Question 3/17 – Telecommunication information security management and security services

(Continuation of Question 3/17)

1 Motivation

For telecommunications organizations, information and the supporting processes, telecommunications facilities, networks and transmission media are important telecommunication business assets. In order for telecommunications organizations to appropriately manage these business assets and to correctly continue the business activity, information security management is extremely necessary. For this reason, Recommendation ITU-T X.1051 was developed to provide code of practice for information security controls for telecommunications organizations.

Based on the code of practice, detailed and specific management areas including risks, assets, governance, management framework and incidents have also been developed together with introducing best practices as Supplement. New areas in relation with Recommendation ITU-T X.1051 should be investigated further. Meanwhile, the series of Recommendations have to be maintained and updated reflecting the latest information security management issues. The aim is to develop a set of Recommendations on security management for telecommunications based on Recommendation ITU-T X.1051 in ITU-T.

In parallel with developing Recommendations for detailed and specific management areas based on Recommendation ITU-T X.1051, the new areas of telecommunication and ICT security services, e.g., Cyber Defence Center (CDC) services including Security Operation Center (SOC) services, Managed Security Services (MSSs), and Computer Incident Response Teams (CIRTs) services, lifecycle management for security controls and effective risk management, and management of personally identifiable information which request emergent and global countermeasures should be considered. Those areas are not only in information security but also covers aspects in cybersecurity. Therefore, the studies particularly should focus on management aspects on above new areas in information security and cybersecurity.

In the course of the studies, a full collaborative effort between ITU-T and ISO/IEC JTC 1 will be continued to ensure the widest possible compatibility of security solutions. The success of solutions developed as national standards in many countries also need to be considered.

This Question differs from Questions in Study Group 2 in that deals with the exchange of network management information between network elements and management systems and between management systems in TMN environment. This Question deals primarily with the protection of business assets, including information and processes in view of information security management.

Recommendations and Supplements under responsibility of this Question as of 7 January 2022: E.409 (in conjunction with SG2), X.1051, X.1052, X.1053, X.1054, X.1055, X.1056, X.1057, X.1058, X.1059, X.1060, X.1061 and Supplements X.Suppl.13, Suppl.27, Suppl.32, Suppl.34, and X.Suppl.36.

Texts under development as of 7 January 2022: X.1051rev2.

2 Question

Study items to be considered include, but are not limited to:

a)   How should specific security management issues for telecommunications organizations be identified?

b)   How should measurement of security management in telecommunications be identified and managed?

c)   How should control objectives and controls be mapped and integrated into organizational management and operational aspects in telecommunication organizations?

d)   How should concepts and principles for the governance of information security, by which organizations can evaluate, direct, monitor and communicate the information security-related activities within the organization be applied?

e)   How should the adoption of risk treatment option to manage the impact of a security incident?

f)   How should best practices providing directions in the security services, e.g., CDC services including SOC services, MSSs and CIRT services, be applied?

g)   How should information security management for telecommunications organizations be properly implemented by using the existing standards (ITU-T, ISO/IEC and others)?

h)   How should management of personally identifiable information be implemented and effective?

i)   What enhancements to existing Recommendations under review or new Recommendations under development should be adopted to reduce impact on climate changes (e.g., energy savings, reduction of greenhouse gas emissions, implementation of monitoring systems) either directly or indirectly in telecommunication and ICT or in other industries?

3   Tasks

Tasks include, but are not limited to:

a)   Study and develop a framework of information security management functions described in Recommendation ITU-T X.1051.

b)   Study and develop a methodology to implement information security management for telecommunications organizations based on the existing standards (ITU-T, ISO/IEC and others).

c)   Study and develop a framework/guidelines for the security services, e.g. CDC services including SOC services, MSSs and CIRT services.

d)   Study and develop guidelines for lifecycle management for security controls.

e)   Study and develop guidelines for effective risk management e.g. risk cyber insurance acquisition for risk treatment.

f)   Study and develop guidelines for management of personally identifiable information.

g)   Propose outline of new Recommendations.

h)   Assess the outputs of above activities in view of usability for telecommunications facilities and services.

i)   Produce draft Recommendations.

j)   Maintenance and enhancements of Recommendations in the X.105x-series.

An up-to-date status of work under this Question is contained in the SG 17 work programme at https://www.itu.int/ITU-T/workprog/wp_search.aspx?sp=17&sg=17.

4   Relationships

WSIS Action Lines:

–   C5

Sustainable Development Goals:

–   8 (Decent Work and Economic Growth)

–   9 (Industry, Innovation and Infrastructure)

Recommendations:

–   X.800-, X.1000-, X.1100- X.1200- and X.1300- series

Questions:

–   ITU-T Qs 1/17, 2/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17, 15/17 and 14/15

Study Groups:

–   ITU-D; ITU-R; ITU-T SGs 2, 9, 11, 13, 15, 16 and 20

Standardization bodies:

–   Asia Pacific Telecommunity Standardization Programme (ASTAP); European Telecommunications Standards Institute (ETSI); ISO/IEC JTC 1/SC 27; ISO/IEC JTC1 SC40, ISO/TC 68, ISO/TC 215, ISO/TC 307; National Institute of Standards and Technology (NIST); Telecommunication Technology Committee (TTC); Third Generation Partnership Project (3GPP); Forum Incident Response and Security Teams (FIRST)