

IS4231

Information Security Management

Lecture 7

Security Management Models

AY 2021/2022 Semester 1

Lecturer: Dr. YANG Lu

Reading: Chapter 8

Learning Objectives

- ▶ Describe the prevalent information security management models that can be used as security frameworks
 - ▶ These are the security frameworks you start with
- ▶ Lower Level Security Models
 - ▶ These are used to help flesh out aspects of the framework
 - ▶ Types of models
 - ▶ Security evaluation models

Security Management Models

Security Management Models

▶ Sources

- ▶ Public domain sources
- ▶ Proprietary models

▶ Models

- ▶ ISO/IEC 27000 series
- ▶ NIST security models
- ▶ COBIT
- ▶ PCI DSS
- ▶ ISF the Standards
- ▶ CIS Standards
- ▶ Others

ISO/IEC 27000 series

ISO/IEC 27000 Series

- ▶ Deal specifically with InfoSec matters
 - ▶ Deliberately broad in scope so that it can be used by organizations of all sizes and kinds
 - ▶ Use it to guide assessment of InfoSec risks, then implement security controls appropriate to their needs
 - ▶ Full standards list:
 - ▶ <https://www.iso27001security.com/html/iso27000.html>

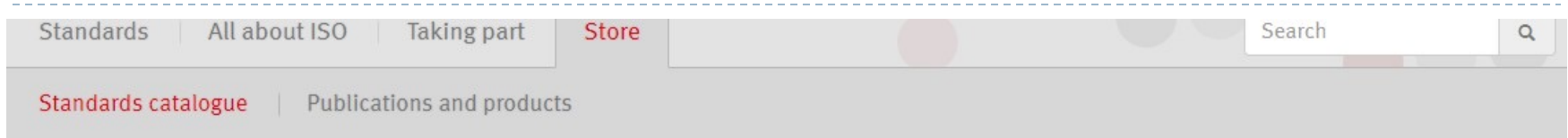
ISO 27000 Series Samples

- ▶ 27000: Overview and vocabulary
- ▶ 27001: InfoSec Mgmt System Specification
- ▶ 27002: Code of Practice for InfoSec Mgmt
- ▶ 27003: InfoSec Mgmt Systems Implementation Guidance
- ▶ 27004: InfoSec Measurements
- ▶ 27005: ISMS Risk Management
- ▶ 27006: Requirements for Bodies Providing Audit and Certification of an ISMS
- ▶ 27007: Guidelines for ISMS Auditing
- ▶ 27008: Guidelines for InfoSec Auditing
- ▶ 27010: Guidelines for Inter-sector and Inter-organizational Communications
- ▶ 27011: Guidelines for Telecomm orgs
- ▶ 27013: Guideline on the Integrated Implementation of ISO/IEC 20000-1 and ISO/IEC 27001
- ▶ 27014: InfoSec Governance Framework
- ▶ 27015: InfoSec Mgmt Guidelines for Financial Services
- ▶ 27016: InfoSec and Organizational Economics
- ▶ 27017: Code of practice for InfoSec controls for cloud computing services based on ISO/IEC 27002
- ▶ 27018: Code of practice for PII protection in public clouds acting as PII processors
- ▶ 27023: Mapping the revised editions of ISO/IEC 27001 and 27002
- ▶ 27031: Guidelines for information and communication technology readiness for business continuity
- ▶ 27032: Guidelines for cybersecurity
- ▶ 27033: Network security
- ▶ 27034: Application security
- ▶ 27701: *The international standard for privacy information management*

ISO/IEC 27001

- ▶ ISO/IEC 27001:2013 - “Information Technology - Security techniques - Information security management systems - Requirements”
 - ▶ Latest revision in 2013
 - ▶ Provides information for how to implement ISO/IEC 27002 and set up an Information Security Management System (ISMS)
 - ▶ Serves better as an assessment tool
 - ▶ Whether the organization system has meet with the security standards

ISO/IEC 27001 (cont.)



Home > Store > Standards catalogue > Browse by ICS > 03 > 03.100 > 03.100.70 > ISO/IEC 27001:2013

ISO/IEC 27001:2013

Preview

Information technology -- Security techniques -- Information security management systems -- Requirements

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

General information

Current status : Published

Publication date : 2013-10

Edition : 2

Number of pages : 23

Technical Committee : ISO/IEC JTC 1/SC 27 IT Security techniques

Buy this standard

Format	Language
<input checked="" type="checkbox"/> PDF + Color PDF + ePub	English ▼
<input type="checkbox"/> PDF + ePub	English ▼
<input type="checkbox"/> PDF + ePub + Redline	English ▼
<input type="checkbox"/> Paper	English ▼
<input type="checkbox"/> PDF	Arabic ▼

SGDI 73

CHF 118

Buy



Example: NUS



Information
Technology

[myEmail](#) [Staff Portal](#) [Student Portal](#) [nTouch](#)

[Home](#) [About](#) [Highlights](#) [Services](#) [Support](#) [Contact](#) [Join NUS!](#)



Achieved Information Security Management System (ISMS) Framework And ISO 27001 Certification

2009



Proudly achieved Information Security Management System (ISMS) framework and ISO 27001 certification on InfoComm security, network services, system services, database administration and data centre operations, and setting best practice in security management in Higher Education.

Estimated Certification Costs

Estimated ISO 27001 certification costs

The table below displays the recommended ISMS audit time according to the size of the organisation, as stipulated in ISO/IEC 27006:2015.

No. of people working for the organisation	No. of days** (Minimum audit time)	Estimated certification cost ***
1 - 45	3 - 6	£2850 - £5,700
46 - 125	7 - 8	£6,650 - £7,600
126-425	9 – 10	£8,550 - £9,500
426-625	11	£10,450
626-875	12	£11,400
876-1175	13	£12,350
1176-1550	14	£13,300
1551-2025	15	£14,250

Source: <https://www.itgovernance.co.uk/iso27001-certification-costs>

Example: Trend Micro


- ▶ The Trend Micro ISMS scope includes the following services:

Endpoint Application Control	Active Update
Deep Discovery Analyzer as a Service	Mobile App Reputation Service
Deep Discovery Analyzer as a Service Add-on	Cloud App Security
Deep Security as a Service	DirectPass
Email Reputation Service	Mobile Security
Web Reputation Service	Encryption Service
File Reputation Service	Remote Manager
Smart Protection Network	Worry-Free Business Security Service
Hosted Email Security	IoT Security
Hosted Mobile Security	Home Network Security
InterScan Web Security as a Service	Yamato Backend (VPN, NBA, ISC)
Apex One as a Service	Email Security
Product Licensing Service	Cloud Edge Cloud Management
Threat Investigation Center	Email Security Platform for Service Provider

ISO/IEC 27002

- ▶ ISO/IEC 27002:2013 - “Information Technology - Security techniques - Code of practice for information security management”
- ▶ One of the most widely referenced InfoSec management models
 - ▶ Originally published as British Standard BS 7799
 - ▶ Adopted as an international standard framework for InfoSec by the ISO and the IEC as ISO/IEC 17799
 - ▶ Last revised in 2013
- ▶ Gives best practice recommendations on InfoSec management to those initiating, implementing or maintaining InfoSec management systems

ISO/IEC 27002 (cont.)

- ▶ ISO/IEC 27002:2013 (the most last version)
 - ▶ Provides information on more than 100 controls over 14 security control clauses
 - ▶ For organizations that want information about implementing security controls.
 - ▶  Works as a *guidance document*

ISO/IEC 27002 (cont.)

▶ ISO/IEC 27002: 2013 structure

- ▶ 0. Introduction
- ▶ 1. Scope
- ▶ 2. Normative references
- ▶ 3. Terms and definitions
- ▶ 4. Structure of this standard
- ▶ 5. Information security policies
- ▶ 6. Organization of information security
- ▶ 7. Human resource security
- ▶ 8. Asset management
- ▶ 9. Access Control
- ▶ 10. Cryptography
- ▶ 11. Physical and environmental security
- ▶ 12. Operations security
- ▶ 13. Communication security
- ▶ 14. System acquisition, development, and maintenance
- ▶ 15. Supplier relationships
- ▶ 16. Information security incident management
- ▶ 17. Information security aspects of business continuity management
- ▶ 18. Compliance

ISO/IEC 27701

- ▶ ISO/IEC 27701:2019 – “Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for **privacy** information management - Requirements and guidelines”
 - ▶ A new standard in the ISO27000 series
 - ▶ It specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for *privacy management* within the context of the organization.
 - ▶ It specifies PIMS-related requirements and provides guidance for *PII controllers* and *PII processors* holding responsibility and accountability for PII processing.

help companies to comply with GDPR / PDPA

Discussions:

▶ Question:

- ▶ What kind of ISO 27000 standards should AWS, as a cloud service provider, be certified with?

AWS has certification for compliance with
ISO/IEC
27001:2013,
27017:2015,
27018:2019,
27701:2019,
9001:2015,
and CSA STAR CCM v3.0.1

CSA STAR Program

▶ CSA – Cloud Security Alliance

- ▶ A non-profit org whose mission is to “promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.”

▶ STAR – Security, Trust, Assurance, and Risk

- ▶ A program to help customers assess and select a Cloud Service Provider through a three-step program of self-assessment, third-party audit, and continuous monitoring.
- ▶ The certification leverages the requirements of the ISO/IEC 27001:2013 Information security management systems standards together with the CSA Cloud Control Matrix

CSA STAR Program (cont.)

- ▶ Reference documents

- ▶ CCM (Cloud Control Matrix)
- ▶ CAIQ (The Consensus Assessments Initiative Questionnaire)
 - ▶ Offers an industry-accepted way to document what security controls exist in IaaS, PaaS, and SaaS services, providing security control transparency

unlike ISO 27017 and 27018 which are proprietary - CSA STAR is free for referencing

NIST Security Models



The Power of Quantum Computing in Silicon

Can Mobile Networks Connect First Responders
in Remote Areas?

Roll-Up TVs and Bendable Smartphones
More Choices for Flexible Electronic Materials

About NIST

The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. Congress established the agency to remove a major challenge to U.S. industrial competitiveness at the time—a second-rate measurement infrastructure that lagged behind the capabilities of the United Kingdom, Germany, and other economic rivals.

From the smart electric power grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips, innumerable products and services rely in some way on technology, measurement, and standards provided by the National Institute of Standards and Technology.

Today, NIST measurements support the smallest of technologies to the largest and most complex of human-made creations—from nanoscale devices so tiny that tens of thousands can fit on the end of a single human hair up to earthquake-resistant skyscrapers and global communication networks.

NIST Security Models

- ▶ Two advantages over the ISO/IEC 27000 standards:
 - ▶ Freely available at no charge
 - ▶ They have been available for some time and thus have been broadly reviewed (and updated) by government and industry professionals
 - ▶ SP 800-12 Rev.1, *An Introduction to Information Security*
 - ▶ SP 800-30 Rev.1, *Guide for Conducting Risk Assessments*
 - ▶ SP 800-53 Rev.4, *Security and Privacy Controls for Federal Information Systems and Organizations*
 - ▶ SP 800-55 Rev.1, *Performance Measurement Guide for Information Security*
 - ▶ SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
 - ▶ SP 800-53 Rev.5, *Security and Privacy Controls for Information Systems and Organizations*
 - ▶ SP 800-171A, *Assessing Security Requirements for Controlled Unclassified Information*
 - <https://csrc.nist.gov/publications/sp800>

Examples:

► FIREEYE:



Privacy Shield certification Products Mandiant Solutions Customers Partners Resources Company

LEARN MORE >

NIST 800-171

National Institute of Standards and Technology Special Publication 800-171 was released in June 2015. It focuses on protecting the confidentiality of Controlled Unclassified Information (CUI) in non-federal information systems and organizations and defines security requirements to achieve that objective. FireEye has undergone a self-assessment that confirmed compliance with NIST 800-171 controls. FireEye continually evaluates compliance with NIST 800-171.

► AWS:

Is AWS compliant with the NIST 800-53 framework?



Yes, AWS Cloud infrastructure and services have been validated by third-party testing performed against the NIST 800-53 Revision 4 controls, as well as additional FedRAMP requirements. AWS has received FedRAMP Authorizations to Operate (ATO) from multiple authorizing agencies for both AWS GovCloud (US) and the AWS US East/West Region. For more information, see the [AWS FedRAMP compliance](#) webpage, or the following FedRAMP Marketplace webpages:

- [AWS East/West Region complete list of authorizing agencies](#)
- [AWS GovCloud \(US\) complete list of authorizing agencies](#)
- [AWS GovCloud JAB P-ATO at the high baseline](#)

COBIT

COBIT

their focus is on the Enterprise Risk - not just focused on security itself

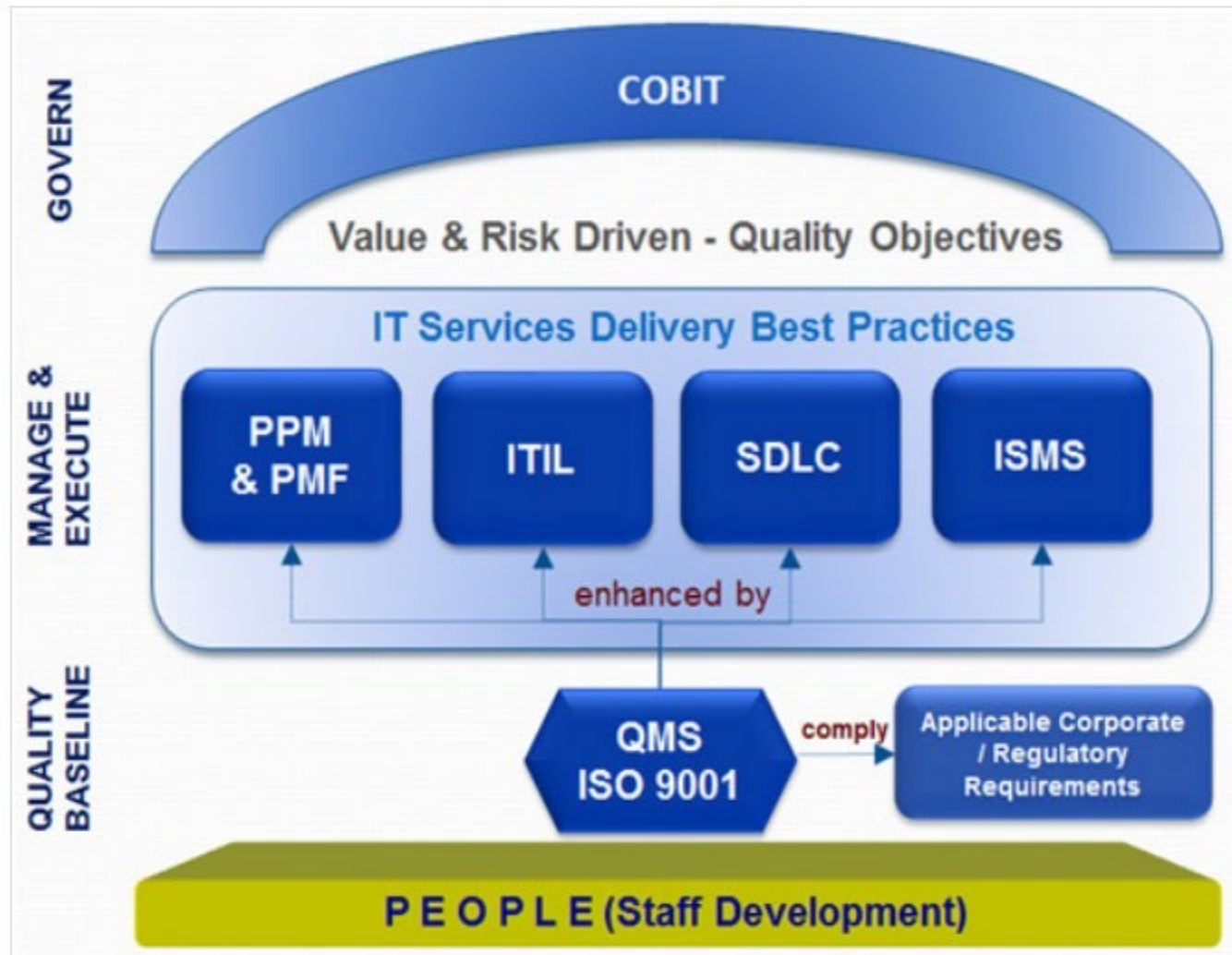
- ▶ **Control Objectives for Information and Related Technology”(COBIT)**
 - ▶ Provides advice about the implementation of sound controls and control objectives for InfoSec
 - ▶ Created in 1992 by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI)
- ▶ **COBIT 2019**
 - ▶ A Business framework for the governance and management of Enterprise IT

COBIT 2019

- ▶ Six principles focus on the governance and management of IT:
 - ▶ Principle 1: Provide stakeholders value
 - ▶ Principle 2: A holistic approach
 - ▶ Principle 3: Dynamic governance system
 - ▶ Principle 4: Governance distinct from management
 - ▶ Principle 5: Tailored to enterprise need
 - ▶ Principle 6: End-to-end governance system

Example: NUS

for an organisation - different models will help different aspects of the organisation and can pick and choose for specific areas to focus on



PCI DSS

PCI Industry Security Standards

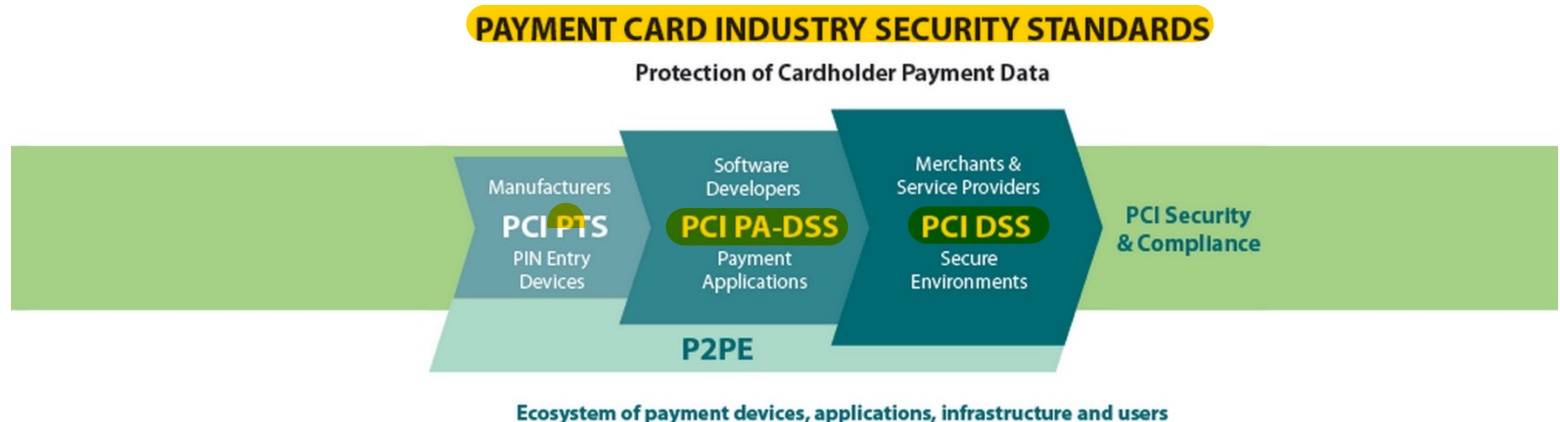
- ▶ **Payment Card Industry Data Security Standards**
 - ▶ A set of industry standards that are mandated for any organization that handle credit, debit and specialty payment cards.
 - ▶ Created by the Payment Card Industry Security Standards Council in an effort to reduce credit card fraud.
 - ▶ <https://www.pcisecuritystandards.org/>

The Council was founded in 2006 by American Express, Discover, JCB International, MasterCard and Visa Inc. They share equally in ownership, governance, and execution of the Council's work.



PCI Industry Security Standards (cont.)

- ▶ The PCI Data security standards help protect the safety of that data.
- ▶ They set the operational and technical requirements for *organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions.*



even a random store needs to ensure they are compliant with PCI PA-DSS

Source: https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

PCI DSS

- ▶ Includes three sets of documents
 - ▶ PCI DSS requirements and security assessment procedures (the Standards)
 - ▶ PCI DSS self-assessment (self-determined surveys to determine status of compliance), and documents for attestation of compliance
 - ▶ PCI DSS support documents (e.g., glossary, abbreviations and acronyms, reference guide)

more clear cut / specific standards as compared to ISO

PCI DSS (cont.)

► The standard focusing on 12 requirements in 6 areas

GOALS	PCI DSS REQUIREMENTS
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

PCI DSS (cont.)

- ▶ How do companies comply with PCI DSS?
 - ▶ Have an **external Qualified Security Assessor (QSA)** assess your applicable environment and then create a Report on Compliance (ROC) and Attestation of Compliance (AOC)
 - ▶ most common for entities that handle large volumes of transactions
 - ▶ Or, perform a Self-Assessment Questionnaire (SAQ)
 - ▶ most common for entities that handle smaller volumes of transaction
- ▶ Certificate validity
 - ▶ Valid for 1 year from the date the certificate is issued.
 - ▶ E.g., PayPal, Lazada, GrabPay
 - <https://www.paypal.com/sg/webapps/mpp/pci-compliance>
 - <https://www.grab.com/sg/pay/security/>

PCI DSS (cont.)

▶ Merchant compliance levels:

- ▶ E.g., level 1, level 2, level 3, level 4
- ▶ Depends on the merchant level (i.e., transaction volume) and slightly varies across different credit card companies (e.g., Visa, MasterCard, AMEX)
 - ▶ Taking VISA as example:

Merchant Level	Description
1	Any merchant — regardless of acceptance channel — processing over 6M Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.
2	Any merchant — regardless of acceptance channel — processing 1M to 6M Visa transactions per year.
3	Any merchant processing 20,000 to 1M Visa e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants — regardless of acceptance channel — processing up to 1M Visa transactions per year.

PCI DSS – VISA Standards

- ✓ Merchants processing over 6 million Visa transactions annually across all channels or Global merchants identified as Level 1 by any Visa region – Level 1

Every year:

- File a Report on Compliance ("ROC") by a Qualified Security Assessor ("QSA") or Internal Auditor if signed by an officer of the company. We recommend the internal auditor obtain the PCI SSC Internal Security Assessor ("ISA") certification.
- Submit an Attestation of Compliance ("AOC") Form

Every quarter:

- Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")

similar to FTC order for zoom

- ✓ 1 to 6 million Visa transactions annually across all channels – Level 2

Every year:

- Complete a Self-Assessment Questionnaire ("SAQ")
- Submit an Attestation of Compliance ("AOC") Form

Every quarter:

- Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")

- ✓ 20,000 to 1 million Visa e-commerce transactions annually – Level 3

Every year:

- Complete a Self-Assessment Questionnaire ("SAQ")
- Submit an Attestation of Compliance ("AOC") Form

Every quarter:

- Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")

- ✓ Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually – Level 4

Every year:

- Complete a Self-Assessment Questionnaire ("SAQ")
- Submit an Attestation of Compliance ("AOC") Form

Every quarter:

- Conduct a quarterly network scan by an Approved Scan Vendor ("ASV") (if applicable)



PCI DSS (cont.) – Mastercard Standards

Site data protection merchant levels

Category	Criteria	Requirements
Level 1	<ul style="list-style-type: none">Any merchant that has suffered a hack or an attack that resulted in an Account Data Compromise (ADC) EventAny merchant having more than six million total combined Mastercard and Maestro transactions annuallyAny merchant meeting the Level 1 criteria of VisaAny merchant that Mastercard, in its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the system	<ul style="list-style-type: none">Annual PCI DSS assessment resulting in the completion of a Report on Compliance (ROC)¹
Level 2	<ul style="list-style-type: none">Any merchant with more than one million but less than or equal to six million total combined Mastercard and Maestro transactions annuallyAny merchant meeting the Level 2 criteria of Visa	<ul style="list-style-type: none">Annual Self-Assessment Questionnaire (SAQ)²
Level 3	<ul style="list-style-type: none">Any merchant with more than 20,000 combined Mastercard and Maestro e-commerce transactions annually but less than or equal to one million total combined Mastercard and Maestro e-commerce transactions annuallyAny merchant meeting the Level 3 criteria of Visa	<ul style="list-style-type: none">Annual Self-Assessment Questionnaire (SAQ)³
Level 4	<ul style="list-style-type: none">All other merchants⁴	<ul style="list-style-type: none">Annual Self-Assessment Questionnaire (SAQ)³

PCI DSS (cont.)

▶ Self-validation tool

▶ Self-Assessment Questionnaire (SAQ)

- ▶ Ideal for small merchants and service providers that are not required to submit a report on compliance, to assess their level of cardholder data security

▶ Levels

- ☐ A - simplest
- ☐ A-EP
- ☐ B
- ☐ B-IP
- ☐ C-VT
- ☐ C
- ☐ P2PE-HW
- ☐ D - most complicated

depending on the business on how they handle transactions or how they design their payment systems

Other Security Management Models

- ▶ **ISF** Standard of Good Practice for Information Security
 - ▶ ISF: Information Security Forum
 - ▶ <https://www.securityforum.org/>
 - ▶ Founded in 1989, an independent, not-for-profit association
 - ▶ Comprehensive coverage of information security controls and information risk-related guidance.
 - ▶ ISF Benchmarks

- ▶ **CIS Cybersecurity Best Practices**
 - ▶ CIS: Center for Internet Security
 - ▶ <https://www.cisecurity.org/>
 - ▶ Founded in 2000, a non-for-profit entity
 - ▶ CIS Controls and CIS Benchmarks

Other Security Management Models (cont.)

- ▶ The Information Technology Infrastructure Library (ITIL)
 - ▶ A collection of methods and practices useful for managing the development and operation of information technology infrastructures
 - ▶ E.g.,
 - Incident management
 - Change management
 - Problem management
 - Service-level management
 - Continuity management
 - Configuration management
 - Release management
 - Capacity management
 - Financial management
 - Availability management
 - Security management
 - Help desk management
 - Knowledge management
 - ▶ The ITIL has been produced as *a series of books*, each of which covers an IT management topic

Lower Level Security Models



Security Architecture Evaluation Models

- Common Criteria

Common Criteria

- ▶ **Common Criteria for Information Technology Security Evaluation** - an international standard for computer security certification
 - ▶ Often called “Common Criteria” or “CC”
 - ▶ International standard for computer security certification (ISO/IEC 15408)
 - ▶ <https://www.commoncriteriaportal.org/>
- ▶ **Downsides of CC certification**
 - ▶ Certification process can be lengthy, costly, not timely
 - ▶ Certification of a system doesn't necessarily mean that it is completely secure

heavily requires documentation for them to check

Common Criteria (cont.)

Common Criteria

LOGIN →

HOME ABOUT THE CC PUBLICATIONS TECHNICAL COMMUNITIES CERTIFIED PRODUCTS COLLABORATIVE PPS PROTECTION PROFILES ICC NEWS

THE COMMON CRITERIA

Common Criteria

The [Common Criteria for Information Technology Security Evaluation](#) (CC), and the companion [Common Methodology for Information Technology Security Evaluation](#) (CEM) are the technical basis for an international agreement, the [Common Criteria Recognition Arrangement](#) (CCRA), which ensures that:

- [Products](#) can be evaluated by competent and independent [licensed laboratories](#) so as to determine the fulfilment of particular security properties, to a certain extent or assurance;
- [Supporting documents](#), are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies;
- The certification of the security properties of an evaluated product can be issued by a number of [Certificate Authorizing Schemes](#), with this certification being based on the result of their evaluation;
- [These certificates](#) are recognized by all the signatories of the [CCRA](#).

The CC is the driving force for the widest available mutual recognition of secure IT products. This web portal is available to support the information on the status of the CCRA, the CC and the certification schemes, licensed laboratories, certified products and related information, news and events.




Certificate Authorizing Members

Certificate Consuming Members

meanwhile China has their own standard - do not use CC

Common Criteria (cont.)

▶ CC terminology

- ▶ Target of evaluation (ToE)-the system being evaluated
 - ▶ Protection profile (PP)  ser-generated specification for security requirements
 - ▶ Security target (ST)  document describing the ToE's security properties  the relationship btwn PP and ST
 - ▶ Security functional requirement (SERs)-catalog of a product's security function
 - ▶ Evaluation assurance level (EAL)-the rating or grading of a ToE after evaluation
-
- ▶ The Target of Evaluation (i.e., system being evaluated) is awarded an Evaluation Assurance Level (EAL)

Common Criteria (cont.)

- ▶ CC EAL scale (lowest to highest assurance):
 - *EAL1:FunctionallyTested*
 - *EAL2:StructurallyTested*
 - *EAL3:MethodicallyTested and Checked*
 - *EAL4: Methodically Designed,Tested,and Reviewed*
 - *EAL5:Semi-formally Designed andTested*
 - *EAL6:Semi-formallyVerified Design andTested*
 - *EAL7:FormallyVerified Design andTested*

The level allocated is by company choosing which level they want to be tested against

CSA Common Criteria

About the Common Criteria (CC)

The genesis of CC was developed through a collaboration among national security and standards organisations in Canada, France, Germany, the Netherlands, the United Kingdom and the United States as a common standard to replace their existing security evaluation criteria.

The CC is now recognised as the ISO/IEC 15408. The CC is adopted by members of the Common Criteria Recognition Arrangement (CCRA) in order to facilitate mutual recognition of evaluation and certification results. As a result, consumers can benefit from having a wider choice of CC certified IT products, and developers will benefit from having greater access to markets and understanding of the security requirements (described in the form of collaborative Protection Profiles). The CC harmonises the evaluation of IT products by defining a common set of security functions which product developers use to establish the security requirements of their IT products in a standardised language. The Common Methodology for IT Security Evaluation (CEM) (ISO/IEC 18045) is used for evaluating the product against the established security requirements, confirming that the product is capable of meeting these requirements with an appropriate level of assurance.

The Singapore Common Criteria Scheme (SCCS) is established to provide a cost effective regime for the information communications industry to evaluate and certify their IT products against the CC standard in Singapore. The SCCS is owned and managed by the Cyber Security Agency of Singapore (CSA).

Discussion

- ▶ Any Trend Micro product is certified under CC scheme?

CC EAL2+ for Deep Security and Tipping Point (2 products)



CSA Cybersecurity Labelling Scheme

- ▶ An initiative under the *Safer Cyberspace Masterplan SG*
 - ▶ Scope
 - ▶ Network-connected smart devices
 - ▶ Labelling scheme
 - ▶ It will provide an indication of the level of security that is embedded in the products, based on a series of assessment and tests on:
 - a. Meeting basic security requirements such as ensuring unique default passwords,
 - b. adherence to the principles of Security-by-Design, [Related to DevSec Ops](#)
 - c. absence of common software vulnerabilities, and
 - d. resistance to basic penetration testing
 - ▶ Benchmark
 - ▶ Will be aligned with European Standard EN 303 645 'Cyber Security for Consumer Internet of Things'.

CSA Cybersecurity Labelling Scheme (cont.)

▶ Product list

- ▶ <https://www.csa.gov.sg/Programmes/cybersecurity-labelling/Product-List>
- ▶ E.g.,
 - ▶ TraceTogether Token
 - ▶ Nest Wifi Router H2D

CREST

- ▶ A not-for-profit accreditation body that represents and supports the technical information security market.
- ▶ What it provides?
 - ▶ Internationally recognized accreditation for organizations and individuals providing penetration testing, cyber incident response and threat intelligence services.
 - ▶ The de factor standard in UK and Australia

different regions will have different standards



Next Week

- ▶ Risk Management – Assessing Risk
 - ▶ Chapter 6