WHITEPAPER

Beyond PCI Compliance: Evaluating Your IT Risk

SecureTrust™
a Trustwave® division

Overview

With its deep roots in adopting and developing PCI Compliance best practices, SecureTrust™, a Trustwave® division, has long championed the prudence and benefits of approaching Payment Card Industry (PCI) compliance initiatives through a security-first approach. In today's threat environment and with the increased cadence of PCI Data Security Standard (DSS) releases, that recommendation to approach compliance as a by-product of a secure foundation becomes a near-imperative. The PCI Security Standards Council (SSC) issued three updates to the DSS over a period of 18 months due to emerging threats. It further forecasts that future updates will be as unpredictable as the next wave of cyberattacks.

The PCI DSS requires an annual risk assessment of your cardholder data environment in order for your organization to achieve PCI compliance. While the PCI DSS sets a clear standard for baseline security for cardholder data, it is a baseline. To stay ahead of upcoming releases of the DSS and cyberthreats, your organization should be considering going beyond it.

Further, the DSS does not address requirements for the security of your IT assets outside the cardholder data environment (CDE). In particular, it does not address business continuity or identification of strategic assets outside the CDE. To encompass those potential risks, you need a broader approach to risk identification and risk assessment.

This white paper addresses the suitability of common risk assessment frameworks to your organization's requirements as you consider strategies to stay ahead of the both cybercriminals and future PCI DSS releases in these turbulent times.

Industry-leading organizations make it an annual best practice to conduct an information technology (IT) risk assessment to meet their own compliance standards, even beyond regulatory mandates. In the current threat landscape, taking a good look at the risk management process you are using and ensuring that it addresses today's daunting challenges might be the most important activity you take on all year.

It's critical that you evaluate your security framework in light of the level of risk that you have determined to be appropriate for your organization and its key assets. Neglecting to develop an effective risk-mitigation and data-protection strategy that addresses your entire organization, including mobile workers, third-party vendors and supply chain partners can leave you exposed to high-profile data compromises, data loss or misuse, or the inability to access critical information. Taking a step back to examine your approach to managing your organization's critical IT assets and making strategic adjustments if necessary has never been more relevant.

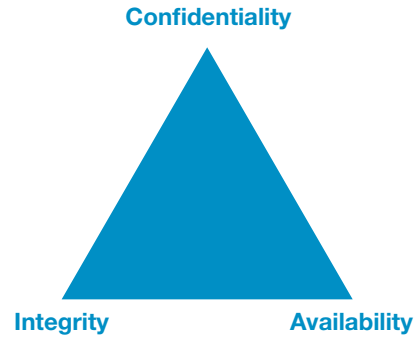
In this white paper, we'll examine:

- Classic principles in risk assessments
- Common risk assessment frameworks and why the NIST Cybersecurity Framework is emerging as a framework of choice
- Where the PCI DSS fits in
- Evolving best practices in risk assessments
- The importance of Maturity Modeling
- Key considerations for every organization in risk assessment planning

Classic Principles in Risk Assessments

The ultimate goal of an information security risk assessment is to translate your assessed IT risks into business-saving decisions, to identify the key IT security deficiencies that put your business at risk, and develop an organizational plan for acknowledging and mitigating those risks.

With the classic CIA triad, it is acknowledged that balancing Confidentiality, Integrity and Availability is at the heart of the dance. A focus on Availability will almost surely compromise Confidentiality and Integrity to some degree; while a focus on Confidentiality or Integrity will inevitably impact Availability. It should be noted that cybercriminals are also aware of these principles and the inherently exploitable tradeoffs.



The CIA triad is a guidance model for information security

A risk assessment should begin with a clear understanding of your organization's business goals, potential threats, likelihood of compromise and the impact of the loss. This may be achieved with a comprehensive interview process involving all aspects of the organization; such as senior management, IT administrators and key stakeholders.

Once the threat landscape and business risk appetite is clearly defined, the current security posture must be determined and the security gaps exposed and documented.

With the in-depth assessment information in-hand, the next step is to determine the best security controls to mitigate business risk and the timeline for putting them in place. These can include a combination of technology, policy, process and procedure.

Evaluating Common Risk Assessment Frameworks

In this section, we will review five common security frameworks, their potential benefit to your organization and why the National Institute of Standards and Technology (NIST) Cybersecurity Framework is emerging as a framework of choice. Highlighted frameworks are:

- International Standards Organization (ISO) 27005: Information technology - Security techniques - Information security risk management
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
- Control Objectives for Information and Related Technologies (COBIT)
- NIST Frameworks:
  - Special Publication (SP) 800-53: Assessing Security and Privacy Controls in Federal Information Systems and Organizations
  - Cybersecurity Framework

ISO 27000x Series

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) jointly publish the ISO/IEC 27000-series.

The series provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system.

Within this framework, organizations are encouraged to assess their information security risks, then implement appropriate information security controls according to their needs, while incorporating continuous feedback and improvement activities that are designed to address changes in the threat landscape or information security incidents.

The standard doesn't specify any specific risk management method. It does, however, imply a continual process consisting of a structured sequence of activities, some of which are iterative:

- Establish the risk management context and the organization's risk tolerance or appetite.
- Assess relevant information risks, taking into account the information assets, threats, existing controls and vulnerabilities to determine the likelihood of incidents or incident scenarios and the predicted business consequences if they were to occur, to determine a "level of risk." Assessments can be qualitative or quantitative.
- Use information security controls and share risks with third parties appropriately.
- Use defined "levels of risk" to prioritize them.
- Keep stakeholders informed throughout the process.
- Monitor and review risks, risk treatments, obligations and criteria on an ongoing basis, identifying and responding appropriately to significant changes.

While the ISO/IEC 27000x series is designed to be applicable to organizations of all shapes and sizes, in some cases the level of detail goes beyond what is applicable for a particular organization and the broader, simpler OCTAVE framework may be incorporated in to the assessment. This helps eliminate a series of "not applicable" responses.

OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a security framework for determining risk level and planning defenses against cyber assaults. OCTAVE was developed in 2001 at Carnegie Mellon University for the United States Department of Defense. The framework is designed to help organizations minimize their exposure to likely threats, determine the probable outcomes of an attack and address attacks that succeed.

OCTAVE defines three phases:

Phase 1: Build Asset-Based Threat Profiles

Phase 2: Identify Infrastructure Vulnerabilities

Phase 3: Develop Security Strategy and Plans

There are two versions of OCTAVE:

- OCTAVE-S, a simplified methodology for smaller organizations that have flat hierarchical structures
- OCTAVE Allegro, a more comprehensive version for large organizations or those with multi-level structures

COBIT

Control Objectives for Information and Related Technologies (COBIT) is a framework that was first released by ISACA, an international professional association focused on IT Governance. The current release is COBIT 5 and it is a business framework designed for the governance and management of enterprise information technology.

COBIT 5 is designed so that IT can be governed and managed in a holistic manner for the entire enterprise, including the full end-to-end business and IT functional areas of responsibility and the IT-related interests of internal and external stakeholders.

There are five subsets to COBIT 5, each covering a domain:

- Audit and Assurance
- Risk Management
- Information Security
- Regulatory and Compliance
- Governance of Enterprise IT

It is an operational framework, focused on uptime, and particularly suitable to organizations with discrete product deliverables, such as manufacturing organizations because they can pick and choose between the governance domains most applicable to their organization and risk categories and priorities.

NIST Frameworks

National Institute of Standards and Technology (NIST) is a unit of the U.S. Commerce Department. Publications evolved as a result of research into workable and cost-effective methods for optimizing the security of IT systems and networks in a proactive manner. The documents are available free of charge, and can be useful to businesses and educational institutions, as well as to government agencies.

Two commonly used NIST frameworks are the 800-53 and the Cybersecurity Framework (CSF). Though released by a U.S. government agency, the CSF is gaining growing acceptance internationally. It references globally recognized standards for cybersecurity and NIST promotes it as a "model for international cooperation on strengthening critical infrastructure cybersecurity."

NIST 800-53

Special Publication 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations, which preceded the CSF, was written to facilitate security control assessments and privacy control assessments conducted within an effective risk management framework. The control assessment results provide organizational officials with:

- evidence about the effectiveness of implemented controls
- an indication of the quality of the risk management processes employed within the organization
- information about the strengths and weaknesses of information systems which are supporting organizational missions and business functions in a global environment of sophisticated and changing threats

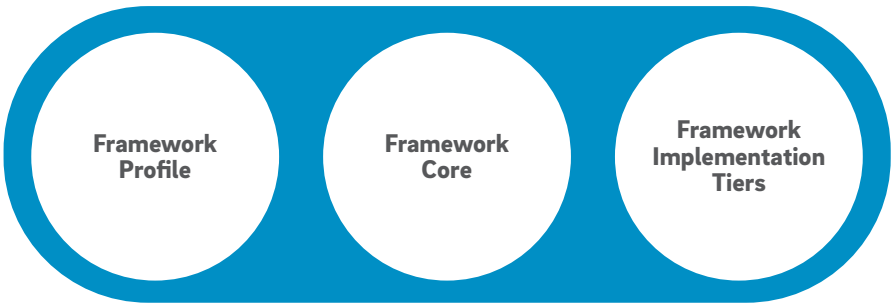
The 800-53 was designed to support compliance with the U.S Federal Information Processing Standards (FIPS), including FIPS 200 and 199. It incorporates strategies for harmonizing the Federal Information Security Management Act of 2002 (FISMA) with the international security standard ISO/IEC 27001. There is growing momentum for the adoption of the newer CSF as an alternate framework that has broad applicability to current risk assessment requirements, well beyond government entities and outside the U.S.

NIST Cybersecurity Framework

The first version of the NIST Cybersecurity Framework, Framework for Improving Critical Infrastructure Cybersecurity, was released in 2014 as a result of the U. S. Cybersecurity Enhancement Act of 2014. It is offered as a living document, with learnings and knowledge of new threats, risks and solutions incorporated in to updates.

The framework was designed to provide a "flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes," including International Organization for Standardization (ISO) standards.

The framework is intended to help organizations of any size, degree of risk or cybersecurity sophistication apply best practices of risk management to their organization. It references globally recognized standards for cybersecurity in its incorporation of standards, guidelines and best practices for cybersecurity, making it relevant for risk assessments outside the U.S. It is composed of three key components.



The NIST Cybersecurity Framework has three key components

The Framework Core provides a set of activities to achieve specific cybersecurity outcomes. It enables communication of cyber risk across an organization.

Framework Implementation Tiers are a qualitative metric of overall cybersecurity risk management practices. They categorize how an organization manages cybersecurity risks:

Tier 1: Partial

Tier 2: Risk Informed

Tier 3: Repeatable

Tier 4: Adaptive

The Framework Profile is used to align the business requirements, risk tolerance, and resources of the organization. It enables a roadmap for reducing cybersecurity risk that reflects the organization's risk management priorities. It is developed from the alignment of organizational goals, legal/regulatory requirements, and industry best practices.

Where The PCI DSS Fits In

The PCI Data Security Standard (DSS) is a model framework for security as well as the regulatory standard for the credit card industry. It has been designed by the PCI Security Standards Council (SSC) to be an actionable framework for developing a robust payment card data security process that includes prevention, detection and appropriate reaction to security incidents. This standard is required for PCI compliance by some of the largest corporations in the world and has been refined over the years with input from the implementation experiences and scrutiny of compliance and security experts around the world.

As the industry standard, the focus of the DSS is protection of payment card data, so in developing a broader security framework for your organization, you must consider elements of security that it does not address, such as other valuable company assets or business continuity. Also, since the DSS is a "pass/fail" standard, the concept of risk acceptance is not factored into the model. This is a key ingredient that needs to be added to expand the DSS into a full organizational framework.

While it is an excellent baseline security framework for the protection of cardholder data within your organization, the PCI DSS will not address the other risk assessment and risk mitigation requirements of most organizations without thoughtful modification in your approach.

It may be advisable to employ one or more of the assessment frameworks detailed above. Whatever framework you develop or choose, be sure to use all regulatory compliance requirements your organization must address to inform the implementation of your framework.

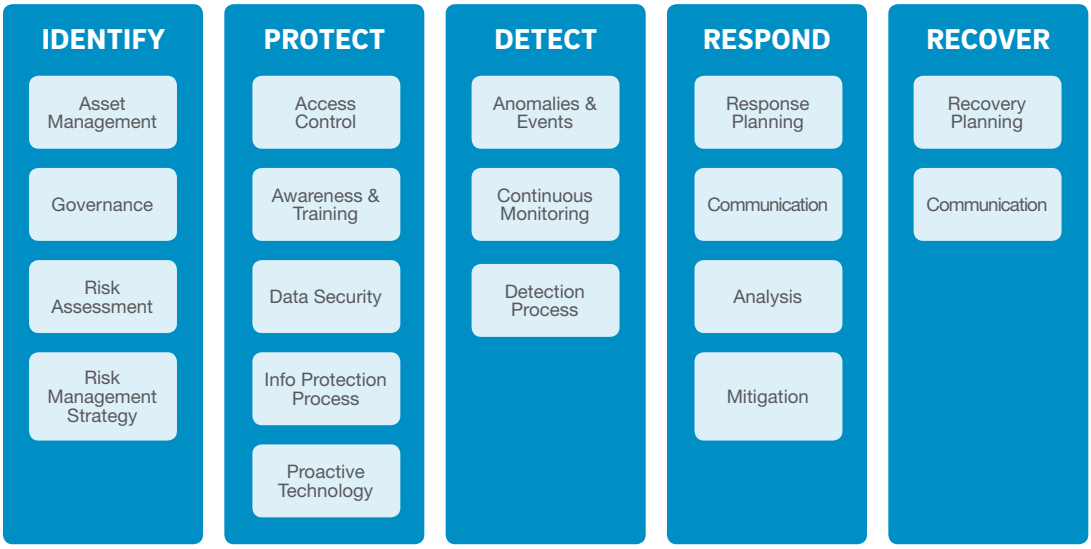
Evolving Best Practices in Risk Assessments

With keen awareness of the commercialization of cybercrime and the prevalence of organizational breaches, many organizations are shifting from a pure compliance approach to a broader risk-mitigation and data-protection strategy. Prioritizing your organization's most critical assets, their vulnerability and correlating that information to your organization's risk tolerance are essential elements of designing the most effective security risk management program.

While risk assessment methodology has always encompassed risks from a perspective of the entire supply chain, not just internal systems, in recent years we are seeing much more focus on assessing the risks of partner and third-party vendor access to the internal systems. This has been true of the PCI DSS as well, which implemented new standards for third-party service providers in its latest PCI DSS version 3.2.

Likewise, the maturation of mobile computing and broad corporate acceptance of bring your own device (BYOD) has led to a need for more focus on endpoint security and the impacts of endpoints to an organization's risk profile.

There is a growing acknowledgement that in today's threat environment, it is likely that the organization has already been breached, and that there isn't a level of functional protection that will change that. Consequently, once state-of-the-art protection is in place, there is an increased focus on detection, response and recovery and making sure that these actions can be swiftly implemented when breaches occur.



The five core functions in the NIST Cybersecurity Framework with category examples

The Importance of Maturity Modeling

Establishing an organizational maturity model for key indices of risk is an essential ingredient of current best practices in risk assessment.

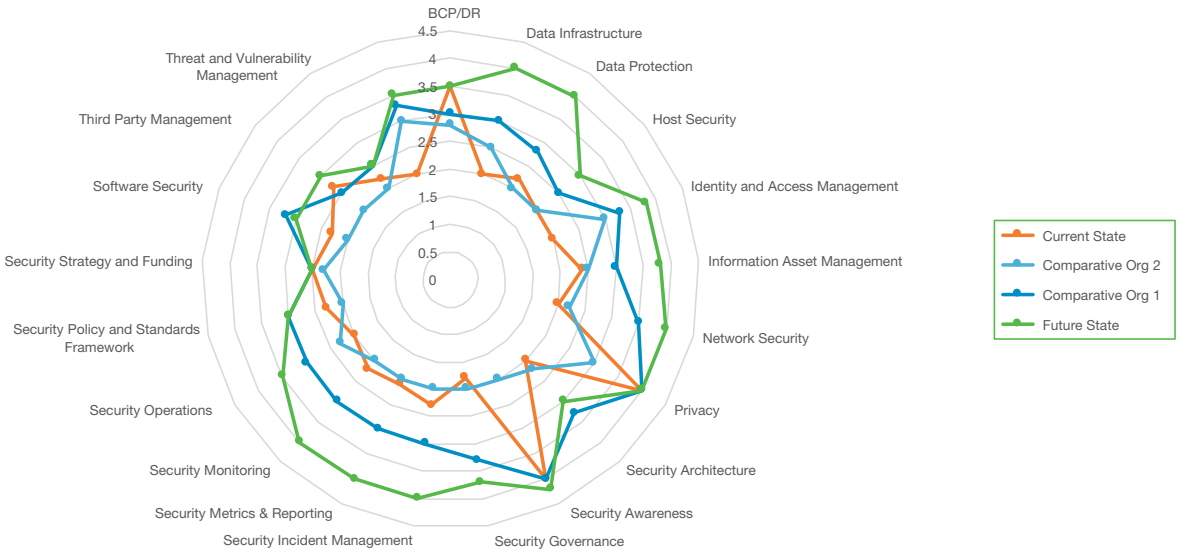
SecureTrust bases its maturity levels on the Capability Maturity Model Integration (CMMI), a globally-recognized set of best practices designed to enable organizations to improve performance, key capabilities, and critical business processes. The model describes a five-level evolutionary path of increasingly organized and systematically more mature processes. A key benefit of the CMMI is that it establishes a framework for continuous process improvement.

SecureTrust Five Maturity Levels

The five Compliance Intelligence levels, based on CMMI, are:

- **Level 1**
  At the initial level, processes are disorganized, even chaotic. Success is likely to depend on individual efforts, and is not considered to be repeatable, because processes would not be sufficiently defined and documented to allow them to be replicated.
- **Level 2**
  At the repeatable level, basic project management techniques are established, and successes could be repeated, because the requisite processes would have been made established, defined, and documented.
- **Level 3**
  At the defined level, an organization has developed its own standard process through greater attention to documentation, standardization, and integration.
- **Level 4**
  At the managed level, an organization monitors and controls its own processes through data collection and analysis.
- **Level 5**
  At the optimizing level, processes are constantly being improved through monitoring feedback from current processes and introducing innovative processes to better serve the organization's particular needs.

The spider graph below provides easy visualization of an example organization's current state (the red line) versus its goal state (the green line). The blue lines show how the organization compares with two model organizations in their industry. This kind of graphing can help an organization understand where they are overinvesting or underinvesting.



Example mapping of organizational capability maturity

Key Considerations for Every Organization

When developing or re-evaluating your risk assessment model for your organization, it is imperative that you have executive sponsorship and support throughout the process. Because ultimately, senior management has to acknowledge and accept risks inherent within the organization.

The individual who is responsible for the risk assessment, whether Chief Information Security Officer (CISO) or Chief Information Officer (CIO) or other, needs to be part of the executive management team or have a direct channel of communication to it. This is important to ensure that the business implications of the threats and vulnerabilities to critical technology and information assets are fully understood by business leadership.

For the execution of the risk assessment, the CISO office may lead, but it should be acknowledged throughout the organization that security is everyone's responsibility and that everyone's participation is required for security to work.

At the same time that the importance of security is emphasized from the top levels down through the entire organization, it must also be acknowledged that "perfect security" is not achievable. Your organization's goal should be to have the correct or optimum level of security for the organization.

As discussed earlier, each organization must accept that they are at risk and plan for a breach.

Summary

Just as it is common for an organization to have a security infrastructure that is a hybrid of standard security frameworks, a risk assessment framework may be a hybrid of different approaches. The overall result, however, must address the objective of a seamless, comprehensive, appropriate and actionable assessment that takes all current internal and external risk factors and dynamics into consideration.

Your risk assessment should follow these overall guidelines:

- Make sure that the individual who is responsible for the risk assessment, whether Chief Information Security Officer (CISO) or Chief Information Officer (CIO) or other, is part of the executive management team or has a direct channel of communication to it.
- A risk assessment should begin with a clear understanding of your organization's business goals, potential threats, likelihood of compromise and the impact of the loss.
- Evaluate your security framework in light of the level of risk that you have determined to be appropriate for your organization and its key assets.
- Make sure that the outcome of the risk assessment is the development of an effective risk-mitigation and data-protection strategy that addresses your entire organization, including mobile workers, third-party vendors and supply chain partners.
- Recognize that in today's threat environment your organization will be or has already been breached and there is no perfect security system that will prevent that. The best strategy is to put state-of-the-art protections in place while making sure that you have an appropriate focus on swift breach detection, response and recovery.
- Create a roadmap for the evolution of your Capability Maturity Model with the ultimate goal of continuous process improvement through monitoring feedback from current processes while introducing innovations to meet your organization's needs.

How SecureTrust Can Help

SecureTrust has developed a proprietary and proven Risk Assessment methodology based on its deep multi-compliance and security expertise. The Risk Assessment methodology may be executed for a number of industry standards including the NIST Cybersecurity Framework, NIST SP 800-30, ISO 27005, OCTAVE, and COBIT. The specific risk methodology Trustwave uses will vary according to the size, complexity and needs of your organization.

We also offer a dedicated PCI risk assessment service. The SecureTrust PCI Plus Risk Assessment enables your organization to execute a security strategy that focuses on continuous compliance.

After considering the risks in today's evolving threat landscape and prioritizing protection efforts, customers will emerge with a defense strategy that fulfills and exceeds PCI DSS requirements. PCI Plus allows you to:

- Strengthen segmentation and security between the corporate environment and the cardholder data environment (CDE)
- Know, exactly, where cardholder data lies and when the environment or data changes
- Increase the likelihood of incident detection at the time of (or soon after) a security event

To learn more, see **Risk Assessments** and **PCI Plus Risk Assessments**.

Sources

www.nist.gov/
nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
www.nist.gov/cyberframework/draft-version-11
www.isaca.org/COBIT/Pages/default.aspx
www.iso.org/home.html
www.cert.org/resilience/products-services/octave/
www.pcisecuritystandards.org/pci_security/maintaining_payment_security
www.pcisecuritystandards.org/pci_security/standards_overview