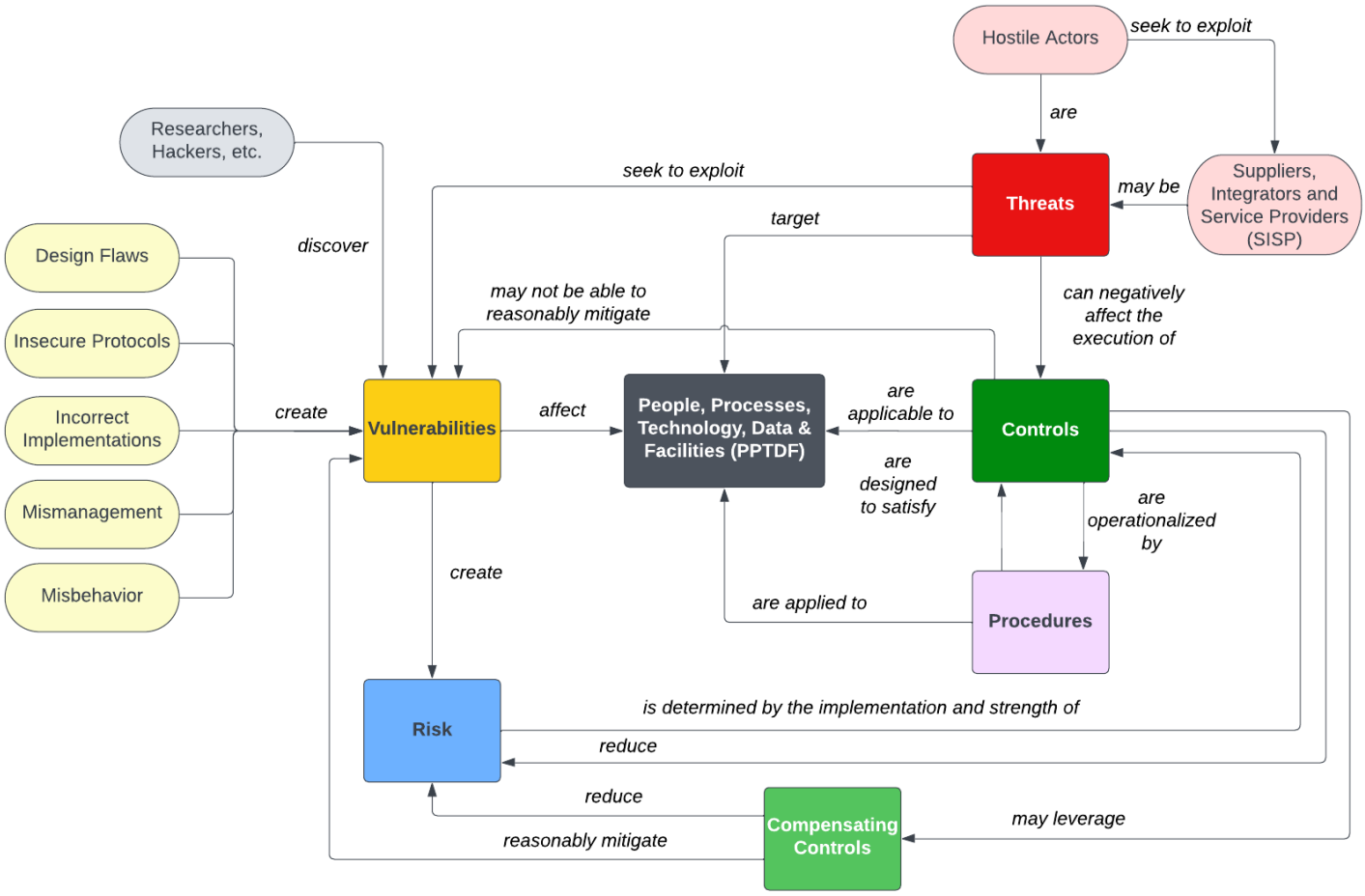
	physical controls to protect regulated personal data throughout the lifecycle of systems, applications and services.	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	OSA does not include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.
		Potential Human Rights Abuses	PRI-16	OSA does not constrain the supply of physical and/or digital activity logs to the host government that can directly lead to contravention of the Universal Declaration of Human Rights (UDHR), as well as other applicable statutory, regulatory and/or contractual obligations.
Project & Resource Management	Operationalize a viable strategy to achieve cybersecurity and/or data protection objectives that establishes cybersecurity as a key stakeholder within project management practices to ensure the delivery of resilient and secure solutions.	Cybersecurity & Data Privacy In Project Management	PRM-04	OSA does not assess cybersecurity and/or data protection controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.
		Secure Development Life Cycle (SDLC) Management	PRM-07	OSA does not ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.
Risk Management	Proactively identify, assess, prioritize and remediate risk through alignment with industry-recognized risk management principles to ensure risk decisions adhere to the organization's risk threshold.	Risk Management Program	RSK-01	OSA does not facilitate the implementation of strategic, operational and tactical risk management controls.
		Risk Assessment	RSK-04	OSA does not conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.
		Risk Register	RSK-04.1	OSA does not maintain a risk register that facilitates monitoring and reporting of risks.
		Risk Remediation	RSK-06	OSA does not remediate risks to an acceptable level.
		Supply Chain Risk Management (SCRM) Plan	RSK-09	OSA does not develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.

Secure Engineering & Architecture	Utilize industry-recognized secure engineering and architecture principles to deliver secure and resilient systems, applications and services.	Secure Engineering Principles	SEA-01	OSA does not facilitate the implementation of industry-recognized cybersecurity and/or data protection practices in the specification, design, development, implementation and modification of systems and services.
		Defense-In-Depth (DiD) Architecture	SEA-03	OSA does not implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.
Technology Development & Acquisition	Develop and test systems, applications or services according to a Secure Software Development Framework (SSDF) to reduce the potential impact of undetected or unaddressed vulnerabilities and design weaknesses.	Technology Development & Acquisition	TDA-01	OSA does not facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.
		Product Management	TDA-01.1	OSA does not design and implement product management processes to update products, including systems, software and services, to improve functionality and correct security deficiencies.
		Cybersecurity & Data Privacy Representatives For Product Changes	TDA-02.7	OSA does not include appropriate cybersecurity and/or data protection representatives in the product feature and/or functionality change control review process.
		Secure Coding	TDA-06	OSA does not develop applications based on secure coding principles.
		Software Design Review	TDA-06.5	OSA does not have an independent review of the software design to confirm that all cybersecurity and/or data protection requirements are met and that any identified risks are satisfactorily addressed.
		Separation of Development, Testing and Operational Environments	TDA-08	OSA does not manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production systems.
		Unsupported Systems	TDA-17	OSA does not prevent unsupported systems by: ▪ Replacing systems when support for the components is no longer available from the developer, vendor or manufacturer; and ▪ Requiring justification and documented approval for the continued use of unsupported system components required to satisfy mission/business needs.

Third-Party Management	Execute Supply Chain Risk Management (SCRM) practices so that only trustworthy third-parties are used for products and/or service delivery.	Third-Party Management	TPM-01	OSA does not facilitate the implementation of third-party management controls.
		Third-Party Services	TPM-04	OSA does not mitigate the risks associated with third-party access to the organization's systems and data.
		Third-Party Processing, Storage and Service Locations	TPM-04.4	OSA does not restrict the location of information processing/storage based on business requirements.
		Third-Party Contract Requirements	TPM-05	OSA does not require contractual requirements for cybersecurity and/or data protection requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.
		Third-Party Scope Review	TPM-05.5	OSA does not perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity and/or data protection control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.
Vulnerability & Patch Management	Leverage industry-recognized Attack Surface Management (ASM) practices to strengthen the security and resilience systems, applications and services against evolving and sophisticated attack vectors.	Vulnerability Remediation Process	VPM-02	OSA does not ensure that vulnerabilities are properly identified, tracked and remediated.
		Software & Firmware Patching	VPM-05	OSA does not conduct software patching for all deployed operating systems, applications and firmware.
Web Security	Ensure the security and resilience of Internet-facing technologies through secure configuration management practices and monitoring for anomalous activity.	Client-Facing Web Services	WEB-04	OSA does not deploy reasonably-expected security controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.

APPENDIX B: RISK TERMINOLOGY NORMALIZATION

Threat, vulnerability and risk management practices are meant to achieve a minimum level of protection - this equates to a reduction in the total risk due to the protections offered by implemented controls. These ecosystem components have unique meanings that need to be understood to reasonably protect people, processes, technology and data. Understanding the context of how these components integrate can lead to more meaningful and practical risk management practices.



As it pertains to the CDPAS:

- Risk Appetite: *the types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value.* [34]
- Risk Tolerance: *the level of risk an entity is willing to assume in order to achieve a potential desired result.* [35]
- Risk Threshold: *values used to establish concrete decision points and operational control limits to trigger management action and response escalation.* [36]

RISK APPETITE

A risk appetite is a broad "risk management concept" used to inform employees about what is and is not acceptable, regarding risk management from an organization's executive leadership team. A risk appetite does not contain granular risk management criteria and is primarily a "management statement" that is subjective. Similar in concept to how a policy is a *"high-level statement of management intent,"* an organization's defined risk appetite is a high-level statement of how all, or certain types of, risk are willing to be accepted. [37]

---

[34] *NIST Glossary for Risk Appetite - https://csrc.nist.gov/glossary/term/risk_appetite*
[35] *NIST Glossary for Risk Tolerance - https://csrc.nist.gov/glossary/term/risk_tolerance*
[36] *NIST Glossary for Thresholds - https://csrc.nist.gov/glossary/term/thresholds*
[37] *ComplianceForge Hierarchical Cybersecurity Governance Framework (HCGF) - https://content.complianceforge.com/Hierarchical-Cybersecurity-Governance-Framework.pdf*

Examples of an organization stating its risk appetite from basic to more complex statements:

- *"[organization name] is a low-risk organization and will avoid any activities that could harm its customers."*
- *"[organization name] will aggressively pursue innovative solutions through Research & Development (R&D) to provide industry-leading products and services to our clients, while maintaining a Moderate Risk Appetite. Developing breakthrough products and services does invite potential risk through changes to traditional supply chains, disruptions to business operations and changing client demand. Proposed business practices that pose greater than a Moderate Risk will be considered on a case-by-case basis for financial, operational and legal implications."*

It is important to point out that in many immature risk programs, risk appetite statements are divorced from reality. Executive leaders mean well when they issue risk appetite statements, but the Business As Usual (BAU) practices routinely violate the risk appetite. This is often due to numerous reasons that include, but are not limited to:

- Technical debt;
- Dysfunctional management decisions;
- Insecure practices;
- Inadequate funding/resourcing;
- Improperly scoped support contracts (e.g., Managed Service Providers (MSPs), consultants, vendors, etc.); and
- Lack of pre-production security testing.

RISK TOLERANCE

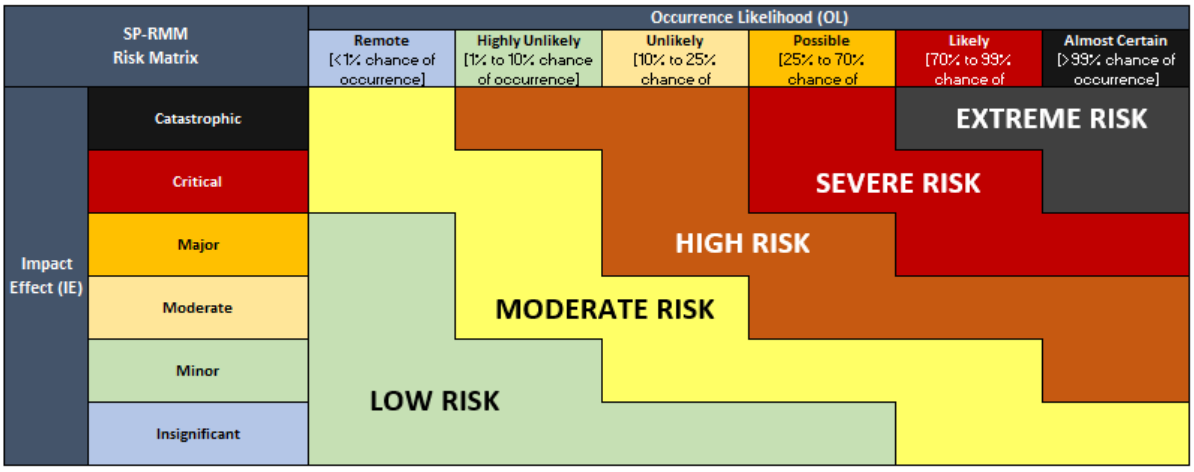
Risk tolerance is based on objective criteria, unlike the subjective, conceptual nature of a risk appetite. Defining objective criteria is a necessary step to categorize risk on a graduated scale. Establishing objective criteria to quantify the impact of risk enables risk assessments to leverage those same criteria and assist decision-makers in their risk management decisions (e.g., accept, mitigate, transfer or avoid).

From a graduated scale perspective, it is possible to define "tolerable" risk criteria to create five (5) useful categories of risk:

1. Low Risk;
2. Moderate Risk;
3. High Risk;
4. Severe Risk; and
5. Extreme Risk.

There are two (2) objective criteria that go into defining what constitutes a low, moderate, high, severe or Extreme Risk includes:

1. Impact Effect (IE); and
2. Occurrence Likelihood (OL).



The six (6) categories of IE are:

1. Insignificant *(e.g., organization-defined little-to-no impact to business operations);*
2. Minor *(e.g., organization-defined minor impacts to business operations)*;

3. Moderate *(e.g., organization-defined moderate impacts to business operations)*;
4. Major *(e.g., organization-defined major impacts to business operations)*;
5. Critical *(e.g., organization-defined critical impacts to business operations)*; and
6. Catastrophic *(e.g., organization-defined catastrophic impacts to business operations).*

The six (6) categories of OL are:

1. Remote possibility *(e.g., <1% chance of occurrence)*;
2. Highly unlikely *(e.g., from 1% to 10% chance of occurrence)*;
3. Unlikely *(e.g., from 10% to 25% chance of occurrence)*;
4. Possible *(e.g., from 25% to 70% chance of occurrence)*;
5. Likely *(e.g., from 70% to 99% chance of occurrence)*; and
6. Almost certain *(e.g., >99% chance of occurrence)*.

There are three (3) general approaches are commonly employed to estimate OL:

1. Relevant historical data;
2. Probability forecasts; and
3. Expert opinion.

An organization's risk tolerance is influenced by several factors that includes, but is not limited to:

- Statutory, regulatory and contractual compliance obligations (including adherence to privacy principles for ethical data protection practices).
- Organization-specific threats (natural and manmade).
- Reasonably expected industry practices.
- Pressure from competition.
- Executive management decisions.

Low Risk Tolerance

Organizations that would be reasonably expected to adopt a Low Risk Tolerance generally:

- Provide products and/or services necessary for the population to maintain normalcy in daily life.
- Are in highly regulated industries with explicit cybersecurity and/or data protection requirements.
- Store, process and/or transmit highly sensitive and/or regulated data.
- Are legitimate targets for nation-state actors to disrupt and/or compromise due to the high-value nature of the organization.
- Have strong executive management support for cybersecurity and data protection practices as part of “business as usual” activities.
- Maintain a high capability maturity level for preventative cybersecurity controls to implement “defense in depth” protections across the enterprise.
- Have a high level of situational awareness (cybersecurity & physical) that includes its supply chain.
- Have cyber-related liability insurance.

Organizations that are reasonably expected to operate with a Low Risk Tolerance include, but are not limited to:

- Critical infrastructure
- Utilities (e.g., electricity, drinking water, natural gas, sanitation, etc.)
- Telecommunications (e.g., Internet Service Providers (ISPs), mobile phone carriers, Cloud Service Providers (CSPs), etc.) (high value)
- Transportation (e.g., airports, railways, ports, tunnels, fuel delivery, etc.)
- Technology Research & Development (R&D) (high value)
- Healthcare (high value)
- Government institutions:
    - Military
    - Law enforcement
    - Judicial system
    - Financial services (high value)
    - Defense Industrial Base (DIB) contractors (high value)

Moderate Risk Tolerance

Organizations that would be reasonably expected to adopt a Moderate Risk Tolerance generally:

- Have executive management support for securing sensitive and/or regulated data enclaves.
- Are in regulated industries that have specific cybersecurity and/or data protection requirements (e.g., CMMC, PCI DSS, SOX, GLBA, RMF, etc.).
- Have "flow down" requirements from customers that require adherence to specific cybersecurity and/or data protection requirements.
- Store, process and/or transmit sensitive and/or regulated data.
- Are legitimate targets for attackers who wish to financially benefit from stolen information or ransom.
- Have cyber-related liability insurance.

Organizations that are reasonably expected to operate with a Moderate Risk Tolerance include, but are not limited to:

- Education (e.g., K-12, colleges, universities, etc.)
- Utilities (e.g., electricity, drinking water, natural gas, sanitation, etc.)
- Telecommunications (e.g., Internet Service Providers (ISPs), mobile phone carriers, etc.)
- Transportation (e.g., airports, railways, ports, tunnels, fuel delivery, etc.)
- Technology services (e.g., Managed Service Providers (MSPs), Managed Security Service Providers (MSSPs), etc.)
- Manufacturing (high value)
- Healthcare
- Defense Industrial Base (DIB) contractors and subcontractors
- Legal services (e.g., law firms)
- Construction (high value)

High Risk Tolerance

Organizations that would be reasonably expected to adopt a High Risk Tolerance generally:

- Are in an unregulated industry, regarding cybersecurity and/or data protection requirements.
- Do not store, process and/or transmit sensitive and/or regulated data.
- Lack management support for cybersecurity and data protection governance practices.
- Do not have cyber-related liability insurance.

Organizations that may choose to operate with a High Risk Tolerance include, but are not limited to:

- Startups
- Hospitality industry (e.g., restaurants, hotels, etc.)
- Construction
- Manufacturing
- Personal services

Severe Risk Tolerance

Organizations that would be reasonably expected to adopt a Severe Risk Tolerance generally:

- Are in an unregulated industry, regarding cybersecurity and/or data protection requirements.
- Do not store, process and/or transmit sensitive and/or regulated data.
- Lack management support for cybersecurity and data protection governance practices.
- Do not have cyber-related liability insurance.

Organizations that may choose to operate with a Severe Risk Tolerance include, but are not limited to:

- Startups
- Artificial Intelligence (AI) developers

Extreme Risk Tolerance

Organizations that would be reasonably expected to adopt an Extreme Risk Tolerance generally:

- Are in an unregulated industry, regarding cybersecurity and/or data protection requirements.
- Do not store, process and/or transmit sensitive and/or regulated data.
- Lack management support for cybersecurity and data protection governance practices.
- Do not have cyber-related liability insurance.

Organizations that may choose to operate with an Extreme Risk Tolerance include, but are not limited to:

- Startups
- Artificial Intelligence (AI) developers

RISK THRESHOLD

Risk thresholds are directly tied to risk tolerance and utilize organization-specific criteria (e.g., acceptable and unacceptable parameters). These risk thresholds exist between the risk tolerance levels (e.g., between Low Risk and Moderate Risk, between Moderate Risk and High Risk, etc.). Establishing these risk thresholds brings the "graduated scale perspective" to life for risk management practices. Risk thresholds are criteria that are unique to an organization, where organization-specific activities/scenarios could:

- Damage the organization's reputation;
- Negatively affect short-term and long-term profitability; and/or
- Impede business operations.

Risk thresholds are unique to each organization, based on several factors that include:

- Financial stability;
- Management preferences;
- Compliance obligations (e.g., statutory, regulatory and/or contractual); and
- Insurance coverage limits.

APPENDIX C: ASSESSMENT RIGOR

The CDPAS' assessment rigor is based on assessment methods described in NIST SP 800-172A Appendix C.[38] There are three (3) levels of rigor:

1. Standard;
2. Enhanced; and
3. Comprehensive.

The definition of each assessment method includes types of objects to which the method can be applied. In addition, the application of each method is described in terms of the attributes of depth and coverage.

- The depth attribute addresses the rigor and level of detail of the assessment.
- The coverage attribute addresses the scope or breadth of the assessment.

LEVEL 1 RIGOR: STANDARD

Standard rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether the applicable controls are:

1. Implemented; and
2. Free of obvious errors.

Standard rigor represents sufficient due care in the evaluation of cybersecurity and/or data protection controls. Standard rigor is appropriate for the Manual Point In Time (MPIT) assessment methodology that:

1. Is relevant to a specific point in time (time at which the controls were evaluated); and
2. Relies on the manual review of artifacts to derive a finding;

<table>
<tr><th colspan="2">STANDARD
Assessment Rigor</th><th>EXAMINE</th><th>INTERVIEW</th><th>TEST</th></tr>
<tr><td colspan="2">Assessment Method</td><td>The process of checking, inspecting, reviewing, observing, studying or analyzing one or more assessment objects to facilitate understanding, achieve clarification or obtain evidence.</td><td>The process of conducting discussions with individuals or groups in an organization to facilitate understanding, achieve clarification or lead to the location of evidence.</td><td>The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior.</td></tr>
<tr><td colspan="2">Assessment Results</td><td colspan="3">Results from examination, interviews and testing are used to support the determination of:
Security safeguard existence;
Functionality;
Correctness;
Completeness; and
Potential for improvement over time.
Standard rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether the applicable controls are:
Implemented; and
Free of obvious errors.</td></tr>
<tr><td rowspan="2">Attributes</td><td>Assessment Depth</td><td>An examination that consists of high-level reviews, checks, observations or inspections of the assessment object.

This type of examination is conducted using a limited</td><td>An interview that consists of broad-based, high-level discussions with individuals or groups of individuals.

This type of interview is conducted using a set of</td><td>A test methodology assumes no knowledge of the internal structure and implementation detail of the assessment object. This methodology is also referred to as "black box" testing.</td></tr>
</table>

[38] *NIST SP 800-172A - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172A.pdf*

		body of evidence or documentation including: ▪ Functional-level descriptions for mechanisms; ▪ High-level process descriptions for activities; and ▪ Documents for specifications.	generalized, high-level questions.	This type of testing is conducted using: ▪ A functional specification for mechanisms; and A high-level process description for activities.
Assessment Objects	Specifications	Review: ▪ Policies; ▪ Plans; ▪ Procedures; ▪ System requirements; and ▪ Designs.	N/A	N/A
	Mechanisms	Review configurations and/or functionality implemented in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.	N/A	Test functionality in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.
	Activities	Review procedures associated with: ▪ Designs; ▪ System operations; ▪ Administration; ▪ Management; and/or ▪ Exercises.	N/A	Test applicable procedures for: ▪ System operations; ▪ Administrative activities; ▪ Management functions; and ▪ Exercises (e.g., incident response, business continuity, security awareness, etc.).
	Individuals or Groups	N/A	Conduct interviews with applicable stakeholders associated with control execution and/or oversight. Interviews should focus on people and/or teams with RASCI-assigned roles and responsibilities: ▪ Responsible - People directly responsible for performing a task (e.g., control/process operator); ▪ Accountable - Person overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ Supportive - People under the coordination of the Responsible person for support in performing the task; ▪ Consulted - People not directly involved in task	N/A

			execution but were consulted for subject matter expertise; and ▪ Informed - People not involved in task execution but are informed when the task is completed.	

LEVEL 2 RIGOR: ENHANCED

Enhanced rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether:

1. The applicable controls are:
    a. Implemented; and
    b. Free of obvious/apparent errors; and
2. There are increased grounds for confidence that the applicable controls are:
    a. Implemented correctly; and
    b. Operating as intended.

Enhanced rigor is appropriate for the Automated Point In Time (APIT) assessment methodology that utilizes automation to augment a traditional assessment methodology, where AAT is used to compare the desired state of conformity versus the current state via machine-readable configurations and/or assessment evidence:

1. Is relevant to a specific point in time (time at which the controls were evaluated);
2. In situations where technology cannot evaluate evidence, evidence is manually reviewed; and
3. The combined output of automated and manual reviews of artifacts is used to derive a finding.

<table>
<tr><th colspan="2">ENHANCED
Assessment Rigor</th><th>EXAMINE</th><th>INTERVIEW</th><th>TEST</th></tr>
<tr><td colspan="2">Assessment Method</td><td>The process of checking, inspecting, reviewing, observing, studying or analyzing one or more assessment objects to facilitate understanding, achieve clarification or obtain evidence.</td><td>The process of conducting discussions with individuals or groups in an organization to facilitate understanding, achieve clarification or lead to the location of evidence.</td><td>The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior.</td></tr>
<tr><td colspan="2">Assessment Results</td><td colspan="3">Results from examination, interviews and testing are used to support the determination of:
Security safeguard existence;
Functionality;
Correctness;
Completeness; and
Potential for improvement over time.
Enhanced rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether:
The applicable controls are:<ol type="a">
Implemented; and
Free of obvious/apparent errors; and
There are increased grounds for confidence that the applicable controls are:<ol type="a">
Implemented correctly; and
Operating as intended.</td></tr>
<tr><td rowspan="2">Attributes</td><td>Assessment Depth</td><td>An examination that consists of high-level reviews, checks, observations or inspections and more in-depth studies and analyses of the assessment object. This type of examination is conducted using a substantial body of evidence or documentation.

Examples include:
Functional-level descriptions and where appropriate and available, high-level design</td><td>An interview that consists of broad-based, high-level discussions and more in-depth discussions in specific areas with individuals or groups of individuals.

This type of interview is conducted using:
A set of generalized, high-level questions; and
More in-depth questions in specific areas where responses indicate a need</td><td>A test methodology assumes some knowledge of the internal structure and implementation detail of the assessment object. This methodology is also referred to as “gray box” testing.

This type of testing is conducted using:
A functional specification and limited system architectural information (e.g., high-level design) for mechanisms and a high-</td></tr>
</table>

		information for mechanisms; ▪ High-level process descriptions and implementation procedures for activities; and ▪ Documents and related documents for specifications.	for more in-depth investigation.	level process description; and ▪ A high-level description of integration into the operational environment for activities.
Assessment Objects	Specifications	Review: ▪ Policies; ▪ Plans; ▪ Procedures; ▪ System requirements; and ▪ Designs.	N/A	N/A
	Mechanisms	Review configurations and/or functionality implemented in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.	N/A	Test functionality in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.
	Activities	Review procedures associated with: ▪ Designs; ▪ System operations; ▪ Administration; ▪ Management; and/or ▪ Exercises.	N/A	Test applicable procedures for: ▪ System operations; ▪ Administrative activities; ▪ Management functions; and ▪ Exercises (e.g., incident response, business continuity, security awareness, etc.).
	Individuals or Groups	N/A	Conduct interviews with applicable stakeholders associated with control execution and/or oversight. Interviews should focus on people and/or teams with RASCI-assigned roles and responsibilities: ▪ Responsible - People directly responsible for performing a task (e.g., control/process operator); ▪ Accountable - Person overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ Supportive - People under the coordination of the Responsible person for support in performing the task; ▪ Consulted - People not directly involved in task	N/A

			execution but were consulted for subject matter expertise; and ▪ Informed - People not involved in task execution but are informed when the task is completed.	

LEVEL 3 RIGOR: COMPREHENSIVE

Comprehensive rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining:

1. Whether the applicable controls are:
    a. Implemented; and
    b. Free of obvious/apparent errors;
2. Whether there are further increased grounds for confidence that the applicable controls are:
    a. Implemented correctly; and
    b. Operating as intended on an ongoing and consistent basis; and
3. There is support for continuous improvement in the effectiveness of the applicable controls.

Comprehensive rigor is appropriate for the Automated Evidence with Human Review (AEHR) assessment methodology that is used for ongoing, continuous control assessments:

1. AAT continuously evaluates controls by comparing the desired state of conformity versus the current state through machine-readable configurations and/or assessment evidence; and
2. Recurring human reviews:
    a. Evaluate the legitimacy of the results from automated control assessments; and
    b. Validate the automated evidence review process to derive a finding.

<table>
<tr><th colspan="2">COMPREHENSIVE
Assessment Rigor</th><th>EXAMINE</th><th>INTERVIEW</th><th>TEST</th></tr>
<tr><td colspan="2">Assessment Method</td><td>The process of checking, inspecting, reviewing, observing, studying or analyzing one or more assessment objects to facilitate understanding, achieve clarification or obtain evidence.</td><td>The process of conducting discussions with individuals or groups in an organization to facilitate understanding, achieve clarification or lead to the location of evidence.</td><td>The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior.</td></tr>
<tr><td colspan="2">Assessment Results</td><td colspan="3">Results from examination, interviews and testing are used to support the determination of:
Security safeguard existence;
Functionality;
Correctness;
Completeness; and
Potential for improvement over time.
Comprehensive rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining:
Whether the applicable controls are:<ol type="a">
Implemented; and
Free of obvious/apparent errors;
Whether there are further increased grounds for confidence that the applicable controls are:<ol type="a">
Implemented correctly; and
Operating as intended on an ongoing and consistent basis; and
There is support for continuous improvement in the effectiveness of the applicable controls.</td></tr>
<tr><td rowspan="2">Attributes</td><td>Assessment Depth</td><td>An examination that consists of high-level reviews, checks, observations or inspections and more in-depth, detailed and thorough studies and analyses of the assessment object.

This type of examination is conducted using an extensive body of evidence or documentation including:</td><td>An interview that consists of broad-based, high-level discussions and more in-depth, probing discussions in specific areas with individuals or groups of individuals.

This type of interview is conducted using:
A set of generalized, high-level questions; and</td><td>Test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. This methodology is also referred to as “white box” testing.

This type of testing is conducted using:
A functional specification;</td></tr>
</table>

		▪ Functional-level descriptions and where appropriate and available:
		  ○ High- level design information;
		  ○ Low-level design information; and
		  ○ Implementation information for mechanisms;
		▪ High-level process descriptions and detailed implementation procedures for activities; and
		▪ Documents and related documents for specifications.
			▪ More in-depth, probing questions in specific areas where responses indicate a need for more in-depth investigation.	▪ Extensive system architectural information (e.g., high-level design, low-level design);
				▪ Implementation representation (e.g., source code, schematics) for mechanisms;
				▪ A high-level process description; and
				▪ A detailed description of integration into the operational environment for activities.

	Breadth of Coverage	Examinations uses a sufficiently large sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide the level of coverage necessary for determining:
		▪ Whether the applicable controls are:
		  ○ Implemented; and
		  ○ Free of obvious/apparent errors;
		▪ Whether there are further increased grounds for confidence that the applicable controls are:
		  ○ Implemented correctly; and
		  ○ Operating as intended on an ongoing and consistent basis; and
		▪ There is support for continuous improvement in the effectiveness of the applicable controls.
			Interviews use a sufficiently large sample of individuals in organizational roles and other specific individuals deemed particularly important to achieving the assessment objective to provide the level of coverage necessary for determining:
			▪ Whether the applicable controls are:
			  ○ Implemented; and
			  ○ Free of obvious/apparent errors;
			▪ Whether there are further increased grounds for confidence that the applicable controls are:
			  ○ Implemented correctly; and
			  ○ Operating as intended on an ongoing and consistent basis; and
			▪ There is support for continuous improvement in the effectiveness of the applicable controls.
				Testing uses a sufficiently large sample of assessment objects by type and number within type and other specific assessment objects deemed particularly important to achieving the assessment objective to provide the level of coverage necessary for determining:
				▪ Whether the applicable controls are:
				  ○ Implemented; and
				  ○ Free of obvious/apparent errors;
				▪ Whether there are further increased grounds for confidence that the applicable controls are:
				  ○ Implemented correctly; and
				  ○ Operating as intended on an ongoing and consistent basis; and
				▪ There is support for continuous improvement in the effectiveness of the applicable controls.

Assessment Objects	Specifications	Review: ▪ Policies; ▪ Plans; ▪ Procedures; ▪ System requirements; and ▪ Designs.	N/A	N/A
	Mechanisms	Review configurations and/or functionality implemented in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.	N/A	Test functionality in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.

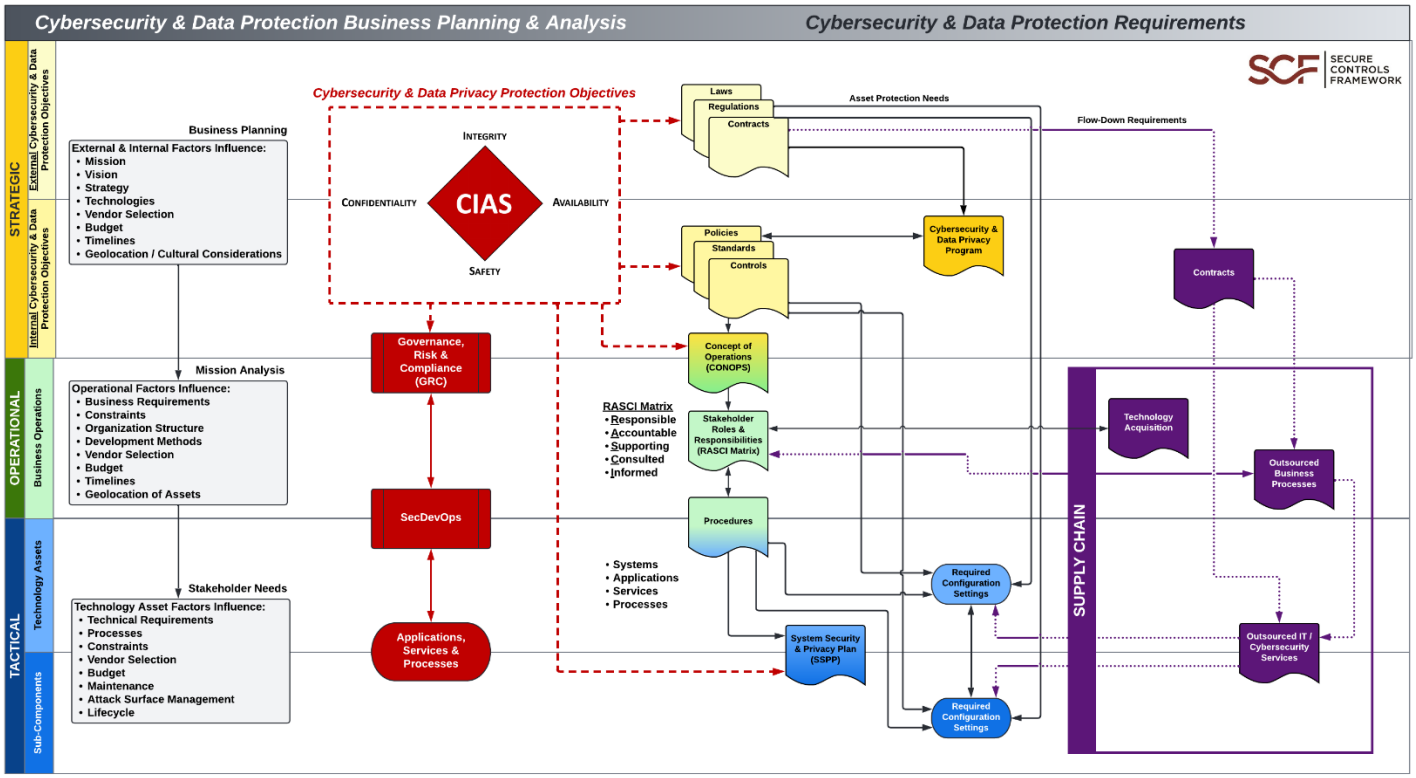
	Activities	Review procedures associated with: ▪ Designs; ▪ System operations; ▪ Administration; ▪ Management; and/or ▪ Exercises.	N/A	Test applicable procedures for: ▪ System operations; ▪ Administrative activities; ▪ Management functions; and ▪ Exercises (e.g., incident response, business continuity, security awareness, etc.).
	Individuals or Groups	N/A	Conduct interviews with applicable stakeholders associated with control execution and/or oversight. Interviews should focus on people and/or teams with RASCI-assigned roles and responsibilities: ▪ Responsible - People directly responsible for performing a task (e.g., control/process operator); ▪ Accountable - Person overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ Supportive - People under the coordination of the Responsible person for support in performing the task; ▪ Consulted - People not directly involved in task execution but were consulted for subject matter expertise; and ▪ Informed - People not involved in task execution but are informed when the task is completed.	N/A

APPENDIX D: ADEQUATE SECURITY

The CDPAS recognizes that no technology can provide "absolute security" due to the limits of human certainty. This uncertainty exists in the lifecycle of every system, application and/or product and is often due to the constraints of cost, schedule, performance, feasibility and practicality. Therefore, trade-offs must be routinely made across contradictory, competing and conflicting needs and limitations. However, these trade-offs must be optimized to achieve "adequate security," reflecting a risk-based decision by stakeholders. [39]

The CDPAS leverages concepts from NIST SP 800-160 to explain the holistic concepts of how broader business planning and analysis ultimately lead to actionable cybersecurity and/or data protection requirements. Understanding this hierarchical nature of requirements is a fundamental construct of cybersecurity and/or data protection control governance processes.

This concept is depicted in the following graphic for how the concept of adequate security is based on business planning and analysis as it relates to establishing protection requirements:[40]



An organization publishes policies to eliminate potential gaps in that desired governed behavior to achieve "adequate security" based on what a reasonable individual would be expected to do in a similar situation. The rules associated with this "governed behavior" must be accurate, consistent, compatible and complete with respect to the executive leadership's objectives to accomplish the organization's mission and overall strategy.

An organization's policies ultimately define the behavior of Individual Contributors (IC) (e.g., engineers, analysts, developers, etc.) in performing their roles and associated responsibilities for developing processes and procedures. This eventually leads to the configuration of technology assets (e.g., systems, applications, services and processes), where a discrete set of restrictions and properties must exist to specify how that asset enforces or contributes to implementing organizational security policies.

The required configuration settings for technology assets must include technical and business requirements, which ultimately fall under organizational cybersecurity and/or data protection policies. Requirements can be categorized as follows: [41]

- Stakeholder requirements that address the need to be satisfied in a design-independent manner; and

[39] *NIST SP 800-160 Vol 1 Rev 1 Appendix C*
[40] *SCF Business Planning & Analysis Processes - https://securecontrolsframework.com/content/graphics/adequate-security.png*
[41] *NIST SP 800-160 Vol 1 Rev 1 Appendix C*

- System requirements express the specific solution that will be delivered in a design-dependent manner.

Establishing Secure Systems

A "secure system" is a system that ensures that only the authorized intended behaviors and outcomes occur, thereby providing freedom from those conditions, both intentionally/with malice and unintentionally/without malice, that can cause a loss of information assets with unacceptable consequences.[42] This definition expresses an ideal that captures three (3) essential aspects of what it means to achieve security:

1. Enable the delivery of the required system capability despite intentional and unintentional forms of adversity;
2. Enforce constraints to ensure that only the desired behaviors and outcomes associated with the required system capability are realized while satisfying the first aspect; and
3. Enforce constraints based on rules to ensure that only authorized human-to-machine and machine-to-machine interactions and operations are allowed to occur, while satisfying the second aspect.

For a system, adequate security is an evidence-based determination that achieves and optimizes security performance against all other performance objectives and constraints. Judgments of adequate security are driven by the stakeholder objectives, needs and concerns associated with the system. Adequate security has two elements:

- Achieve the minimum acceptable threshold of security performance; and
- Maximize security performance to the extent that any additional increase in security performance degrades some other aspects of system performance or requires an unacceptable operational commitment.

Defining Stakeholder Security Requirements

Stakeholder security requirements are those stakeholder requirements that are security-relevant. Stakeholder security requirements specify:

- The protection needed for the mission or business, data, information, processes, functions, human and system assets;
- The roles, responsibilities and security-relevant actions of individuals who perform and support the mission or business processes;
- The interactions between the security-relevant solution elements; and
- The assurance that is to be obtained in the security solution.

Defining System Security Requirements

System requirements specify the technical view of a system or solution that meets the identified stakeholder needs. The system requirements are a transformation of the validated stakeholder requirements. System requirements specify what the system or solution must do to satisfy the stakeholder requirements. System security requirements are those system requirements that are security relevant. These requirements define:

- The protection capabilities provided by the security solution;
- The performance and behavioral characteristics exhibited by the security solution;
- Assurance processes, procedures and techniques;
- Constraints on the system and the processes, methods and tools used to realize the system; and
- The evidence required to determine the system security requirements have been satisfied.

System of Systems Mindset

A system is *"an arrangement of parts or elements that together exhibit a behavior or meaning that the individual constituents do not."*[43] Since engineers/architects/developers do not design, code and maintain Applications, Services and Processes (ASP) in a vacuum, they need to embrace a "system of systems" mindset toward system interaction since there are legitimate cybersecurity and/or data protection concerns with untrustworthy dependencies. A system of systems is a *"set of systems and system elements interacting to provide a unique capability that none of the constituent systems can accomplish on their own."*[44]

[42] *NIST SP 800-160 Vol 1 Rev 1*
[43] *NIST SP 800-160 Vol 1 Rev 1*
[44] *NIST SP 800-160 Vol 1 Rev 1*

A system of systems consists of several constituent systems plus any inter-system infrastructure, facilities and processes necessary to enable the constituent systems to integrate or interoperate.

This concept includes "interfacing systems" that have an interface for exchanging data or information, energy, or other resources. Interfacing systems have two specific subsets:

- Enabling Systems. These provide essential services required to create and sustain the system. Examples of enabling systems include:
  - Development environments;
  - Production systems, applications and services;
  - Training systems; and
  - Maintenance systems; and
- Interoperating Systems. These interact with systems to jointly perform a function during the utilization and sustainment stages of the system life cycle. Interoperating systems often form a system of systems.