# SERVICES

## ASSESSMENTS *(SECURITY AUDITS AND ASSURANCE)*

Information security and cybersecurity are about more than just ensuring all the checkboxes are filled – they are about understanding what a company needs to protect in a cost-efficient manner. Many organizations choose to have security assessments done in order to understand their current security posture or to learn which areas could use improvement. Sometimes companies need an objective, external auditor that can attest to another party that the organizations' systems and processes are secure. Other times, organizations may simply want to do an environment scoping and discovery to either confirm or document how all the systems interact. No matter the motivation, Privity can help as its Principals have been conducting security assessments since 2005 and have been PCI Qualified Security Assessors since 2010.

### CATEGORIES OF SERVICE OFFERINGS

#### 1. Readiness Checks and Assessments

When working with business partners and their data, assurances are often needed to demonstrate an organization will handle data entrusted to them securely. Additionally, as the company's own business data is likely its most valuable asset, obtaining an opinion related to the security of company systems may bring the peace of mind necessary to trust one's business is not immediately vulnerable. Both of these goals can be met by having an objective, qualified third-party conduct a formal audit that looks not just at technical configurations and settings, but also how these systems are managed and maintained to ensure an organization can achieve a consistent security posture. Formal assessments tend to capture processes and management issues which manifest in technical misconfigurations or insecure settings, discover root causes, and help with remediation planning.

Our Readiness Checks and Assessments services include the following:

- *Scoping*
    - The first phase of any formal audit or assessment, such as PCI DSS, ISO 27001, or Privacy Assessment
        - ✓ Determine which systems and devices should be included in an assessment by mapping "data flows" onto the network and system architectures
        - ✓ Determine which processes and people should be included in an assessment
        - ✓ Determine the extent of outsourcing impact on the scope of the assessment

- ✓ Determine company's regulatory and/or legal obligations related to the environment being scoped
  - In some cases, the scope is determined based on the data being stored, processed, transmitted, and collected; in others, the company may be able to dictate the scope of the assessment
- ➢ May result in recommendations that can reduce scope and costs associated with regulatory or legislative compliance

- *IT Security Health Checks / Readiness Assessments*
  - Provide full IT Security Architecture Review
    - ✓ The audited company determines the scope and depth of an assessment
      - The review can be used to prepare for 3rd party audits such as SSAE 18 SOC 2 Type 2, NERC CIP, NIST CSF, Cloud Security Alliance CCM, FedRAMP, SOX 404, etc.
    - ✓ Conduct review of one or more different areas
      - Governance (policies, management procedures, daily operating procedures, standards and baselines, guidelines, awareness training)
      - Network Architecture (placements of firewalls, routers, IDS/IPS, WIPS/WIDS; wireless security, segmentation, VPN and remote access to data and systems; multi-cloud / hybrid cloud; virtualization / on-premises / cloud-native configuration, container orchestration, DevOps integrations)
      - Identity and Access Management (authentication, authorization and permissions, audit logging)
      - Logging and Monitoring (system logging, device logging, data logging, log aggregation, log storage, frequency of log reviews)
      - Security Software (antimalware management, file integrity monitoring management, etc.)
      - Device and System Hardening (use of insecure services, patching, vulnerability management, configuration standard reviews, encryption types in use)
      - Outsourcing Arrangements (due diligence, contract reviews, responsibility matrix reviews and gap analysis)
      - Data and Information lifecycle Management (data classification, labelling, retention periods, sharing, and destruction)
      - Incident Response Management (processes, technology, training, testing, disaster recovery, business continuity)

- *ISO/IEC 27001 Readiness Assessments*
  - Conduct an ISO readiness assessment

- ✓ The company determines the scope of the Information Security Management System (ISMS) assessment
  - Audit against ISO/IEC 27001
  - Use ISO/IEC 27002 as a guide
- ✓ Walk through the process of obtaining certification with an accredited auditor

- *Threat Risk Assessments*
  - Provide a threat risk assessment of an organization's IT environment
    - ✓ The company determines the scope of the threat risk assessment
      - Identify threats to the organization
      - Analyze the threats relevant to the organization
      - Translate the threats into risks
      - Quantify the risks into financial exposure
      - Assess the risk to the organization

- *Cloud Security Risk Assessments*
  - Conduct a security risk assessment of a cloud environment
    - ✓ Review current cloud environment and/or plans for future deployment using industry best practice frameworks (Cloud Security Alliance Cloud Control Matrix, NIST CSF, etc.)
    - ✓ Ascertain risk to company data related to current management activities
    - ✓ Determine areas that warrant in-depth program audit
      - Prioritize follow-up activities with higher risk
      - Outline future program audit plans

- *Privacy Assessments*
  - Conduct a privacy assessment of an organization's environment
    - ✓ Confirm compliance with relevant privacy legislations (PIPA, PIPEDA, FOIPPA, GDPR, CCPA, etc.)
    - ✓ Privacy impact assessments (PIA) can also be conducted when changes to an already assessed environment are proposed
    - ✓ The scope is determined by the nature of the Personally Identifiable Information being collected, stored, processed, or transmitted
    - ✓ Privacy assessments use a subset of tasks from an IT Security Health Check
  - ➢ Requires *Scoping* to be completed either beforehand or in conjunction with the privacy assessment

## 2. Specific Area Spot-Checks and Reviews

An organization may not want to conduct a full security audit of its environment and may only want to review a single component to ensure it is headed in the right direction. Spot-check services are often used to support project initiatives (ex. installation of a new system or device

which may have an impact on existing operations), or to confirm the operational procedures used internally are sound.

Our Specific Area Spot-Checks and Reviews services include:

- *Firewall Ruleset and ACL Reviews*
    - Review documented rules outlined within a "baseline" or configuration standards against practices
        - ✓ Reconcile the running configuration with the baseline
        - ✓ Reconcile the rules with change requests
        - ✓ Compare the rules to recommendations from industry best practices
    - Reconcile rules with business requirements
        - ✓ Identify rules which introduce unnecessary risk to the organization
        - ✓ Identify any areas where configurations could be tightened to better secure a device or a system
- *Technology Baseline Evaluations*
    - Review business processes meant to ensure baselines are kept current
        - ✓ Reconcile baseline to the running configuration (configuration export)
        - ✓ Reconcile baseline to change requests
        - ✓ Reconcile all vendor patches with baseline
        - ✓ Reconcilie baseline content with industry best practices, such as Center for Internet Security (CIS) baselines, or with vendor guidance (such as those from Microsoft, Amazon, Oracle, etc.)
        - ✓ Reconcile running services and open ports with business requirements
            - Identify areas where configurations could be altered to be more secure without impacting business operations
- *Cloud Security Management Program Audits*
    - Review individual management programs based on risk to the organization
        - ✓ Look for alignment with ITIL style or DevOps management, ISO 27002, NIST 800-53, etc., consider emerging and leading-edge technology
    - Review governance and confirm organizational adherence
        - ✓ Review program policies
        - ✓ Review program management procedures
        - ✓ Review program daily operating procedures
        - ✓ Review cloud technology in use
        - ✓ Review configuration standards and baselines in use
        - ✓ Review running configurations
        - ✓ Interview staff and management about operations
- *Governance Reviews*
    - Review ownership of policies related to IT, security, and information management

- ✓ Review communication methods and staff training of policies
- ✓ Review content of policies used within the organization
- ✓ Reconcile policy content to industry best practices
- ✓ Identification of areas where policies can better reflect the intentions of management

- Review of documented procedures
  - ✓ Reconcile policies with management procedures and daily operating procedures
  - ✓ Reconcile procedure content to industry best practices
  - ✓ Reconcile documented procedures with actual practices

- *Outsourcing and Service Provider Due Diligence*
  - Provide legal document reviews and analysis
    - ✓ Review contract for content appropriateness, relevance, and risk
    - ✓ Review and evaluate SSAE 18 SOC 2 Type 1 / Type 2 or SOC 3 for relevance
    - ✓ Review or formalize a Responsibility Matrix documenting roles
      - Confirm responsibility assignments, determine which responsibilities remain with the organization and which are outsourced to service provider(s)
    - ✓ Review Service Level Agreements (SLAs)
    - ✓ Review Service Level Objectives (SLOs)
  - Provide service provider suitability reviews
    - ✓ Validate or confirm status of service providers' compliance
    - ✓ Conduct a suitability-of-solution analysis
    - ✓ Conduct compliance impact assessments
    - ✓ Conduct privacy impact assessments (PIA)

- *RFP Response Scoring and Proposed Solution Reviews*
  - Provide RFP design support
    - ✓ Develop suitable content for inclusion in RFPs
    - ✓ Develop methodology for determining the scoring of future security and compliance proposals against issued RFPs
  - Provide RFP evaluation support
    - ✓ Review of independently developed RFP solutions for impact on security, privacy, and compliance
    - ✓ Ranking of respondents with respect to alignment with RFP
    - ✓ Offering recommendations based on a risk-benefit analysis

## 3. Compliance Validation and Assurance

Regulations such as PCI DSS periodically require qualified independent reviews of an organization's environment in order to confirm its compliance. These formal compliance audits yield an attestation by the auditor, verifying that testing has been done in accordance with the regulation and that all the tests were passed accordingly. Other times, business partners may

want some assurance that the company's systems have expected levels of security prior to sharing their critical data, and compliance validation services can be used to easily demonstrate this.

Our Compliance Validation and Assurance services include:

- *PCI DSS Assessments*
    - Provide PCI DSS assessments to: merchant organizations (that collect, process, transmit, and/or store credit card data), payment service providers (who manage some or all credit card handling services on merchants' behalf), or service providers that can either directly or indirectly affect the security of merchants' cardholder data environments (even if they are uninvolved in handling merchants' credit card data)
        - ✓ Provide PCI Qualified Security Assessor (QSA) assessments of all types
            - Report on Compliance (ROC)
            - Self-Assessment Questionnaires or SAQ (SAQ A, SAQ A-EP, SAQ B, SAQ B-IP, SAQ C, SAQ C-VT, and SAQ D)
            - Attestation of Compliance for ROCs
            - Attestation of Compliance for SAQs
        - ✓ Conduct all testing procedures outlined by the PCI DSS
            - Ranges from 64 to more than 800, depending on the nature of the company and the way in which it handles cardholder data
    - ➢ Requires *Scoping* to be completed either before or as part of an assessment
- *PCI DSS Attestations of Compliance*
    - Provided as part of formal *PCI DSS Assessments*
    - Documents a company's compliance status
        - ✓ Reflective of the level of assurance we have with the organization adhering to PCI DSS at a specific point in time
        - ✓ Used to prove to the merchant bank / acquirer or Payment Card Brands that the company is PCI DSS compliant
        - ✓ May need to be provided to 3rd parties if requested as part of a contractual obligation
    - Valid for 1 year from issue or until the next assessment
- *Formal Opinion Letters*
    - Provide formal opinion letter(s) addressed to either the company or its 3rd parties' inquiries regarding the status of the company's security posture or its compliance
        - ✓ Consider company's choice of technology, deployments, service provider(s), business decisions, etc.

## 4. Compliance Remediation Advisory

Non-compliance with an applicable industry regulation (i.e. PCI DSS) or a legislation (i.e. GDPR, PIPA, PIPEDA, CCPA, etc.) is typically exacerbated for organizations by them unnecessarily having multiple systems and devices in scope unrelated to the relevant operations, although it is rare that successful remediation gets achieved through a single change in the environment, be it through removal or deployment of new technology. Most instances of non-compliance are indicative of a larger, more systemic problem that necessitates a material change to both systems and processes to truly address the underlying issues.

Compliance remediation advisory services are a specific type of security consulting where the main objective is the reduction of the regulatory risk to the company, often by focusing on decreasing applicable scope. Although scope reduction itself may be the fastest way of addressing non-compliance, it does not necessarily improve the company's overall security posture (i.e. outsourcing the storage of credit card data can dramatically reduce the company's external compliance obligations, but will not make the company's databases any more secure). The rest of the remediation advisory services can be leveraged to address security project objectives in conjunction with meeting the immediate compliance requirements.

Our Compliance Remediation Advisory services include:

- *Solution Architecture Development*
    - Identify requirements and translate them to technical architecture
        - ✓ Develop formal enterprise architecture
        - ✓ Develop formal network architecture and design
        - ✓ Develop formal security architecture (focusing on Confidentiality, Integrity, and Availability or the CIA triad)
        - ✓ Develop formal system architecture
            - Design with resiliency in mind
            - Integrate with disaster recovery plans
            - Modernize legacy systems with automation and scalability
            - Leverage different technologies (traditional tech, virtualization, Iaas, PaaS, SaaS cloud, containers, orchestration, serverless, etc.)
            - Integrate with Agile, DevOps, ITIL, and other processes
- *Scope Reduction Strategy Development*
    - Develop strategies to remove unnecessary systems and devices from compliance scope to focus on core business rather than compliance
        - ✓ Advise on network segmentation (installation of firewalls or routers, incorporation of VPNs, mixed-mode virtualization, encryption, etc.)

- ✓ Advise on data tokenization (change of regulated data like credit card numbers or Personally Identifiable Information into devalued data for internal use)
- ✓ Reengineer business processes (change of business processes that currently result in exposure to regulated data)
- ✓ Advise on outsourcing (leverage compliance-validated service providers to handle the collection, processing, storage, and/or transmission of regulated data on behalf of the company)

- *Legacy System Protection and Compensating Control Design*
  - Identify the shortcomings of the existing system relative to the compliance objective
    - ✓ Identify the risk to the organization with respect to not meeting its compliance objective
    - ✓ Identify methods to isolate the legacy system that cannot be replaced
  - Design cost-effective controls using additional technology and/or processes to protect the system and company
    - ✓ Conduct a risk assessment and evaluate the risk associated with using the compensating control
    - ✓ Identify any residual risk associated with using the compensating control
    - ✓ Document the compensating control as related to the control objective and compliance requirements

- *Governance Development*
  - Augment existing and/or develop new policies and procedures
    - ✓ Leverage industry best practices to provide best value
    - ✓ Use ITIL and/or DevOps methodologies, reflective of management's direction
    - ✓ Use different policy and procedure language for different target audiences (i.e. IT department policy vs. acceptable use policy)
    - ✓ Balance formal rules with management discretion
  - Formalize critical management programs (i.e. incident management, change management, configuration management, project delivery, supplier management, etc.)