HKT Here To Serve

What is the value of ISO-27001 to an internal organization?

Eric Wong

Senior Vice President

Technical Service, Operation and Security

Jul 2021

a PCCW Group member

The Group

HKT (SEHK: 6823) is Hong Kong's premier telecommunications service provider and a leading innovator. Its fixed-line, broadband, mobile communication and media entertainment services offer a unique quadruple-play experience. HKT meets the needs of the Hong Kong public and local and international businesses with a wide range of services including local telephony, local data and broadband, international telecommunications, mobile, media entertainment, enterprise solutions and other telecommunications businesses such as customer premises equipment sales, outsourcing, consulting and contact centers.

HKT is the first local mobile operator to launch a true 5G network in Hong Kong. Backed by its substantial holding of 5G spectrum across all bands and a robust and extensive fiber backhaul infrastructure, HKT is committed to providing comprehensive 5G network coverage across the city.

HKT delivers end-to-end integrated solutions employing emerging technologies such as 5G, cloud computing, Internet of Things (IoT) and artificial intelligence (AI) to accelerate the digital transformation of enterprises and contribute to Hong Kong's development into a smart city.

Riding on its massive loyal customer base, HKT has also built a digital ecosystem integrating its loyalty program, e-commerce, travel, insurance, FinTech and HealthTech services. The ecosystem deepens HKT’s relationship with its customers thereby enhancing customer retention and engagement.

Employing approximately 15,900 staff, HKT is headquartered in Hong Kong and maintains a presence in mainland China as well as other parts of the world.

The share stapled units of the HKT Trust and HKT Limited are listed on The Stock Exchange of Hong Kong Limited (SEHK: 6823).

HKT Limited is a company incorporated in the Cayman Islands with limited liability.

Background

- Strong management commitment towards Cyber Security
- Comprehensive Information Security policies and processes in place
- Well-established 3 layers of defense mechanism
  - Dedicated Cyber Security team to orchestrate and execute corporate-level controls
  - Group Risk Management and Compliance team to manage and prioritize overall risk portfolio
  - Group Internal Audit team to assure compliance of practices to regulations and policies in all levels
- On top of product-level, demonstrate the current internal operation is on par with international standard

Why ISO 27001 for Internal Organization?

- Increasing demand of internal customers on internal operation to meet international standards
- Assure our internal practices are adhering to a comprehensive and trustworthy information security standard
- Simplify internal assurance process using the accredited result of a recognized body
- Promote information security as a culture within the organization and make it business as usual
- Extra guarantee on legal and regulatory compliance
- Reduce costs due to security incidents

Implementation Principles

- Structure the comprehensive information security management practices that are already in place
- Target not to introduce new process just for the sake of ISO 27001
- Refine and streamline existing processes whenever possible

Top Management's Leadership & Commitment

- Establish information security objectives in alignment with organization strategy and direction
- Envision and motivate security culture within the organization
- Communicate the importance of ISMS to staff at all levels of the business
- Ensure adequate resources and budget
- Promote continuous improvement

Scoping

- Prioritize what needs to improve
- Identify physical locations that conduct the main business operations
- Include people, processes, systems, applications, and facilities
- Identify interfaces and dependencies from other processes
- Extend scope to cover more facilities after certification

Planning

- Organization Context
  - Roles and responsibilities
  - Stakeholder’s interests
  - Internal and external issues
- Gap analysis
  - Identify gap between ISO 27001 and current processes and controls
- Risk assessment
  - Identify, analyse, and prioritise threats to an organisation
  - Implement treatment plan to reduce the level of risk to which acceptable to the businesses' risk appetite
  - Perform regularly as an ongoing exercise

Developing

- While most other ISO 27001 candidates are working on
  - Establishing/ finalizing missing parts of information security policy
  - Incorporating corporate policies, standards, guidelines and procedures
- We focus on
  - Managing residual risks
  - Refining existing processes and controls adhering to the requirements of ISO 27001

Implementing

- Update a list of all related information assets
- Integrate security processes and controls into operational environment
- Provision adequate training to ensure staff competence with information security roles
- Perform regular security awareness training

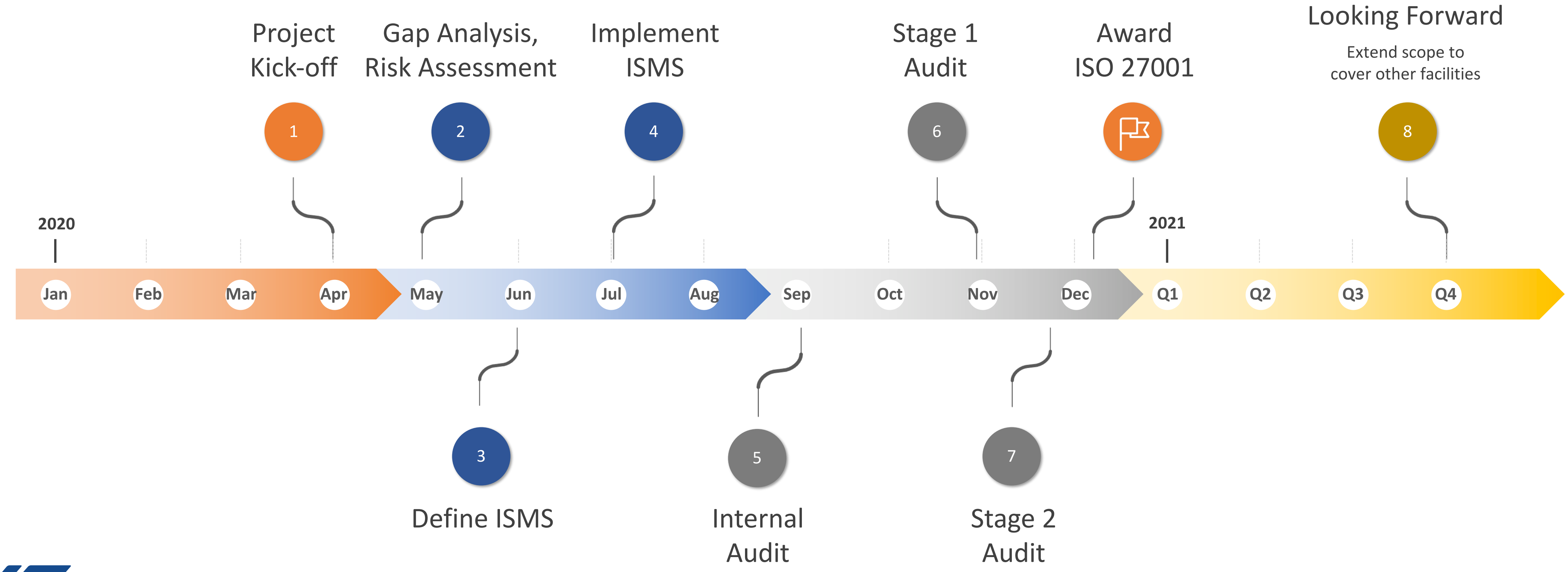
Monitoring

- Regular management review
- Measure the information security objectives
- Monitor the effectiveness of security controls, and take corrective and preventive action accordingly
- Identify areas for improvement

Assurance

- Pre-Audit
  - Like a mock exam, a preliminary test if we were up to standard
- External Audit by Certification Body
  - Stage 1 initial assessment - Review of the ISMS that make sure all of the proper policies and controls are in place
  - Stage 2 initial assessment - Review of the actual practices and activities that ensure they are in-line with ISO 27001 and the written policies
  - Continuing Assessment
    - Perform yearly after initial assessment
    - Reassure the actual practices and activities are doing what originally planned for

Our Journey



Project Kick-off

Gap Analysis, Risk Assessment

Implement ISMS

Stage 1 Audit

Award ISO 27001

Looking Forward

Extend scope to cover other facilities

Define ISMS

Internal Audit

Stage 2 Audit

Critical Success Factors

- Think big, start small
  - Start implementing ISO 27001 with a small team covering board process areas
  - Manageable cost
  - Achievable in relative short period
  - Plan for expansion to cover additional facilities and operation
- Commitment and engagement from top management to all staff
- Make information security business as usual

Questions?