Security & Privacy by Design Principles (S|P)

The S|P establishes 32 common-sense principles to guide the development and oversight of a modern security and privacy program. The S|P is sourced from the Secure Controls Framework (SCF), which is a free resource for businesses. The SCF’s comprehensive listing of nearly 750 cybersecurity and privacy controls is categorized into 32 domains that are mapped to over 100 statutory, regulatory and contractual frameworks. Those applicable SCF controls can operationalize the S|P principles to help an organization ensure that secure practices are implemented by design and by default. Those 32 S|P principles are listed below:

1. Security & Privacy Governance
   Govern a documented, risk-based program that encompasses appropriate security and privacy principles to address all applicable statutory, regulatory and contractual obligations.

2. Asset Management
   Manage all technology assets from purchase through disposition, both physical and virtual, to ensure secured use, regardless of the asset’s location.

3. Business Continuity & Disaster Recovery
   Maintain the capability to sustain business-critical functions while successfully responding to and recovering from incidents through a well-documented and exercised process.

4. Capacity & Performance Planning
   Govern the current and future capacities and performance of technology assets.

5. Change Management
   Govern change in a sustainable and ongoing manner that involves active participation from both technology and business stakeholders to ensure that only authorized changes occur.

6. Cloud Security
   Govern cloud instances as an extension of on-premise technologies with equal or greater security protections than the organization’s own internal controls.

7. Compliance
   Oversee the execution of cybersecurity and privacy controls to create appropriate evidence of due care and due diligence, demonstrating compliance with all applicable statutory, regulatory and contractual obligations.

8. Configuration Management
   Govern the establishment and ongoing management of secure configurations for systems, applications and services according to vendor-recommended and industry-recognized secure practices.

9. Continuous Monitoring
   Maintain situational awareness of security-related events through the centralized collection and analysis of event logs from systems, applications and services.

10. Cryptographic Protections
    Utilize appropriate cryptographic solutions and industry-recognized key management practices to protect the confidentiality and integrity of sensitive data both at rest and in transit.

11. Data Classification & Handling
    Publish and enforce a 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.

12. Embedded Technology
    Provide additional scrutiny to the risks associated with embedded technology, based on the potential damages posed when used maliciously.

13. Endpoint Security
    Harden endpoint devices to protect against reasonable threats to those devices and the data they store, transmit and process.

14. Human Resources Security
    Foster a security and privacy-minded workforce through sound hiring practices and ongoing personnel management.

15. Identification & Authentication
    Implement an Identity and Access Management (IAM) capability to ensure the concept of “least privilege” is consistently implemented across all systems, applications and services for individual, group and service accounts.

16. Incident Response
    Maintain a practiced incident response capability that trains all users on how to recognize and report suspicious activities so that trained incident responders can take the appropriate steps to handle incidents, in accordance with an Incident Response Plan (IRP).

17. Assurance
    Utilize an impartial assessment process to validate the existence and functionality of appropriate security and privacy controls, prior to a system, application or service being used in a production environment.

18. Maintenance
    Utilize secure practices to maintain technology assets, according to current vendor recommendations for configurations and updates, including those supported or hosted by third-parties.

19. Mobile Device Management
    Govern mobile devices through a centralized or decentralized model to restrict logical and physical access to the devices, as well as the amount and type of data that can be stored, transmitted or processed.

20. Network Security
    Architect a defense-in-depth methodology that enforces the concept of “least functionality” through restricting network access to systems, applications and services.

21. Physical & Environmental Security
    Implement layers of physical security and environmental controls that work together to protect both physical and digital assets from theft and damage.

22. Privacy
    Implement a privacy program that ensures industry-recognized privacy practices are identified and operationalized throughout the lifecycle of systems, applications and services.

23. Project & Resource Management
    Utilize a risk-based approach to prioritize the planning and resourcing of all security and privacy aspects for projects and other initiatives to allocate foreseeable governance, risk and compliance roadblocks.

24. Risk Management
    Govern a risk management capability that ensures risks are consistently identified, assessed, categorized and appropriately remediated.

25. Secure Engineering & Architecture
    Implement secure engineering and architecture processes to ensure industry-recognized secure practices are identified and operationalized throughout the lifecycle of systems, applications and services.

    Assign appropriately-qualified personnel to deliver security and privacy operations that provide reasonable protective, detective and responsive services.

27. Security Awareness & Training
    Develop a security and privacy-minded workforce through ongoing user education about evolving threats, compliance obligations and secure workplace practices.

28. Technology Development & Acquisition
    Govern the development process for any acquired or developed system, application or service to ensure secure engineering principles are operationalized and functional.

29. Third-Party Management
    Implement ongoing third-party risk management practices to actively oversee the supply chain so that only trustworthy third-parties are used.

30. Threat Management
    Identify, assess and remediate technology-related threats to assets and business processes, based on a thorough risk analysis to determine the potential risk posed from the threat.

31. Vulnerability & Patch Management
    Utilize a risk-based approach to vulnerability and patch management practices that minimizes the attack surface of systems, applications and services.

32. Web Security
    Govern all Internet-facing technologies to ensure those systems, applications and services are securely configured and monitored for anomalous activity.
In simple terms, controls exist to protect an organization's data. Requirements for asset management do not primarily exist to protect the inherent value of the asset, but the data it contains, since assets are merely data containers. Assets, such as laptops, servers and network infrastructure are commodities that can be easily replaced, but the data cannot. This concept of being data-centric is crucial to understand when developing, implementing and governing a cybersecurity and privacy program. In the seven steps listed below, the guidance is focused on building secure processes so that compliance is a natural byproduct. This is an industry-agnostic approach that applies to any combination of compliance requirements your organization needs to address.

1. **Develop a vision, mission and strategy that supports your organization's specific needs.**

   An indicator of a well-run cybersecurity and privacy program is personnel at all levels clearly knowing their role in making the organization successful through the implementation of a vision, mission and strategy to drive its operations. This is leadership in its purest form, since it involves providing appropriate direction and empowering staff to make the right things happen. Everything starts with the assigned mission - it defines the big picture of why you have a job at your organization!

2. **Adopt appropriate cybersecurity and privacy frameworks to support your strategy.**

   You need to identify all applicable laws, regulations and contracts that your organization is required to comply with. This includes both domestic and international cybersecurity and privacy laws, industry-specific regulations and legally-binding contract requirements from clients and partners. Knowing what is required from a compliance perspective helps identify the appropriate cybersecurity and privacy principles that will best fit your organization's specific needs.

   It is critical to understand that this step is more of a business decision, than a technical decision. Additionally, what works well for one situation may not necessarily work well for another organization, so ample due diligence is required to find what is right for your unique situation.

3. **Develop policies, standards and procedures to support your cybersecurity & privacy principles.**

   Documentation is the foundation of any governance program and it requires written policies, standards, controls and procedures. Well-designed documentation is hierarchical and builds on supporting components to enable a strong governance structure that utilizes an integrated approach to managing requirements.

   Understanding the hierarchy of cybersecurity documentation can lead to well-informed risk decisions, which influence technology purchases, staffing resources, and management involvement. That is why it serves both cybersecurity and IT professionals well to understand the cybersecurity governance landscape for their benefit, as it is relatively easy to present issues of non-compliance in a compelling business context to get the resources you need to do your job.

   All too often, documentation is not scoped properly, and this leads to the governance function being viewed as more of an obstacle as compared to being an asset. A multiple-page “policy” document that blends high-level security concepts (e.g., policies), configuration requirements (e.g., standards), and work assignments (e.g., procedures) is an example of poor documentation that leads to confusion and inefficiencies across technology, cybersecurity, and privacy operations. Several reasons why this form of documentation is considered poorly-architected documentation include:

   - **Human nature is always the mortal enemy of unclear documentation,** as people will not take the time to read it. An ignorant or ill-informed workforce entirely defeats the premise of having the documentation in the first place.
   - **If the goal is to be “audit ready” with documentation,** having excessively-wordy documentation is misguided. Excessive prose that explains concepts of noun/verb in paragraph after paragraph makes it very hard to understand the exact requirements, and that can lead to gaps in compliance.

4. **Identify a target maturity state that is based on your mission and strategy.**

   Using a recognized maturity model, such as the Systems Security Engineering: Capability Maturity Model (SSE-CMM), helps organizations avoid “moving targets” for expectations. Maturity goals define “what right looks like” in terms of the required people, processes and technology that are expected to exist in order to carry out procedures at the individual contributor level. Without maturity goals, it is very difficult and subjective to define success.

5. **Implement appropriate controls to achieve / measure your target maturity state.**

   Controls are “where the rubber meets the road” in a cybersecurity and privacy program - this is where the combination of people, processes and technology come together to operationalize a cybersecurity and privacy program. Essentially, controls bring your policies and standards to life by identifying the exact requirements necessary to comply with a statutory, regulatory or contractual obligation. You may have a control set specific to NIST 800-17, PCI DSS, HIPAA, SOX, SOCs or any other compliance obligation. You might even be managing multiple control sets based on your needs.

6. **Use those controls to assess both risk and maturity across technology and business processes.**

   There are numerous methodologies available for an organization to manage risk. These risk models range from NIST 800-37 to FAIR, ISO 31010, OCTAVE and others. What is similar between these risk methodologies is they all have to assess how well controls are implemented and the extent that risk is reduced from the control’s existence and level of maturity.

   It is important to keep in mind that a “perfect” risk methodology does not exist to assess risk across technology and business processes. What matters is that the risk methodology chosen best supports how the organization actually functions. It is acceptable to have a different risk methodology used for tactical, operational and strategic risk decisions, since each methodology has its own strengths and weaknesses. The goal is to define and attain a level of optimal risk taking.

   Managing risk is a process that must exist across all phases of the Secure Development Lifecycle (SDL), regardless if the solution being worked on is a system, application or service. The scope of assessing risk must consider not only the immediate assets in the scope of the SDLC, but those supporting systems, processes and possibly third-party service providers that impact confidentiality, integrity, availability and safety aspects.

7. **Utilize metrics from control execution to identify areas of improvement.**

   The concept of “monitoring controls” is synonymous with gathering metrics. While metrics are a point-in-time snapshot into a control’s performance, the broader view of metrics leads to longer term trend analysis. It is through this trend analysis that your organization’s leadership can identify areas of improvement. This can be done through defining Key Performance Indicators (KPIs) and Key Risk Indicators (KRI) to have insight into the controls that are particularly important to the organization. KPIs and KRIs will differ between organizations, due to varying priorities assigned to controls from regulations in statutory, regulatory and contractual obligations that affect the relative importance of certain controls.
Without an overarching concept of operations for the broader GRC function, organizations will often find that their governance, risk, compliance and privacy teams are siloed in how they think and operate. These siloed functions and unclear roles often stem from a lack of a strategic understanding of how these specific functions come together to build a symbiotic working relationship between the individual teams that enables quality control over people, processes and technology. The Plan, Do, Check & Act (PDCA) approach is a logical way to design a governance structure:

- **Plan.** The overall GRC process beings with planning. This planning will define the policies, standards and controls for the organization. It will also directly influence the tools and services that an organization purchases, since technology purchases should address needs that are defined by policies and standards.
- **Do.** Arguably, this is the most important section for cybersecurity and privacy practitioners. Controls are the "security glue" that make processes, applications, systems and services secure. Procedures (also referred to as control activities) are the processes how the controls are actually implemented and performed.
- **Check.** In simple terms, this is situational awareness. Situational awareness is only achieved through reporting through metrics and reviewing the results of audits/assessments.
- **Act.** This is essentially risk management, which is an encompassing area that deals with addressing two main concepts (1) real deficiencies that currently exist and (2) possible threats to the organization.

**Plan, Do, Check & Act (PDCA) Approach To Governance, Risk & Compliance (GRC)**

**Identify External Influencers:**
- Statutory & Regulatory Obligations
- Contractual Obligations
- Industry-Recognized Practices

**Identify Internal Influencers:**
- Business Processes
- Risk Tolerance
- Audit Findings

**Identify External Influencers**
- Compliance Requirements

**Identify Internal Influencers**
- Corporate Policies & Management Intent

**Policies & Standards**
- Policies are Enforced By
- Standards are Generated
- Controls Objectives are Aligned & Evaluated With

**May Influence**
- Guidelines
- May Influence
- Policies
- Standards
- Controls Objectives

**Tool Selection**
- Are Implemented By

**Plan, Do, Check & Act (PDCA) Approach**
- **Plan**
  - Policies & Standards
- **Do**
  - Procedures / Control Activities
- **Check**
  - Audits / Assessments
- **Act**
  - Remediation Actions

**Risk Management**
- Identifies Requirements For
- Identified Needs For

**Corporate Leadership**
- Requires

**Stakeholder Confidence**
- Influences

**Security Metrics**
- Generate

**Analytics & Trends**
- [KPIs / KRI / KCS]

**Systems, Applications Services & Processes**
- Are Reviewed Through
- Are Applied To

**Verify**
- Are Linked To

**Deficiencies**
- Influence

**Situational Awareness**
- Influence

**Copyright © 2019 by Verutus, LLC. All rights reserved.**

All text, images, logos, trademarks and information contained in this document are the intellectual property of Verutus, LLC, unless otherwise indicated. Modification of any content, including text and images, requires the prior written permission of Verutus, LLC. Requests may be sent to support@securecontrolsframework.com.