Malaysian Technical Standards Forum Bhd

TECHNICAL CODE:
INFORMATION AND NETWORK SECURITY - CLOUD SERVICE PROVIDER SELECTION

MCMC MTSFB TC G017:2018

AGENDA

- Document Scope, References & Structure
- Why Technical Code
- Target User
- Main Requirement for TC
- Summary for each clause
- Challenge Faced
- Acknowledgement

SCOPE

- Specifies requirements for selecting the cloud service provider for organisations in ensuring all security requirements are taken into account based on the assessment of the current environment and objectives.
- Registered date 15 Oct 2018

Why we need the TC?

- Provide a minimum baseline / guideline
- To be used as Internal Control/Compliance Checklist
- To educate on the potential risk and threat and mitigation controls

Target Audience

- Any organization that intend to move its data/services to from on-prem/local to Cloud environment
- IT Strategy Team
- IT Infra Team
- IT Security Team
- Business user

TC Main Structures

- Clause 1 : Introduction
- Clause 2: Scope
- Clause 3: Terms and definitions
- Clause 4: Abbreviations
- Clause 5: Cloud Computing service
- Clause 6: Organisation Assessment
- Clause 7: Selection Criteria
- Annex A : Cloud service model
- Annex B : Common information security threat
- Annex C: Cloud controls matrix
- Annex D: Compliance checklist for cloud service provider
- Annex E: Service level agreement responsibilities
- Annex F: Example of terms of services and privacy policy
- Bibliography

Clause 5 : Cloud Service Model

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

The common deployment models as below:

- Private cloud - The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organisation, a third party, or some combination of them, and it may exist on or off premises.
- Public cloud - The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider.
- Hybrid cloud - The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Clause 6 : Organisation Assessment

- Understand the risk
  - RA / BIA / Policy / Terms / Governance /etc

- Cloud Policy
  - Cloud service customer
  - Cloud service provider

- Technical and Business driver
  - Business strategy
  - Security Policy enhancement
  - Access management
  - Data protection

Clause 7: Selection Criteria

- Selection Criteria
  - Certification and Standards (ISO / CSA / PCIDSS / etc)
  - Pre-assessment checklist – capability / competency /track record
  - Information Security Governance – assurance by CSP
  - Data Security – SOPs on data classification and handling
  - Service Dependency –subconcontractors
  - Contracts & Agreement – terms / SLA
  - Service Reliability – system / service performance / DR / Monitoring
  - Exit Provisions – exit strategy

Annex A - F

- Annex A : Cloud service model
- Annex B : Common information security threat
- Annex C: Cloud controls matrix
- Annex D: Compliance checklist for cloud service provider
- Annex E: Service level agreement responsibilities
- Annex F: Example of terms of services and privacy policy
- Bibliography

REFERENCE

- ISO/IEC 27017:2015, *Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- ITU-T X.1601, *Cloud computing security - Overview of cloud computing security*
- CREST, *Cyber Security Incident Response Supplier Selection Guide*
- ENISA, *Cloud Standards and Security*
- Cloud Security Alliance, *Top Threats to Cloud Computing V1.0.*
- 8 criteria to ensure you select the right cloud service provider | Cloud industry forum
- https://www.cloudindustryforum.org/content/8-criteria-ensure-you-select-right-cloud-service-provider
- Developing a Cloud Provider Selection Model -
- https://subs.emis.de/LNI/Proceedings/Proceedings190/163.pdf
- Tips for Small and Medium Enterprises in Choosing Cloud Service Providers
- http://www.infocloud.gov.hk/home/10785
- Developer Works Cloud Computing Editors IBM. (2010). Review and Summary of Cloud Service Level Agreements. Retrieved on 14 January 2013, from
- http://agimo.govspace.gov.au/files/2011/11/Cloud-Legal-Draft-Better-Practice-Guide-November-2011.pdf
- http://www.ibm.com/developerworks/cloud/library/cl-rev2sla-pdf.pdf
- Cloud Security Alliance Cloud Controls Matrix (CSA CCM)

Challenge

- Data sovereignty
- Contract requirements
- Right to audit

Malaysian Technical Standards Forum Bhd

TECHNICAL CODE: INFORMATION AND NETWORK SECURITY - INCIDENT MANAGEMENT

MCMC MTSFB TC G015:2018

AGENDA

- Document Scope, References & Structure
- Why Technical Code
- Target User
- Main Requirement for TC
- Summary for each clause
- Challenge Faced
- Acknowledgement

SCOPE

- This Technical Code is to provide a specification on information security incident management for organisations within Communication and Multimedia Industry (CMI).
- Registered date 15 Oct 2018

Target Audience

- IT Department:
  - IT help Desk / IT Service Desk
  - IT Support
  - IT Infra Team
  - IT Security Team
  - Senior Management

TC Main Structures

- Clause 0: Introduction
- Clause 1: Scope
- Clause 2: Terms and definitions
- Clause 3: Abbreviations
- Clause 4: Plan and prepare
- Clause 5: Handling an incident
- Clause 6: Post Incident activities
- Clause 7: Information sharing
- Annex A : Example of the roles and responsibilities
- Annex B : Pre-requisite requirement for handling incidents
- Annex C: Questions to use as a guidance to understand the incidents
- Bibliography

Clause 4 : Plan and Prepare

- Information security incident management policy
- Information security incident management plan
- Standard Operating Procedures (SOPs)
- Incident Response Team (IRT) structure
- Communication with external party
- Awareness and training
- Exercise and testing

Clause 5: Handling an incident

- Resource in handle/support Incident
- Incident detection
- Incident analysis
- Incident documentation
- Incident prioritization/severity
- Incident notification
- Incident containment
- Incident eradication
- Gathering and preserving evidence
- Recovery

Clause 6: Post Incident

- Lessons Learned
- Collected Incident Data
- Evidence Retention
- Reporting to relevant Stakeholders

- Other Improvement
  - X-MAYA / NSC

Clause 7: Information sharing

- Sharing with External Parties
- Sharing Agreement
- Information Sharing Methods

Annex

Annex

- Annex A : example of RACI Table
- Figure 1: example of IRT Structure
- Annex B: Pre-requisite for handling incidents
- Annex C: Guidance to understand Incidents

REFERENCE

- ISO/IEC 27035, Information technology - Security techniques - Information security incident management
- MCMC Network Security Centre Standard Operating Procedure
- CREST, Cyber Security Incident Response Guide
- ISACA, Incident Management and Response
- NIST 800-61 Revision 2, Computer Security Incident Handling Guide

ACKNOWLEDGEMENT

- **Members of the Working Group**
- Al Hijrah Media Corporation
- Measat Broadcast Network System
- Basis Bay Malaysia
- Celcom Axiata Berhad
- Malaysia Digital Economy Corporation Sdn Bhd
- Malaysian Communications and Multimedia Commission
- Maxis Communications Berhad
- MYTV Broadcasting Sdn Bhd
- TIME dotCom Berhad
- Provintell Technologies
- Telekom Applied Business Sdn Bhd
- Telekom Malaysia Berhad
- Universiti Kuala Lumpur
- Universiti Tenaga Nasional
- webe digital Sdn Bhd

Q & A

Thank You