

chapter 1 ITIL

1.1 Introduction to ITIL

ITIL, which stands for Information Technology Infrastructure Library, is a public domain that provides a practical framework for IT service management, representing the IT industry's best ideas of how IT should operate by establishing "Good Practices" that define a quality standard for IT services for customers to demand and providers to meet ^[1]. ITIL is an application of management science to information technology (IT) and is a Flow-based approach.

1.1.1 Characteristics of ITIL

ITIL is the best practice of IT service management. ITIL is a customer-oriented approach to give customers high quality and low cost IT services by asking and helping users to use them, collecting and analyzing their views and suggestions, following up on their dissatisfaction, and monitoring their evaluation of IT services ^[1]. ITIL provides holistic service management, starting from the service ITIL provides a holistic approach to service management, analyzing the life cycle of service from the strategic requirements to consider how to design, convert, operate and continuously improve it, as demonstrated by the consideration of requirements to ensure operation and maintenance, testing plans for development, identification of the impact on the original system infrastructure due to new system construction or modification of the system, and analysis of future requirements ^[1].

1.1.2 ITIL framework

ITIL consists of five core processes that map the entire ITIL lifecycle (as shown in Figure 1), starting with the identification of customer requirements and drivers for IT requirements, through the design and implementation of services, and finally to the monitoring and improvement of services ^[2].



Figure 1 Lifecycle of ITIL

(i) ServiceStrategy

Service Strategy (SS), a guide on how to design, develop and implement service management, considering both organisational capabilities and strategic assets, is simply a direction for our service management, telling us what to do and what not to do. There are three processes involved in the service strategy phase: activity portfolio management, financial management, and demand management. The purpose of service strategy is to help organisations to have a win-win strategic way of thinking, to have a strategic asset of great value and long-term effectiveness, and to help organisations convert service management into a strategic asset. In the service strategy phase, organisations will gain cost efficiencies, a customer value-focused starting point, and standardisation of processes, ultimately creating value ^[2,3].

(ii) Service Design (SD)

Service design (SD) is responsible for designing new or changed services (including architecture, processes, policies, and documentation) for introduction into the production environment. Service design consists of seven major processes and functions: service catalog management; service level management; capacity/capability management; availability management; information security management; vendor management; and IT service continuity management. The key to service design is the adoption of a unified strategy for all service design, i.e. the consistency and integrity of all activities and processes across the technical scope of IT and the provision of end-to-end business-relevant functionality and quality, ensuring that business needs are met in a cost-effective without compromising quality while enabling improved service quality, performance and consistency, improved IT control and information and decision making, and easier implementation of the service catalog or service level management. It can also make it easier to implement euphoric or changing services ^[4,5].

(iii) Service Transition (ST)

Service Transition (ST) is the definition of high-quality services by managing change and risk and consists of three main processes: change management, configuration management, and release management. Service Transition aligns new or changed services with customer business requirements and business operations to ensure that customers and users can use the new or changed services to bring maximum value to business operations, to reduce consumption and rework, reduce the defense of planning resources and budgets, and increase productivity to enhance business value ^[6,7]. Release management is one of the important management processes of ITIL Service Transformation (ST). For the business or users of the business, it can minimize the service performance with customer requirements; minimize the number of service failures; and maximize customer satisfaction. And the provider of the business can reduce the resources and costs used to diagnose and fix fault-level problems in deployment and production, increase the adoption of common standard frameworks and reusable processes and documentation, and reduce the variance between plan and actual ^[6,7].

(iv) ServiceOperation (SO)

ServiceOperation (SO) is to effectively and efficiently complete service support and service delivery, ensuring the interests of customers and service providers to provide guidelines, including incident management, incident, and problem management, request fulfillment, access management 4 major processes, its main functions include service desk, technical management, IT operations management, application management. Service Operations coordinates realize the activities and processes required to deliver and manage services by the service level with the customer and completes the management of the technology that delivers and supports the services. Service operations are the stage where planning, design, optimisation, etc. are realized and measured. From the customer's point of view, it is the stage where value is truly seen ^[8,9].

(v) Continuous ServiceImprovement (CSI)

Continuous Service Improvement (CSI) is responsible for managing the improvement of IT service management processes and IT services themselves, as well as continuously measuring and improving the performance of IT service providers. The purpose of Continuous Service Improvement is to keep IT services aligned with business changes and to implement IT service improvements to support business processes. Continuous service improvement is responsible for finding ways to improve the effectiveness and efficiency of processes while keeping an eye on cost-effectiveness. By linking improvement efforts and results to service strategy, service design, and service transformation through continuous service improvement, a closed-loop feedback system (based on the Plan, Do, Check, Act (PDCA) model as defined in ISO/IEC 20000) is established that accepts change inputs from any planning method and feeds into each other for continuous improvement ^[10,11].

chapter 2 ISO27000

2.1 Steps in implementing an ISO27001 risk assessment

Risk assessment is clearly defined in the ISO 27001 standard as the entire process of risk analysis and risk evaluation. Risk analysis is the systematic use of information to identify sources and estimate risks; risk evaluation is the process of comparing estimated risks based on given risk criteria to determine the severity of the risk ^[12].

A methodology for risk assessment is given in ISO 27001, which indicates the steps for implementing risk assessment in an organisation, as follows.

- 1) Define the organisation's risk assessment methodology
 - a) Identify the risk assessment methodology applicable to the information security management system and the identified business information security, legal and regulatory requirements.
 - b) Establish guidelines for accepting risk and identify acceptable levels of risk.
- 2) Identify risks
 - a) Identify the assets within the control of the ISMS and the owners of those assets.
 - b) Identify threats to those assets.
 - c) Identify weak points that could be exploited by threats.
 - d) Identify the potential impact on assets from loss of confidentiality, integrity, and availability.
- 3) Analyze and evaluate the risks
 - a) Assess the potential organisational business impact of a security failure, considering the consequences of loss of confidentiality, integrity, and availability of assets.
 - b) Assess the realistic likelihood of a security failure occurring, based on the main threats to the asset, points of vulnerability, related impacts, and the security controls already in place.
 - c) Evaluation of the level of risk.
 - d) Determine whether the risk is acceptable or needs to be addressed based on the established guidelines.

2.2 About the PDCA model

The chapter structure of the ISO standard PDCA has been reconstructed. Here is a brief explanation of the PDCA model and the divisions of the new version of the standard: The PDCA model is an internationally recognized model, which is followed by many well-known standards and management systems. The model is a good cyclical framework, with each stage being linked to the others.

The PDCA model is made up of four separate components.

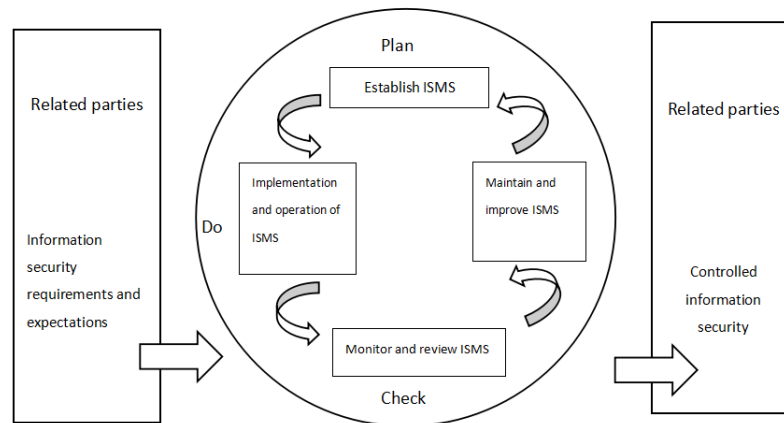


Figure 2 PDCA model

P (Plan) - establishing the ISMS, defining the plan of activities based on the overall strategy and objectives of the organisation, - organisational context, leadership, planning, support.

D (Do) - implementing and operating the ISMS to do what is planned - running.

C (Check) - monitoring and reviewing the ISMS, summarising the results of implementation and operation, identifying problems including - performance evaluation.

A (Action) - maintain and improve the ISMS, make treatment of the results of the review, successful experience to be maintained and replicated, failure to find the reasons to avoid the same mistakes next time, the problems that are not solved into the next PDCA cycle - improvement

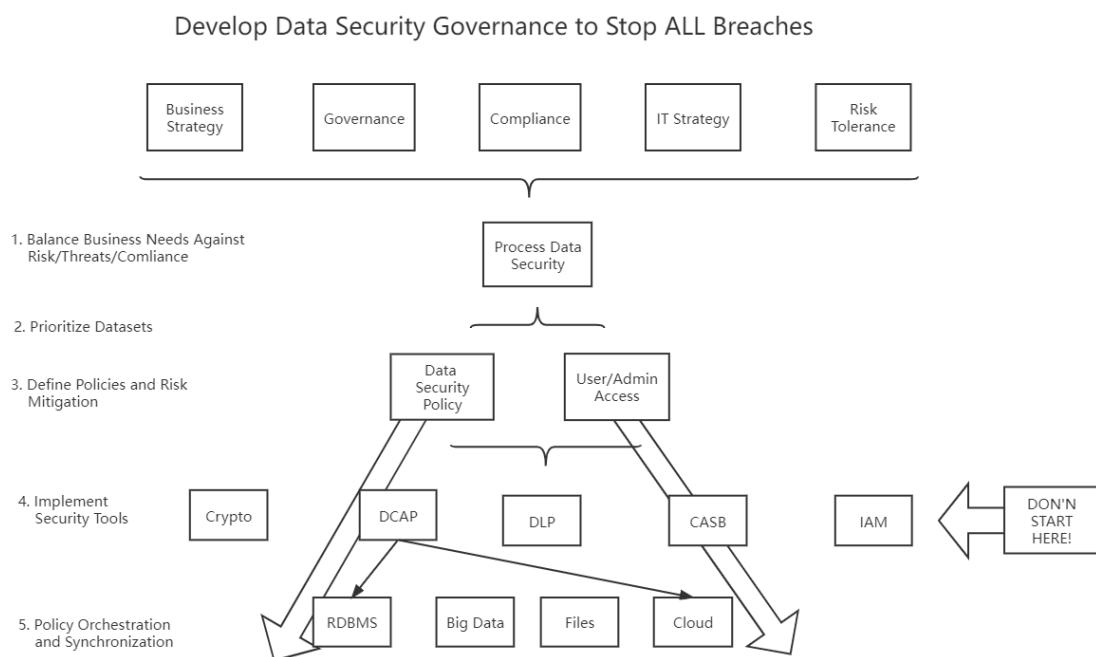
The PDCA model is a model commonly used in management. The model operates in a sequence of P-D-C-A. A complete cycle can be seen as a management cycle in management science, and after each cycle, the management situation will be improved, while entering a higher P-D-C-A cycle, the management system of the organisation is continuously improved and the management level is constantly improved. And these four steps become a closed loop through which the information security management system is continuously improved and information security performance spirals upwards.

The new content will make the focus of the enterprise different, from the above discussion it is obvious that the new standard in the enterprise before the establishment of information security system has increased the importance of the enterprise internal and external environment information security, in the construction of information security system before the enterprise needs to consider its organisation environment, enterprise resources, management status quo, understand the opportunities and risks faced by its development, so that high standards, high precision, high requirements to treat information security management work.

For the software industry, the information security system has been initially established and implemented, mainly to monitor the review and continuous improvement of its information security system - the C and A of the PDCA model.

chapter 3 Gartner's overall framework for data security governance

Gartner has developed a holistic top-down framework for database security governance^[13], including a complete system from governance prerequisites and specific objectives to technical support, a "skeleton" that is then filled with "meat" by enterprises and organisations when implementation is carried out. It is a "skeleton" that is then filled with "flesh" when the implementation is carried out.



Step1: Balancing business needs with risk/threat/compliance

There are five dimensions to consider here: business strategy, governance, compliance, IT strategy, and risk tolerance, and these are the five elements that need to be agreed upon before the governance team can work.

Business strategy: establishing how the handling of data security supports the development and implementation of business strategy

Governance: the need for a deep governance approach to data security

Compliance: the compliance requirements facing the business and the organisation

IT strategy: synchronisation of the enterprise's overall IT strategy

Risk tolerance: where the enterprise's tolerance for security risk lies

Step2: Data Priorities

Before conducting data security governance, you need to clarify the target of governance, enterprises have huge data assets, in line with the principle of efficiency, Gartner recommends that priority should be given to the security of important data governance work, Anhua Jinhe

governance ideas also "data classification" as the first link of the overall plan, which will greatly improve This will greatly improve the efficiency and input-output ratio of governance. By sorting out all data assets, clarifying data types, attributes, distribution, access objects, access methods, frequency of use, etc., and drawing a "data map", we will use this as the basis for hierarchically classifying data in a manner, to implement reasonable security measures for different levels of data. This foundation will also provide policy support for the implementation of each step of the governance technology.

Step3: Developing a strategy to reduce security risks

Consider how to implement data security governance in two directions: firstly, to identify the data visitors (application users/data managers), access targets, and access behaviour; secondly, to develop different, targeted data security policies based on this information. The implementation of this step is further backed up by the results of data asset grooming to provide protection strategies that meet business needs while safeguarding data security in different scenarios such as data access, storage, distribution, and sharing.

Step4: Implementing security tools

Gartner has proposed 5 tools for security and risk control in the DSG system, which refers to 5 security areas, which may include several specific technical tools.

Crypto (encryption): this should include encryption of structured data in databases, as well as encryption at the transport layer or application side before the data is stored on the ground, and a variety of technologies such as key management and ciphertext access rights control associated with encryption.

DCAP (Data-Centric Auditing and Protection): allows centralized management of data security policies and unified control of structured, semi-structured, and unstructured databases or data silos. These products can audit log records for abnormal behaviour through compliance, reporting, and forensic analysis while using techniques such as access control, desensitisation, encryption, and tokenisation to delineate responsibilities between application users and administrators.

DLP (Data Leakage Prevention). DLP tools provide visibility into sensitive data, whether it is used on an endpoint, in motion on the network, or at rest on a file share. Using DLP, organisations can protect unstructured data extracted from endpoints or emails in real-time. The fundamental difference between DCAP and DLP is that DCAP tools focus more on data accessed by users within the organisation, whereas DLP focuses more on data that will leave the organisation.

IAM (Identity and Access Management). IAM is a comprehensive set of business processes and management tools for establishing and maintaining digital identities and providing effective and secure access to IT resources, thus enabling unified authentication, authorisation, and centralized management and auditing of identity data for an organisation's information assets. Identity and access management is a set of business processes and a supporting infrastructure for creating and maintaining and using digital identities.

Step5: Policy Configuration Synchronisation

Policy configuration synchronisation is mainly for DCAP implementation, centralized management of data security policies is the core function of DCAP, and regardless of access control, desensitisation, encryption, tokenisation that means must pay attention to the data access and use of security policies to maintain synchronisation issued, policy implementation

objects should include relational databases, big data types, document files, cloud data, and other data types.

"Data Security Governance" is different from any previous security solution, it is a bigger project, technology and products are no longer the main body of the data security governance framework, together with organisational decisions, systems, assessments, audits are the soul and guiding principle of this framework.

chapter 4 case analyze

4.1 Introduction to background

CoffeeBlue sells Blue Mountain Peak coffee from Jamaica, one of the best and most sought-after blends in the world. CoffeeBlue has an extensive presence around the globe. The company uses cloud services to deliver IT services to its staff and clients. It is estimated that almost 95% of the company's network is wireless-based. The company also has a massive online presence and social media presence to promote its activities. Owing to its large staff and international customer base, the company has recently come under immense pressure to allow both its staff and customers to use their devices to access the company's network/resources. Security of personal staff's data and client's data is the company's major concern. The company is also concerned about protecting its intellectual properties, which are worth billions. Information Security is a priority to the company, but everything is in disarray. There is no established policy covering their security need. This paper will build a security framework for a Caribbean coffee company based on ITIL.

4.2 solution

4.2.1 General objectives of the implementation

The results of the ITIL assessment model also show that the lack of release management processes has become the shortest part of Coffillue's IT barrel. The implementation of improvements was urgent. The Information Centre and the business units considered setting up and re-engineering the specific provision, scope, service levels, processes, and specifications of the required software development services. The goal of the information centre is to provide the business units with high-quality services using ITIL service management processes, further reducing service costs and increasing satisfaction.

The main strategy to achieve this goal is to develop, maintain and manage a set of ITIL Release Management-based software development management processes based on the improvement methods provided by the ITIL Service Management Improvement Model, based on existing realities, comparing ITIL best practices, learning, and incorporating lessons learned from others, based on existing resources and conditions, and continuously and continuously

improving their service quality, reducing costs, increasing efficiency and improving satisfaction.

4.2.2 Overall plan for implementation

To achieve the objectives, the responsibilities of the business departments, the functional groups of the information centre, and the outsourcing units need to be clarified and the management process needs to ensure that service support is in place, the key point of which is the standardisation, traceability, control and quantifiable assessment of the service. Only by putting processes into a truly controlled, traceable, and quantifiable perspective can behavioural patterns truly be facilitated ^[17]. And release management achieves the goal of planning, testing, and documenting these activities by following a rigorous, consistent and repeatable process to ensure that appropriate requirements are collected, applications are tested and operations are ready and successfully implemented into the production environment ^[14-16].

Meanwhile, the release lifecycle (RLC: ReleaseLifeCycle) is different from the system/software development lifecycle (SDLC: SoftwareDevelopmentLifeCycle) in that the release lifecycle complements the system/software development lifecycle and guides all releases by ensuring that they are planned, tested, and scheduled software/system releases ^[6,7,14-16].

The release lifecycle is aligned with the development lifecycle. The release lifecycle consists of seven related phases ^[6,14].

- (1) Launch
- (2) New Environment Request (NER: NewEnvironmentRequest)
- (3) Build and release configuration
- (4) Quality Assurance (QA)
- (5) OperationsReadiness
- (6) Implementation
- (7) Post-implementation

Each phase needs to produce specific deliverables to ensure that each release is properly designed, constructed, tested, and operationally prepared before implementation and release. Each stage needs to pass a review that matches the description in the development lifecycle before moving on to the next stage. Managing outsourced software development activities through releases is a facilitator and complement to outsourced software development.

So the overall plan for ITIL implementation is that the responsibilities of business departments, functional groups in the information centre, and outsourcing units need to be clarified, the focus is on implementing ITIL release management by addressing the deficiencies identified by the ITIL assessment model, strengthening the ITIL release management process, refining performance data, analyzing performance information, producing performance reports and continually improving them.

Reference

- [1] ITIL-baidu[OL]. <https://baike.baidu.com/item/ITIL/10498690>
- [2] ITIL V3 Service Strategy. US: OGC,2007.
- [3] Best Practice Insights. Focus On: ITIL® Service Strategy For ITIL 2011, BMC,2016.1
- [4] ITIL V3 Service Design. US: OGC,2007.
- [5] Best Practice Insights. Focus On: ITIL® Service Design For ITIL 2011, BMC,2016.1
- [6] ITIL V3 Service Transition. US: OGC,2007.
- [7] Best Practice Insights. Focus On: ITIL® Service Transition For ITIL 2011, BMC,2016.1
- [8] ITIL V3 Service Operation. US: OGC,2007.
- [9] Best Practice Insights. Focus On: ITIL® Service Operation For ITIL 2011, BMC,2016.1
- [10] ITIL V3 Continual Service Improvement. US: OGC,2007.
- [11] Best Practice Insights. Focus On: ITIL® Continual Service Improvement For ITIL 2011, BMC,2016.1
- [12] ISO / IEC 27001: 2005 Information technology-Security techniques-Information security management systems-Requirements.Geneva: International Organisation for Standardisation.International Standards Organisation, 2005
- [13] Gartner defines data security governance
<https://cloud.tencent.com/developer/article/1552305>
- [14] Dave Howard. ITIL Release Management A Hands-on Guide,2010, Taylor and Francis Group, LLC
- [15] RS Hall.D Heimbigner AL Wolf. Software release management[J], European Software Engineering Conference Held J...,1997,22 (6):159-175
- [16] Release Management. Harvard University Information Technology,2013.11
- [17] IT Management: From Human Governance to Process [J]. Chinese Economy and Information Technology, 2006(26):27-27