ISO/IEC JTC 1/SC 27/WG 4 Standards Application against Advanced Cybersecurity Attacks

Jinghua Min, CEC (China)
2018-08-28

Scope of SC 27/WG 4

- The scope of ISO/IEC JTC 1/SC 27/WG4 covers aspects related to security controls and services, emphasizing standards for IT security and its application to the security of products and systems in information systems, as well as the security in the lifecycle of such products and systems.

Topics of SC 27/WG 4

- ICT security operations
  - e.g. readiness, continuity, incident and event management, investigation
- Information lifecycle
  - e.g. creation, processing, storage, transmission and disposal
- Organizational processes
  - e.g. design, acquisition, development and supply
- Security aspects of Trusted services
  - e.g. in the provision, operation and management of these services
- Cloud, internet and cyber security related technologies and architectures
  - e.g. network, virtualization, storage, big data, IoT

for digital environments, such as: Cloud computing, Cyber, Internet, Organizations

ICT security operations

- ISO/IEC 27031 Information technology – Security techniques – Guidelines for ICT readiness for business continuity (1st ed.)
  —> Information technology – Cybersecurity – Information and communication technology readiness for business continuity (revision)
- ISO/IEC 27035 Information technology – Security techniques – Information security incident management
  - Part 1: Principles of incident management
  - Part 2: Guidelines to plan and prepare for incident response
  - Part 3: Guidelines for incident response operations

ICT security operations cont.

- ISO/IEC 27037 Information technology – Security techniques – Guidelines for the identification, collection, acquisition and preservation of digital evidence
- ISO/IEC 27041 Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative methods
- ISO/IEC 27042 Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence

ICT security operations cont.

- ISO/IEC 27043 Information technology – Security techniques – Incident investigation principles and processes
- ISO/IEC 27050 Information technology – Security techniques – Electronic discovery
  - Part 1: Overview and concepts
  - Part 2: Guidance for governance and management of electronic discovery
  - Part 3: Code of Practice for electronic discovery
  - Part 4: Technical readiness
- SP Investigation of need for guidelines on Security Operation Center (SOC)

Information lifecycle

- ITU-T X.842 | ISO/IEC TR 14516 Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services
- ITU-T X.841 | ISO/IEC 15816 Information technology – Security techniques – Security information objects for access control
- ITU-T X.843 | ISO/IEC 15945 Information technology – Security techniques – Specification of TTP services to support the application of digital signatures

Information lifecycle cont.

- ISO/IEC 27038 Information technology – Security techniques – Specification for digital redaction
- ISO/IEC 27040 Information technology – Security techniques – Storage security
- ISO/IEC TR 29149 Information technology – Security techniques – Best practice on the provision and use of time-stamping services

Organizational processes

- ISO/IEC 27034 Information technology – Security techniques – Application security
  - Part 1: Overview and concepts
  - Part 2: Organization normative framework
  - Part 3: Application security
  - Part 4: Validation and verification
  - Part 5: Protocols and application security control data structure
  - Part 5-1: Protocols and application security control data structure – XML Schemas
  - Part 6: Case studies
  - Part 7: Assurance prediction framework

Organizational processes cont.

- ISO/IEC 27036 Information technology – Security techniques – Information security for supplier relationships
  - Part 1: Overview and concepts
  - Part 2: Requirements
  - Part 3: Guidelines for ICT supply chain security
  - Part 4: Guidelines for security of cloud services
- SP Provenance Model for Information Security Attribution and Accountability

Security aspects of Trusted services

- ISO/IEC 27070 Information technology – Security techniques – Security requirements for virtualized roots of trust
- SP Security recommendations for Trusted Connection based on hardware security models between devices and services
- SP Public key infrastructure

Cloud, internet and cyber security related technologies and architectures

- ISO/IEC 19086-4 Information technology – Cloud computing – Service level agreement (SLA) framework – Part 4: Components of security and of protection of PII
- ISO/IEC 20547-4 Information technology – Big data reference architecture – Part 4: Security and privacy
- ISO/IEC 21878 Information technology – Security techniques – Security guidelines for the design and implementation of virtualized servers

Cloud, internet and cyber security related technologies and architectures cont.

- ISO/IEC 27030 Information technology – Security techniques – Guidelines for security and privacy in Internet of Things (IoT)
- ISO/IEC 27032 Information technology – Security techniques – Guidelines for cybersecurity (1st ed.)
  —> Information technology – Cybersecurity – 213 Guidelines for Internet security (NWIP)

Cloud, internet and cyber security related technologies and architectures cont.

- ISO/IEC 27033 Information technology – Security techniques – Network Security
  - Part 1: Overview and concepts
  - Part 2: Guidelines for the design and implementation of network security
  - Part 3: Reference networking scenarios – Risks, design techniques and control issues
  - Part 4: Securing communications between networks using security gateways
  - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
  - Part 6: Securing wireless IP network access

Cloud, internet and cyber security related technologies and architectures cont.

- ISO/IEC 27039 Information technology – Security techniques – Selection, deployment and operation of intrusion detection and prevention systems (IDPS)
- ISO/IEC 27045 Information technology – Big data security and privacy – Processes
- ISO/IEC 27070 Information technology – Security techniques – Security requirements for establishing virtualized roots of trust

Cloud, internet and cyber security related technologies and architectures cont.

- SP Security recommendations for Trusted Connection based on hardware security models between devices and services
- SP Big data security and privacy – Guidelines for implementation
- SP Security Reference Model for Industrial Internet Platform (SRM-IIP)
- SP Security and privacy for IoT-Domotics

Risk management and cybersecurity at SC 27

- ISO/IEC 27005:2018 Information security risk management
- ISO/IEC TS 27100 Information technology – Cybersecurity – Overview and concepts (WG1)
- ISO/IEC TS 27101 Information technology – Cybersecurity – Framework development guidelines (WG1)
- ISO/IEC TR 27103:2018 Information technology – Security techniques – Cybersecurity and ISO and IEC Standards (WG1)
- ISO/IEC 27032 Information technology – Cybersecurity – Guidelines for Internet security (WG4)
- ISO/IEC 27031 Information technology – Cybersecurity – Information and communication technology readiness for business continuity (WG4)

Standards Application against Advanced Cybersecurity Attacks

- Cybersecurity processes against advanced cybersecurity attacks
  - – Understanding *through out the following processes*
  - – Plan & Preparation *before cybersecurity incidents*
  - – Detection & Decision *when cybersecurity incidents*
  - – Response & Recovery *during cybersecurity incidents*
  - – Investment & Improvement *after cybersecurity incidents*

Standards Application against Advanced Cybersecurity Attacks cont.

- Understanding of cybersecurity
  - Basic concepts related to cybersecurity for communication with the terms of same meaning
    - ISO/IEC TS 27100 Cybersecurity – Overview and concepts
  - Methodology to deal with cybersecurity
    - ISO/IEC TS 27101 Cybersecurity – Framework development guidelines
    - ISO/IEC TR 27103:2018 Cybersecurity and ISO and IEC Standards

Standards Application against Advanced Cybersecurity Attacks cont.

- Plan & Preparation for cybersecurity
  - Risk assessment
    - ISO/IEC 27005 Information security risk management
  - Safeguards for risk treatment
    - Cybersecurity
      - ISO/IEC 27031 Cybersecurity – ICT readiness for business continuity
      - ISO/IEC 27032 Cybersecurity – Guidelines for Internet security
    - Information security
      - ISO/IEC 27033 Network Security
      - ISO/IEC 27034 Application security
      - ISO/IEC 27036 Information security for supplier relationships
      - ISO/IEC 27038 Specification for digital redaction
      - ISO/IEC 27040 Storage security

Standards Application against Advanced Cybersecurity Attacks cont.

- Plan & Preparation for cybersecurity cont.
  - Safeguards for risk treatment cont.
    - Cloud computing security
      - ISO/IEC 19086-4 Cloud computing – Service level agreement (SLA) framework – Part 4: Components of security and of protection of PII
      - ISO/IEC 21878 Security guidelines for the design and implementation of virtualized servers
      - ISO/IEC 27070 Security requirements for establishing virtualized roots of trust
    - Big data security and privacy
      - ISO/IEC 20547-4 Big data reference architecture – Part 4: Security and privacy
      - ISO/IEC 27045 Big data security and privacy – Processes
    - Internet of Things (IoT) security and privacy
      - ISO/IEC 27030 Guidelines for security and privacy in IoT

Standards Application against Advanced Cybersecurity Attacks cont.

- Detection & Decision
  - ISO/IEC 27035 Information security incident management
  - ISO/IEC 27039 Selection, deployment and operation of intrusion detection and prevention systems (IDPS)
  - ISO/IEC 27050 Electronic discovery
- Response & Recovery
  - ISO/IEC 27035 Information security incident management
  - ISO/IEC 27039 Selection, deployment and operation of intrusion detection and prevention systems (IDPS)

Standards Application against Advanced Cybersecurity Attacks cont.

- Investment & Improvement
  - Investment to obtain evidence
    - ISO/IEC 27037 Guidelines for the identification, collection, acquisition and preservation of digital evidence
    - ISO/IEC 27041 Guidance on assuring suitability and adequacy of incident investigative methods
    - ISO/IEC 27042 Guidelines for the analysis and interpretation of digital evidence
    - ISO/IEC 27043 Incident investigation principles and processes
  - Lessons learnt for improvement
    - ISO/IEC 27035 Information security incident management

Thank you!