PCI Security Standards Council®

New vs. New

Exploring PCI DSS v4.0 and ISO/IEC 27001:2022

Yan Liu

Principal Consultant, PCI QSA, QPA, PFI, SSF Assessor
atsec information security

the information security provider

Guohua Shen

Principal Consultant, ISMS Auditor, PMP
atsec information security

the information security provider

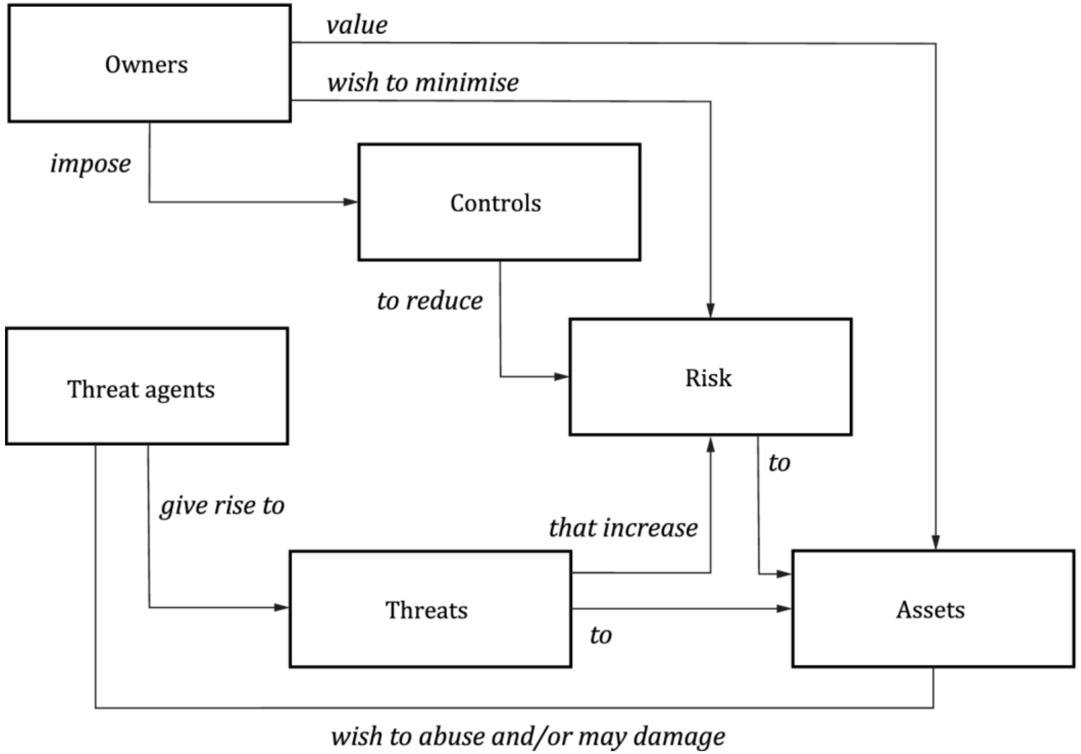
PCI Security Standards Council®

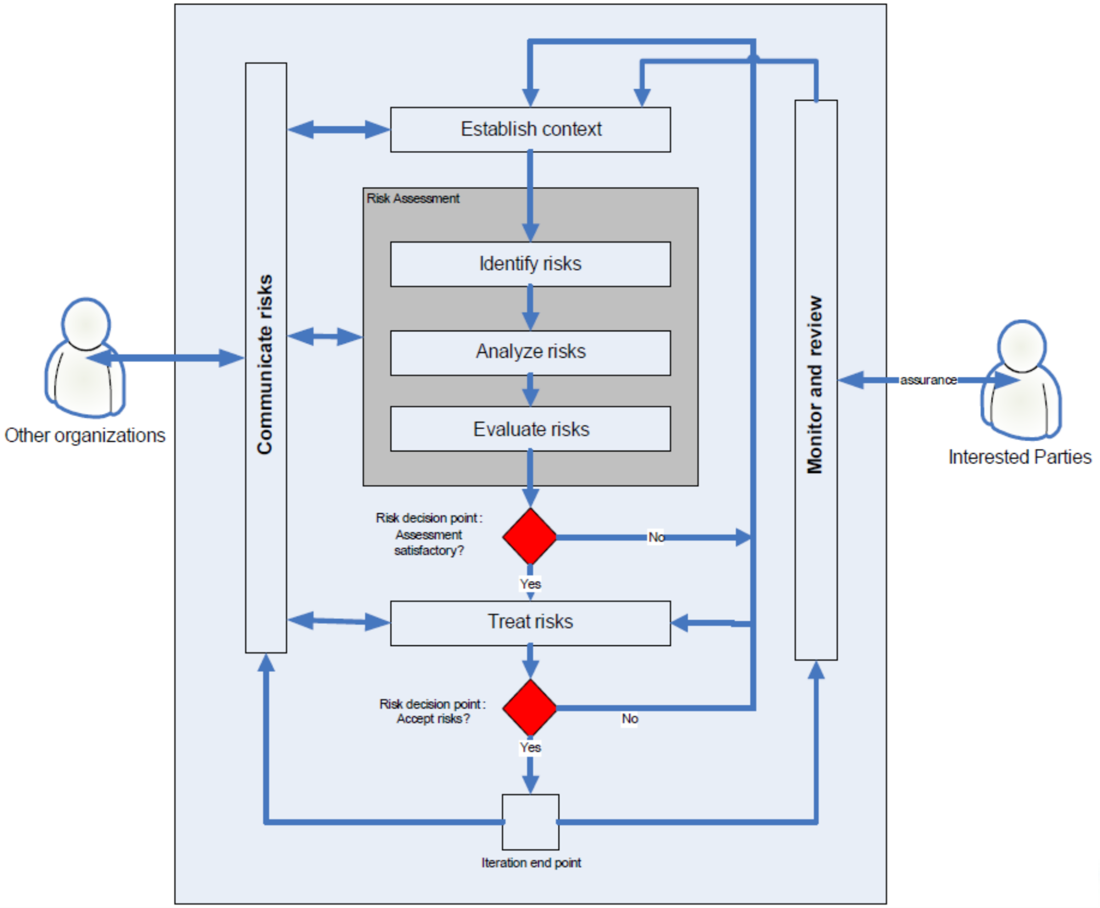
Content

- Risk management concept
- Defined Approach vs. Risk-based Approach
- Requirements on Data protection and Risk assessment
- Integrated management system
- Case studies
- Summary

Resuming the Discussion from Risk Management

Concepts and relationships defined in
Common Criteria and ISO/IEC 27005: 2022





Risk management process

PCI Security Standards Council®

@SEC the information security provider

Defined Approach vs. Risk-based Approach

- “PCI DSS provides clear and direct security requirements (defined approach), and it helps us to push the security implementation internally.”
  - by a CISO of a payment SP in 2010
- Risk-based approaches could be used, including Compensating Control, as well as Customized Approach (introduced in new PCI DSS v4.0)
- How to track the issues found during an initial assessment more effectively?

- Statement of Applicability
- Risk-based approaches were widely used for being compliant with standards like ISO/IEC 27001 (used for certifying information security management systems)
  - Avoiding the risk
  - Reducing the risk to an acceptable level
  - Transferring the risk
  - Accepting the residual Risk
- Corrective action

Compensating Control Used in PCI DSS (v4.0 and earlier)

An actual example for addressing Requirement 4.2.1

- Constrains: If HTTPS TLS 1.0/1.1 in xxx.com is disabled, those cardholders/merchants using legacy Internet browser versions and/or legacy mobile phone OSs could be blocked, and the payment authorization process could be affected.

- Definition of Compensating Control: The use of TLS version 1.0/1.1 may result in being exploited with known vulnerabilities and, thus, data disclosure. The compensating controls are defined below:
  - Strong cryptographic algorithms with ECDH: The risk of exploitation against insecure cipher suits in TLS version 1.0/1.1 and data disclosure are reduced
  - Implement data encryption for an additional layer
  - Cardholders/merchants are advised to address the security issues of TLS version 1.0/1.1
  - Monitor the usage of TLS version 1.0/1.1 for affected URLs and define the business acceptable percentage. Once the usage reaches the acceptable percentage, the entity disables the support of TLS version 1.0/1.1

- *“Objective, Identified Risk, Validation of CC, Maintenance” are stripped for this CCW example.*

Risk analysis is considered behind the development of the Compensating Control.

Introduction to ISO/IEC 27001:2022

- **ISO/IEC 27001** is a standard for Information Security Management System (ISMS) requirements.

Features of ISO/IEC 27001	Corresponding in PCI DSS
Composed of **documented information**, including policies, procedures, guidelines, etc.	Maintain an Information Security Policy
Focused on protecting the **confidentiality, integrity, and availability of assets.**	Protection of account data.
Based on risk assessment.	Targeted Risk Analysis
Implemented through controls.	Defined Approach.

- **ISO/IEC 27001:2022** version was published in October 2022, with a transition period until October 2025.
  - The scope was extended from information security to encompass information security, cybersecurity, and privacy protection.
  - The controls in Annex A were reorganized, and some new controls were added.

PCI DSS v4.0 vs. ISO/IEC 27001:2022 (1)

How to handle non-fulfillment of standard requirements?

- **Customized Approach (New)**
  - Focuses on each PCI DSS requirement's objective, allowing entities to meet the customized objective without strictly following the defined requirement.
- **Compensating Control**
  - As part of the Defined Approach, entities facing constraints may implement alternative or compensating controls to mitigate the risk if they cannot meet a PCI DSS requirement as stated.
- They both focus on entities that cannot meet the Defined Approach directly.

- **Nonconformity**
  - Non-fulfilment of a requirement, including standards, and/or entities' internal policies.
- **Correction**
  - Action to eliminate a detected nonconformity.
- **Corrective Action**
  - Action to eliminate the cause of a nonconformity and to prevent recurrence.
- They are part of a single process to detect and eliminate non-fulfillment of requirements.

PCI DSS v4.0 vs. ISO/IEC 27001:2022 (2)

The new privacy protection controls in ISO/IEC 27001:2022

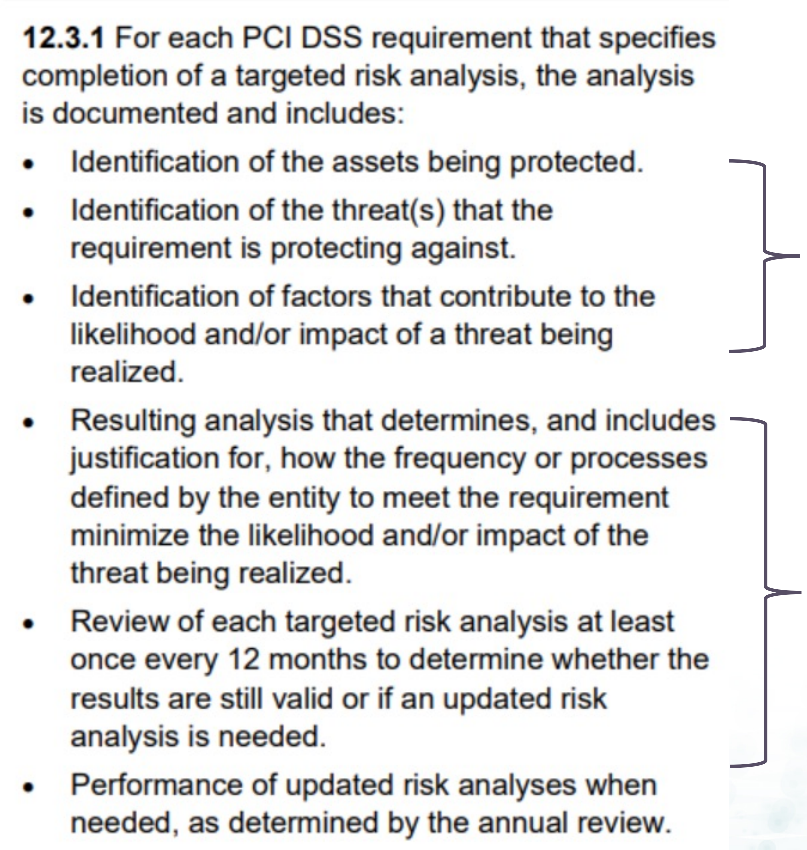
- The 2022 version of ISO/IEC 27001 added privacy protection controls, which may include account data as defined in PCI DSS.

PCI DSS V4.0.1	ISO/IEC 27001:2022
3.2 Storage of account data is kept to a minimum.	Annex A 8.10 Information deletion (New)
3.4 Access to displays of full PAN and ability to copy PAN are restricted.	Annex A 8.11 Data masking (New)
(New) 3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need. (New) 12.10.7 Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected.	Annex A 8.12 Data leakage prevention (New)

PCI DSS v4.0 vs. ISO/IEC 27001:2022 (3)

Risk Assessment

- Risk Assessment is important for both PCI DSS and ISO/IEC 27001.

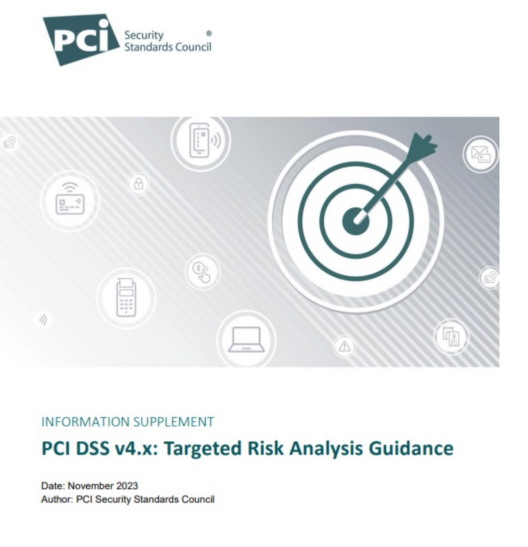


12.3.1 For each PCI DSS requirement that specifies completion of a targeted risk analysis, the analysis is documented and includes:

- Identification of the assets being protected.
- Identification of the threat(s) that the requirement is protecting against.
- Identification of factors that contribute to the likelihood and/or impact of a threat being realized.
- Resulting analysis that determines, and includes justification for, how the frequency or processes defined by the entity to meet the requirement minimize the likelihood and/or impact of the threat being realized.
- Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed.
- Performance of updated risk analyses when needed, as determined by the annual review.

The same methodology as ISO/IEC 27001:2022 is used to identify risks by asset, threat, and vulnerability, as well as to evaluate risks by impact and likelihood.

The unique risk assessment methodology (Targeted Risk Analysis) of PCI DSS is used to determine the necessary frequency or processes.



INFORMATION SUPPLEMENT

PCI DSS v4.x: Targeted Risk Analysis Guidance

Date: November 2023
Author: PCI Security Standards Council

How to Integrate PCI DSS and ISO/IEC 27001

Principle – Combined ISMS integrated with PCI DSS & ISO/IEC 27001

- **Before:** Organize ISMS based on Appendix A of ISO/IEC 27001:2013 and incorporate the standards of PCI DSS.

- **After:** Due to the reorganization of ISO/IEC 27001:2022 Appendix A, the organization of ISMS is more flexible. It is suggested to use the Operational Capabilities attributes defined in ISO/IEC 27002:2022, which are:

1. Governance	2. Asset management	3. Information protection	4.Human resource security	5. Physical security
6. System and network security	7. Application security	8. Secure configuration	9. Identity and access management	10. Threat and vulnerability management
11. Continuity	12. Supplier relationships security	13. Legal and compliance	14. Information security event management	15. Information security assurance

How to Integrate PCI DSS and ISO/IEC 27001

Challenge - Scope

- The scope required to comply with PCI DSS and ISO/IEC 27001 often differs, so the compliance requirements for different system components also vary.
- It is important to identify the scope of compliance for PCI DSS and ISO/IEC 27001 and to adopt appropriate integration measures.
  - **Scenario 1: If the scopes are the same**. PCI DSS requirements can be integrated into the ISMS documentation based on ISO/IEC 27001 on a requirement-by-requirement basis.
  - **Scenario 2: If the scopes differ, typically the scope of PCI DSS is encompassed within that of ISO/IEC 27001**. Since PCI DSS requirements are generally stricter and more detailed than those established by ISO/IEC 27001, it is usually recommended to create a separate policy to address and implement the PCI DSS requirements.

Case Study – Scenario 1

An independent payment provider located in Shanghai, China

- In this case, the company established an ISMS based on ISO/IEC 27001 and integrated the PCI DSS requirements into the ISMS on a requirement-by-requirement basis. The relationship between the two standards was also documented in the *“ISMS.S4.SP.003 Controlled Document List”.*

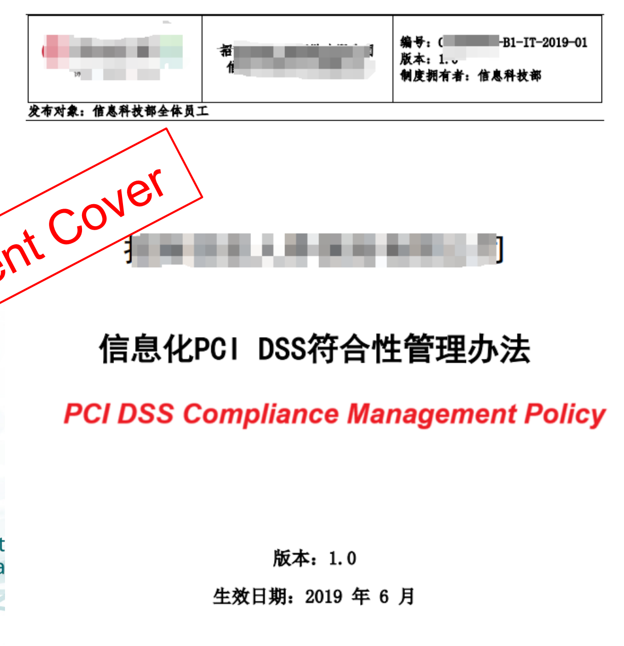
The ISMS documents	PCI DSS compliance (V4.0)
ISMS.S2.SP.001 Risk Assessment and Treatment Procedures	12.3
ISMS.S2.HR.001 Human Resources Security Management Policy	12.1.3, 12.6, 12.7
ISMS.S2.LA.001 User Access Control Management Policy	7
ISMS.S3.LA.001 Guidelines for User Identification and Password Management	8

Part of *“PCI DSS Compliance Mapping Table”*

Case Study – Scenario 2

An insurance company located in Shenzhen, China

- In this case, the company added a new document titled *“PCI DSS Compliance Management Policy”* specifically for PCI DSS compliance to its existing ISMS and also created a *“PCI DSS Compliance Mapping Table”* to describe the relationship between the two standards.



[redacted]	[redacted]	编号：[redacted]-B1-IT-2019-01 版本：1. 制度拥有者：信息科技部

发布对象：信息科技部全体员工

[redacted]

信息化PCI DSS符合性管理办法

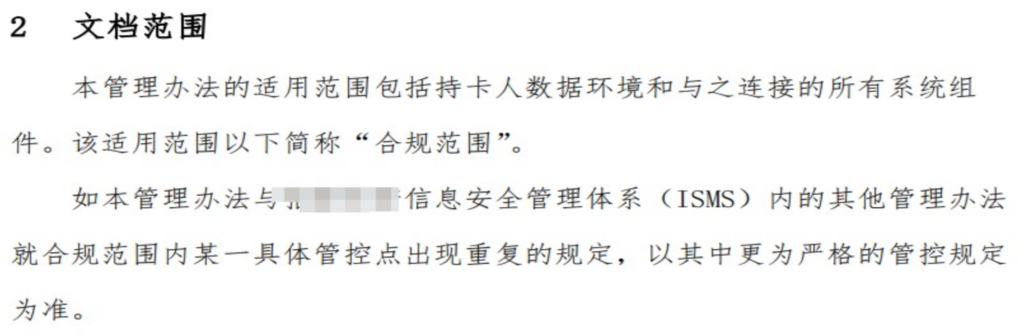
PCI DSS Compliance Management Policy

版本：1.0

生效日期：2019 年 6 月

Document Cover

- The scope of the *“PCI DSS Compliance Management Policy”* within the ISMS framework is defined as follows.



2　文档范围

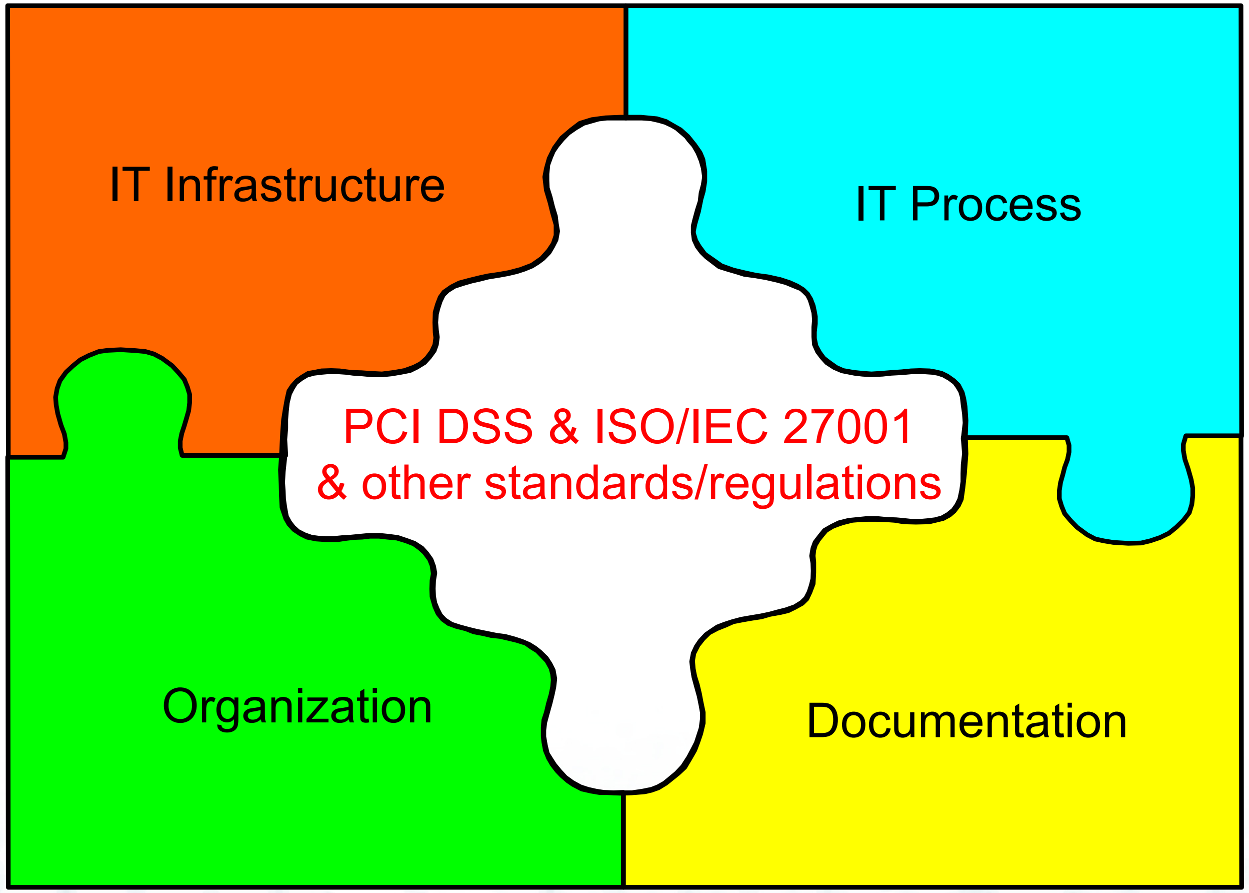
本管理办法的适用范围包括持卡人数据环境和与之连接的所有系统组件。该适用范围以下简称“合规范围”。

如本管理办法与[redacted]信息安全管理体系（ISMS）内的其他管理办法就合规范围内某一具体管控点出现重复的规定，以其中更为严格的管控规定为准。

If there are overlapping regulations regarding a specific control within the scope of the PCI DSS policy and other policies in the ISMS, the stricter control regulation shall prevail.

Takeaways

- The defined approach is always important for most of organizations in the payment industry, especially middle or small size organizations
- Suggest implementing an organization-specific and unique Management System to meet related industry requirements by introducing the risk management methodology
- The goal of compliance assessment or audit is for security improvement.
  Not just for an attestation or certificate.



PCI Security Standards Council®