# CENTRALE BANK VAN CURAÇAO EN SINT MAARTEN
# (Central Bank)

# Provisions and Guidelines

# For

# Information Technology Service Management

---

*WILLEMSTAD, Version July 2014*

# Provisions and Guidelines for Information Technology Service Management

# I. Introduction

The "Provisions and Guidelines for Information Technology Service Management" (hereafter "ITSM Provisions") aims to further promote and ensure safe and sound practices regarding Information Technology Service Management (hereafter "ITSM") of the institutions subjected to the supervision (hereafter "supervised institutions") of the Centrale Bank van Curaçao en Sint Maarten (hereafter "the Bank").

The objective of ITSM Provisions is to deliver Information Technology (IT) service support to the supervised institutions, in order to fulfill their IT requirements and thus provide internal and external customers with high quality service. This includes the design, transition, delivery, monitoring and improvement of IT services that support business processes.

Furthermore, the ITSM Provisions aims to further align IT and business processes. In order to do so, a paradigm shift needs to be made. IT should no longer be considered as the technology supplier, but as a business enabler. Institutions can adapt to new IT service models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These new models can exist next to the classical IT service model, where IT is an internal department delivering IT services to the organization. ITSM involves the delivery of efficient and effective end-to-end IT services to meet the changing demands of the organization, and to measure and show improvements in the quality of IT services offered.

In the earlier issued "Provisions and Guidelines for Business Continuity Management", the business impact analysis is created with the business processes in mind. In the business impact analyses we determined the "Recovery Time Objective (RTO)" and the "Recovery Point Objective (RPO)" per business process. Both objectives are part of the service level that is demanded from IT in case of a disruptive event. **Single points of failure in the organization and IT are eliminated** and other measurements are taken in order to achieve appropriate resilience levels for the business.

Also the earlier issued "Provisions and Guidelines for Information Security Management" was created with the business processes in mind. An important aspect of this guideline is to perform a risk analyses per business process and to indentify information assets, its owners, assigning accountability and responsibility, establish policies and procedures and adapt the organization to improve the internal control environment. Risk is also mitigated or better controlled by changing or enhancing business applications with preventive and detective controls.

The ITSM Provisions continue to align IT services with business processes and add controls to IT processes to reduce risk. Work performed to comply with the "Provisions and Guidelines for Business Continuity Management" and the "Provisions and Guidelines for Information Security Management" can be added upon. In addition, by properly documenting ITSM processes, the ITSM Provisions will contribute to further improve the maturity level of IT within the supervised institutions.

Procedures should be in place in order to make IT tasks repeatable, prevent individual IT "heroes", or ad hoc decision making, which result in disorganized behavior. In order to prevent such behavior, procedures should provide the answers to the questions regarding who needs to do what, when, where, why and how, and who is responsible and accountable. Documented procedures not only give guidance to employees, but also create transparency for management and facilitate the auditing process. It allows others to detect the presence of weak controls in processes.

**The ITSM Provisions offer principles for structuring a comprehensive ITSM Framework.**

As supervised institutions play a crucial role in the economy, it is important that IT services offered, are solid and of high quality, which will contribute to maintain public trust and confidence in the financial sector.

The ITSM Provisions apply to all supervised institutions. These provisions are also tailored to accommodate smaller supervised institutions. Additionally, we encourage larger supervised institutions to implement the ISO 20000-series, COBIT version 5 or the Information Technology Infrastructure Library 'ITIL' Version 3.

The ITSM Provisions contain the principles that a supervised institution should adhere to. The manner in which the supervised institution implements the ITSM Provisions and to which extent inherent information technology risks are mitigated, is the responsibility of the supervised institution. The institution's internal and external auditors must verify if the principles provided in the ITSM Provisions are adhered to, and if controls are in place to ensure that inherent information technology risks are managed adequately.

# II. Legal base and scope

The ITSM Provisions are issued pursuant to:

- Article 2, paragraph 2 of the National Ordinance on the Supervision of Banking and Credit Institutions 1994 (N.G. 1994, no. 4)
- Article 31, paragraph 1 of the National Ordinance on Insurance Supervision (N.G. 1990, no. 77)
- Article 9, paragraph 1 and Article 18 paragraph 1 of the National Ordinance on the Supervision of Investment Institutions and Administrators (N.G. 2002, no. 137)
- Article 11, paragraph 1 of the National Ordinance on the Supervision of Trust Service Providers (N.G. 2003, no. 114)
- Article 2, paragraph 5 of the National Ordinance on the Supervision of Securities Exchanges (N.G. 1998, no. 252)

The ITSM Provisions apply to all supervised institutions. However, ITSM controls should be proportionate to their operational risk (arising from both internal and external sources) and tailored to the nature, size and scope of its operations and the complexity of its business.

The ITSM Provisions are in addition to or stand next to other provisions issued by the Bank.

# III. Implementation

The Bank considers all principles of the ITSM Provisions as common best practice that should be in place. Supervised institutions should cross check for any shortcomings and should resolve likewise.

The ITSM Provisions contain the minimum requirements for establishing sound and effective ITSM practices. The Bank may prescribe additional rules and regulations to administer and carry out the purposes of the ITSM Provisions. This may include rules and regulations to (further) define terms used and to establish limits or requirements other than those specified in the ITSM Provisions. The Bank also reserves the right, in individual cases of (partially) non-compliance, to impose mandatory instructions.

The Bank will periodically review the quality of the ITSM at the supervised institution.

The Board of Supervisory Directors and the Board of Managing Directors of the supervised institutions should familiarize themselves with the ITSM Provisions and understand the objectives and implications of the principles elaborated upon in the following chapters.

# IV. IT Service Management principles

**Principle 1.**

**The Board of Supervisory Directors and the Board of Managing Directors of a supervised institution should establish effective management oversight with respect to IT service management.**

## 1.1 Establishing ITSM policies, standards and procedures.

The Board of Supervisory Directors and the Board of Managing Directors are ultimately responsible for identifying, assessing, prioritizing, managing, and controlling services provided by the IT function. By establishing ITSM policies, management sets out:

- The organization's aims, principles, and approach to ITSM;
- The importance of fulfilling business requirements with the use of IT;
- Ways to assure that risks to services are identified, assessed and managed;
- How to examine new possibilities for IT and ITSM;
- The implementation of key roles and responsibilities for the ITSM process;
- How ITSM will be governed and reported upon, including key performance indicators and key goal indicators; and
- Compliance with legislation, regulatory requirement and contractual obligations.

The effectiveness of ITSM depends on management's commitment and ability to clearly identify what makes existing business processes work properly and safely and what not. Each supervised institution should evaluate its own unique circumstances and environment to develop appropriate ITSM policies, standards and procedures.

Adapting to the international standards for ITSM such as: ISO 20000-series, Control Objectives for Information and Related Technology (COBIT), Microsoft Operations Framework (MOF), and/or the Information Technology Infrastructure Library (ITIL), will provide the supervised institution a solid base to build upon. Supervised institutions are free to choose any standard. However, in order to have a common and solid foundation for ITSM, supervised institutions need at least to comply with the principles set out in this ITSM Provisions.

## 1.2 Allocating sufficient resources and knowledgeable/competent staff

The Board of Supervisory Directors and the Board of Managing Directors should allocate sufficient time and adequate resources to verify whether the ITSM Principles are in place. Any weaknesses to the control environment should be resolved without delay.

### 1.3 Formally approving ITSM policies, standards and plans

The Board of Managing Directors should formally approve the ITSM policies, standards and all plans to ensure that IT delivers and supports services at the required level of the business. The Board of Supervisory Directors should at least annually verify the effort of the Board of Managing Directors on ITSM activities and whether service level agreements are achieved.

### 1.4 Ensuring the quality of the ITSM activities and products through independent audits

The Board of Supervisory Directors and the Board of Managing Directors should ensure that audits are scheduled in accordance with the supervised institution's nature, size, scope of operations and the complexity of its business. The findings thereof should be reported promptly to both Boards.

**Principle 2.**

**Supervised institutions should define the level of service required for critical business functions.**

The objective of this principle is to align IT services with business requirements.

Supervised institutions should periodically examine whether the IT function is delivering efficient and effective end-to-end IT services to meet the changing demands of the organization and or market.

The IT function should no longer be considered the technology supplier, but should be considered the business enabler. Organizations can adapt to new IT service models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). The organization can also outsource specific business functions such as payroll, human resource management or marketing, and multi-source the development of a business application with befriended institutions. These models can exist next to the classical IT service model, where the IT function is an internal department delivering IT services to the organization.

During the business risk assessment and impact analysis, which is performed as part of the "Provisions and Guidelines for Business Continuity Management", the RPO[1] and RTO have been defined. The RPO and RTO are important indicators to indicate the level of service required from IT. However, these indicators are set up for extreme circumstances, including failover to a different location.

Supervised institutions should also define what level of service is important for the business[2] and its customers during normal circumstances. This includes amongst others: new IT service models (e.g. cloud computing); required uptime for business applications; service required during critical time windows (e.g. end of month processing); system performance (e.g. system response time perceived by the end-user); time to respond to and fix incidents; legal requirements (e.g. laws for data retention, privacy); external business requirements (e.g. Sarbanes-Oxley compliance); financial performance measures (e.g. delivering services within budget constraints); human resource measures (e.g. required competence level); and risk management measures[3]. In this regard, the level of services required per critical business function needs to be investigated and documented.

[1] RPO – Recovery Point Objective RTO – Recovery Time Objective; see appendix for further explanation

[2] Availability of e-mail and internet services are also critical components for business functions next to critical business applications. Also, it is good practice to document per critical business function current problems and whishes with regard to the IT systems in use.

[3] As part of Principle 3 of the Provisions and Guidelines for Information Security Management these risk requirements may already been set by the information security risk assessment.

Supervised institutions should ensure that the IT environment can accommodate the level of service required. As a result, the desired outcome may exceed the organization's budget. In such case, a trade off may be needed to meet a level of service that is not ideal, but ultimately feasible to the organization. This will serve as a roadmap for IT to plan future activities.

After the service level requirements for critical business functions are agreed upon, a formal Service Level Agreement[4] ('SLA') may be composed.

[4] Please refer to section 8.2 Third Party Service Level Agreement /Contract as a reference of what could be included in the SLA. In practice only larger organizations might create internal SLA's. This is not obligatory by the Bank.

**Principle 3.**

**Supervised institutions should set up the support and delivery functions for IT services.**

The objective of this principle is to ensure that current, changed, and new services will be delivered and managed according to the service levels required by the business functions.

All aspects of the IT environment should be well known, managed and documented in order to accomplish the required service levels for the various critical business functions[5]. IT should set up the processes and controls for the support and delivery functions of IT services, which are amongst others:

- IT Support services & Incident management:
  The day-to-day process that restores normal acceptable service with a minimal impact on business;
- Problem management:
  The diagnosis of the root causes of incidents in an effort to proactively eliminate and manage them; and
- Change management[6]:
  Standard methods and procedures for effective management of changes to the IT environment.

## 3.1 IT Support Services & Incident Management

The objective of IT support services and incident management is to provide an organized communication channel between users and/or customers and the IT service provider[7] in order to restore interrupted services or to register service requests in a controlled manner.

This service desk, also known as help desk, registers incoming calls and e-mails regarding service incidents and service requests. The service desk provides an organized and coordinated front line to its internal or external technical support staff members. Intelligent service desks use standardized call scripts[8] and try to solve incidents head on. If a service desk member is not able to solve the problem, the incident is dispatched to a technician, who will try to solve the incident.

To organize IT support services and incident management there should be a documented procedure for managing the service request process from recording to closure. The use of an automated system is highly recommended.

[5] See also Par. 10.1.1 ISO 27002 - Documented operating procedures
[6] Release management is considered to be part of the change management process. In the future "Provisions and Guidelines for System Development and Acquisition" this process will be further detailed.
[7] The IT service provider can relate to the internal IT department or an external party.
[8] Call scripts in this regard are standardized questions with possible solutions.

The service desk application should include data such as; user, problem description, affected system (platform, application, or other), prioritization code, current status toward resolution, individual(s) responsible for the resolution, root cause (when identified), target resolution time, and a comment field for recording user/customer contacts and other pertinent information.

When prioritizing incidents and service requests, the service provider should take into consideration the impact and urgency of the incident or service request. Key factors when establishing priority include the number of users or customers affected, revenue losses, expenses incurred, skills available, or the number of SLA's affected, impacted or breached.

The service provider should keep the user/customer informed of the progress of their reported incident or service request. If service targets cannot be met, the service provider should inform the customer and interested parties and escalate according to the procedure. Only qualified personnel must be involved to solve incidents and execute service requests.

The service provider should document and agree with the user/customer the definition of a major incident. Major incidents should be classified and managed according to a documented procedure. The board of managing directors should be informed on major incidents. The board shall ensure that a designated individual responsible for managing the major incident is appointed. After the agreed service has been restored, major incidents must be reviewed to identify opportunities for improvement.

Special attention must be given to "Information Security" incidents. Please refer to "Principle 5 of the Provisions and Guidelines for Information Security Management". Security incidents need involvement of the Information Security Manager or the person(s) entrusted with this role. The same applies to service requests that involve security and access requests such as password resets, new accounts, access to applications, and deactivation of accounts no longer in use. These types of requests must be executed by employees with information security roles who should follow specific change management procedures.

In order to review service level agreements and the performance of IT Operations, a monthly report should be created for ITSM[9]. Automated service desks should have standardized reports that can be included in the monthly ITSM report. The report should not only indicate statistical figures, e.g. amount of incidents resolved within time limits, but why and where performance is failing to meet the plan.

[9] The monthly ITSM report refers to performance of IT Operations and compliance with service level agreements/requirements. IT projects should also create a monthly overview for management. This will be covered in the 'Provisions and Guidelines for System Development and Acquisition'.

## 3.2 Problem Management

The primary objective of Problem Management is to prevent problems and resulting incidents, eliminate recurring incidents, and minimize the impact of unpreventable incidents.

Incident Management deals with the restoring of service to users/customers, whereas Problem Management includes the activities required to diagnose the root cause of an incident and to determine the resolution to those problems. It will also store information about problems and the appropriate workarounds and resolutions, so that the organization is able to reduce the number of incidents and impact over time.

Although Incident Management and Problem Management are separate processes, they are closely related and will typically use the same tools, and may use similar categorization, impact and priority coding systems. This will ensure effective communication when dealing with related incidents and problems. As a result, resolution time will be reduced resulting in less downtime and less disruption to business critical systems.

Supervised institutions should have a standardized procedure for Problem Management.

## 3.3 Change Management

The objective of Change Management is to ensure all changes are assessed, approved, implemented and reviewed in a controlled fashion. Standardized procedures should be used when implementing changes to the IT infrastructure.

Change Management includes changes involving:

- Hardware;
- Configuration of hardware;
- Software;
- Operating systems;
- Middleware;
- Databases;
- Business applications; and
- Documentation and procedures associated with the running, support and maintenance of live systems.

### 3.3.1 Planning and Implementation

The Change Management processes and procedures should ensure that:

- Changes have a clearly defined and documented scope;
- Changes are scheduled based on priority;
- Changes to configurations can be verified after the implementation;
- The time to construct and implement a change is documented;

- It can be demonstrated how a change is:
  - raised, recorded and classified;
  - assessed for its impact, urgency, cost, benefits, and risk of the change;
  - reversed or remedied if unsuccessful;
  - approved or rejected by a change authority;
  - tested, verified, and signed off by the IT assets owner(s);
  - closed and reviewed;
  - scheduled, monitored and reported on; and
  - linked to incident, problem, or service request.

Before implementing a change, scheduling information should be made available to those affected by the change and those needed to implement the change.

### 3.3.2 Back-out Plan

There should always be a back-out plan to restore the previous production environment in case a change corrupts the production environment. In this regard, a full system backup of the updated server should be made prior to the change and for devices, a copy of the configuration of the device, should be kept as a checkpoint to which to return after a change failure.

Change management procedures should also consider:
- changes to be made to recovery sites;
- changes to be made to older backup data;
- changes to technical and functional documentation; and
- training of personnel when new products are introduced.

### 3.3.3 Closing and reviewing the change request

All changes should be reviewed for success or failure after implementation and any improvements recorded. A post-implementation review should be undertaken for major changes to check that:
- the change met its objectives;
- the customers are satisfied with the results;
- there have been no unexpected side effects; and
- IT assets inventory lists and/or configuration information is updated (See principle 4).

Supervised institutions should record and act on any nonconformity. Also, any weaknesses or deficiencies identified in a review of the change management process should lead to plans for improving the service.

### 3.3.4 Emergency changes

Emergency changes are sometimes required, bypassing some of the steps of the change management procedure. The bypassed steps should be accomplished as soon as practical. Emergency changes should be justified by the implementer and reviewed after the change to verify that it was a true emergency.

### 3.3.5 Change Management reporting, analysis and actions

Change records should be analyzed regularly to detect increasing levels of changes, frequently recurring types, emerging trends, and other relevant information. The results and conclusions drawn from change analysis should be recorded and acted upon if necessary.

### 3.3.6 Routine changes

Routine changes shall be governed by their own procedures. Routine tasks include patch management of the operating environment, office applications and utilities, and anti-virus and intrusion detection signature updates. Patches on the operating system should always be tested in a test environment using formal test scripts. The test scripts should test the basic functionality of critical business applications, which run on the server that is affected by the change. Patches to office applications and utilities can create conflicts or bugs, but these types of deflects are difficult to test for and therefore are dealt with using the incident management procedure. Some organizations use a predefined group of user/customers (pilot group) in the production environment to test routine changes before implementing the change company wide.

**Principle 4.**

**Supervised institutions should manage IT assets and configuration information.**[10]

The objective of this principle is to accommodate financial, insurance, contractual, information security, risk assessment, inventory, incident management, problem management, and change management functions. Assets in this regard include all elements of software and hardware that are needed to run a business in a safe and sound manner.

With respect to the management of IT assets, supervised institutions should undertake the following:

### 4.1 Keep up-to-date inventory of all IT assets[11]

The Bank recommends registering the following information:

*Hardware:*
All items should be documented in an inventory list.
At least the following information should be captured per hardware item:

- ID;
- Serial number;
- Vendor and model;
- Processor capacity;
- Memory;
- Function;
- Owner;
- Custodian;
- Location;
- Purchase date;
- Purchase price.

[10] This principle enhances 'Asset Management' which is part of the ISO 27002, which was introduced in the 'Provisions and Guidelines for Information Security Management'

[11] When operating an IT system, it is important to understand the relationships between the components of the IT system, the function, the capacity, the location, and the configuration of the components. To accommodate smaller supervised institutions, we have made some suggestions of what information to collect for IT systems. However, supervised institutions should collect all information necessary for its unique circumstance and create all necessary procedures to achieve the objective of this principle.

In addition, at least the following information should be captured on servers:
- Operating system in use;
- Utilities running on the server;
- Storage capacity and amount of hard disks in use; and
- Applications running on the server.

Above mentioned server information can be captured using automated tools. Supervised institutions should capture and store such information at least monthly.

*Software:*
The following information should at least be included on the software inventory list:
- ID
- Application name;
- Version number;
- Manufacturer or vendor;
- Patch level;
- Number of copies installed;
- License information;
- Maintenance information;
- Business owner;
- Application administrator;
- Purchase date;
- Purchase price.

The supervised institution should have a software library[12] with the purpose to rebuild a business machine when deflects (bugs) occur or when upgrading or installing new business machines.

To support an automated application for incident, problem, and change management (principle 3), hardware and software components, often referred to as configuration items, are collected and stored in a database called the configuration management database 'CMDB'. It can be a challenge to record hardware and software components only once, and accommodate financial, insurance, contractual, information security, risk assessment, inventory, incident management, problem management, and change management functions, without having redundant information, which as a result, often causes maintenance issues.
Supervised institutions should create the necessary procedures to maintain updated information on hardware and software items in the various locations of use.

[12] Electronic libraries will be further detailed in the Provisions and Guidelines for System Development and Acquisition.

*Network topologies or other diagrams that detail the internal and external connectivity of communication networks:*
The following information should at least be captured and kept up to date regarding the internal and external connectivity:

- Blue print of the network infrastructure including all servers and devices;
- Type, location and volume of information stored and transmitted on the network;
- All internal and external connectivity (including dialup, modem, wireless, internet);
- Bandwidth of connectivity within and between network segments;
- Type and capacity of network segments linkages (e.g. switches, routers, hubs, gateways); and
- Configuration information of hardware devices (e.g. switches, routers, hubs, gateways), including technical documentation to describe the meaning of the configuration scripts.

## 4.2 Label IT assets

The Bank recommends to uniquely identify all hardware servers, PC's, peripherals, and communication lines using tamper-proof label stickers. Unique labeling facilitates inventory administration, documentation and communication purposes, and easy recognition when performing daily tasks.

## 4.3 Create and maintain technical documentation

Lack of technical documentation increases continuity and information security risks. For maintenance purposes, it is very important to create technical documentation for:

- In-house created software[13];
- Scripts (e.g. server scripts);
- Technical configuration of devices (e.g. routers, switches, firewalls); and the
- Network diagrams.

## 4.4 Inventory Review

Periodically, the inventory lists, network information and configuration information need to be reviewed to verify the integrity of such records.

## 4.5 Procurement of IT assets

There must be a documented procedure for the procurement of IT assets and IT services.

## 4.6 Disposal of IT assets

There must be a documented procedure for the disposal of IT assets. IT assets should not be taken off the premises without prior authorization. All sensitive data and licensed software should be removed or securely overwritten prior to their disposal.

[13] This process will be further detailed in the future "Provisions and Guidelines for System Development and Acquisition".

**Principle 5.**

**Supervised institutions should protect the physical computer environment to guarantee IT services.**

The objective is to prevent unauthorized physical access, damage, theft, and interference with the organization's computer environment[14].

### 5.1 Site Selection and Layout

The selection and design of a site should take into account energy use, the risk associated with natural and man-made disasters, and relevant laws and regulations, such as occupational health and safety regulations.

### 5.2 Physical Security Measures

Physical security measures must be capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, humidity, fire, smoke, water, vibration, terror, vandalism, and power outages.

- The computer environment should reside in a secure area, protected by defined security perimeters, with appropriate security barriers and entry controls.
- The computer environment should consist of fire resistant materials, surveillance cameras and a fire suppression system.
    - When fire extinguishers are used to control fires, preferably use carbon dioxide (CO2) fire extinguisher or any other type especially designed to extinguish electrical fires.
- Emergency marshals should be appointed and trained in carrying out the duties to be effective in the event of an incident.
- Temperature controls and fire/smoke detectors must be installed, where the alarm system should not only boast a sound alarm, but also automatically warn the fire department, management or a security company.
- The building, including the computer environment, should be inspected by the fire department regularly.
- Physical security measures should be tested for effectiveness periodically.

### 5.3 Physical Access

Procedures to grant limit and revoke access to premises, buildings and areas should be defined and implemented according to business needs, including emergencies. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors, or any other third party.

### 5.4 Physical Facilities Management

Managed facilities, including power and communications equipment, should be in line with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines.

[14] Also refer to ISO 27002 Chapter 9 Physical and environmental security

**Principle 6.**

**Supervised institutions should monitor the IT infrastructure in order to ensure continuous service on the network.**

The objective of network monitoring is to detect problems and optimize the performance of IT infrastructure, resources, and capabilities.

### 6.1 Determine log content

Procedures to monitor the IT infrastructure and related events should be defined and implemented. Management should ensure that sufficient chronological information is being stored in operation logs to enable the reconstruction, review, and examination of the time sequences of operations and the other activities surrounding or supporting operations.

### 6.2 Current Performance and Capacity

Current performance and capacity of IT resources should be assessed to determine if sufficient capacity and performance exist to deliver against agreed-upon service levels.

### 6.3 Future Performance and Capacity

Performance and capacity forecasting of IT resources should be conducted at regular intervals to minimize the risk of service disruptions due to insufficient capacity or performance degradation, and identify excess capacity for possible redeployment. Workload trends should be identified and forecasts should be determined, to be inputted into performance and capacity plans.

### 6.4 IT Resources Availability

The required capacity and performance should be provided, taking into account aspects such as normal workloads, contingencies, storage requirements and IT resource life cycles. Provisions such as prioritizing tasks, fault-tolerance mechanisms and resource allocation practices should be made. Management should ensure that contingency plans properly address availability, capacity and performance of individual IT resources.

### 6.5 Monitoring and Reporting

The performance and capacity of IT resources should be continuously monitored. The objective is to maintain and tune current performance within IT and address such issues as resilience, contingency, current and projected workloads, storage plans, and resource acquisition. A procedure should exist to create exception reports with recommendations for corrective action.

**Principle 7.**

**Supervised institutions should implement a backup/restore procedure to comply with business needs and legislation.**

The objective of a backup/restore procedure is to create a safety net to recover from computer deflects, major incidents, human error, and to comply with legislation.

### 7.1 Legislation.

Supervised institutions should have a backup/restore procedure in place to comply with legislation[15].
Supervised institution should create backup/restore procedures to ensure that all backup data remains accessible for future access.

If data is kept in an electronic format, it needs to stay accessible over time. For data that is stored for ten years, this can be a challenge for the following reasons:

- the hardware is no longer available to read the electronic information (e.g. in order to read a zip disk a zip drive is needed);
- the application version to display the data may not be available (e.g DisplayWrite 4 files need the application DisplayWrite 4, a DB3 file needs dBase III); or
- the operating system to run the application is not available (e.g to run dBase III the operating system DOS is needed).

### 7.2 Grandfather/father/son principle[16].

Supervised institutions should have a backup/restore procedure using the grandfather/father/son principle according to the following three cycles of backup:

- Daily backup cycle: The daily backup cycle should contain at least 5 weeks of daily data backups.
- Monthly backup cycle: The monthly backup cycle should contain at least 12 end of month full system backups.
- Yearly backup cycle: The yearly backup cycle should contain at least 10 end of year full system backups. If a supervised institution is able to comply with legislation through other means such as hard copy of information, then the yearly backup cycle should contain at least the last 5 end of year full system backups.

Supervised institutions are advised to create the monthly backup after the month-end book closing and the yearly backup after the year-end book closing.
The end-of-month and end-of-year backups must consist of a full system backup (data, operating system, application executable and source files) of all servers[17] and should be locked away in a secure environment.

[15] Appendix 3 contains some legislation with respect to data retention.
[16] See also ISO 27002 Par. 10.5 Back-up
[17] Including: Domain controller, Webs sites hosted outside the company, Hardware configuration

### 7.3 Daily backup procedure.

A procedure should be available for the backup operators to use. The following is recommended:

- To label the backup media indicating to which cycle (day, month, year) and which sequence in the cycle (e.g. 1, 2, 3) the media belongs.
- To write on the label[18] the first day of usage of the media in order to determine the age the media;
- To take the media out of service after a standard period of usage (media dependent) or after the media is not working properly;
- To check if the backup job came to a faultless finish;
- To encrypt the data on the backup media;
- To keep backup media in a secure environment e.g. in a waterproof fire resistant safe, but it should not stay longer than one day on-site ;
- To keep a daily log of all the steps performed regarding the backup process (e.g. a checklist); and
- To mention any out of the ordinary events in the daily log and report such events to the IT manager.

### 7.4 Transportation of backup media.

A procedure should be available for transportation of backup media[19]. The procedure will (or should) contain the following:

- A log file containing the following information; the name of the person taking, transporting, and keeping the backup media, including the date, time, and media number of the backup media being transported;
- That the backup files should be transported directly from the on-site to an off-site location with no stops in between;
- That Backup files are placed in a dust-free cabinet;
- That Backup files are never subjected to heat, moisture, electromagnetic fields or direct sunlight that could damage the backup media contents; and
- That Backup files are kept off-site in a secure location and environment, e.g. waterproof and fire resistant safe.

### 7.5 Restore testing.

Backup files must be periodically restored in a test environment. The integrity of the data is tested using formal test scripts. The frequency should be at least quarterly and randomly choosing backup files from all the three cycles. The test and test results should be documented.

[18] Refers to physical labels on physical backup media.
[19] Backups may be transferred on-line. In such case no physical transportation procedure is needed.

**Principle 8.**

**Supervised institutions should manage third party services.**

The objective of this principle is to govern third party services. Services obtained from third parties should be in line with the third party service level agreement/contract.

## 8.1 Acquiring third party services

Supervised institutions should thoroughly investigate third parties before entering into a long-term agreement.

The background check should at least include:

- Financial status, including reviews of the audited financial statements;
- References of customers (including long term and more recent customers);
- Internal control environment, security/service history, and audit coverage;
- Technology and systems architecture in use;
- IT Security controls in use;
- Legal and regulatory compliance performed;
- Current legal issues with customers and other parties;
- Insurance types and coverage; and
- The ability to meet disaster recovery and business continuity requirements.

The Bank requires that at least three requests for proposals (RFP's) be solicited, received and reviewed, to compare third parties.

## 8.2 Third party service management[20]

The supervised institution should ensure that the security controls, service definitions, and delivery levels included in the third party service level agreement/contract, are implemented, operated, and maintained by the third party.

The third party service level agreement/contract should at least contain the following:

- Duration of the contract;
- Termination conditions of the contract;
- Rights and responsibilities of both parties;
- Description of the service, communication including reporting, scheduled and agreed interruptions, and notification process;
- Contact details of people authorized to act in emergencies, to participate in incidents and problem correction, recovery and work around;
- Workload limits (upper and lower) e.g. the ability of the service to support the agreed number of users/volume of work, system throughput and system performance;
- Dispute and escalation procedure;

[20] See also ISO 27002 Par. 10.2 Third Party Service Delivery Management

- Overview of the relationships of the third party and subcontractors of the third party, and work performed by subcontractors;
- Adequate and measurable service level agreement (e.g. availability and time windows of services response/resolve effort);
- Initial and yearly license and maintenance fees (prevent hidden fees);
- Non-disclosure agreement;
- Types and coverage of insurance by third party;
- Change management controls (take into consideration item '3.3 Change Management';
- Notifying requirements and approval rights for any material changes to service, systems, controls, key personnel, subcontracting to other parties, insurance coverage, and service location;
- Notifying requirements for organizational changes such as mergers, changes in partnerships, and when the third party files for suspension of payments (such as the US laws for filing with a federal bankruptcy court for protection under either Chapter 7 or Chapter 11);
- Notifying requirements for any intrusion that has lead or may have lead to a security breach (e.g. data leakage, illegitimate system access) and other events, which may cause reputational damage to the supervised institution or causes interference of normal production of the IT system in use by the supervised institution;
- Agreement concerning disaster recovery and business continuity;
- Frequency and types of reports received from third party;
- Obligations concerning daily IT Operation management, such as:
    - Patch and anti-virus management;
    - Backup and restore management;
    - Operating System fine-tuning (e.g. deletion of temp- and unused compressed; files, disk- error checks and defragmentation);
    - Log analysis;
    - Network monitoring;
    - User account management for the network;
    - User account management for the business applications; and
    - Sign-off procedure for performed work;
- Compliance with all regulations of the Bank, including provisions and guidelines for Business Continuity Management, Information Security Management and IT Service Management

In case a model is used where the application and data is stored with the third party, the following needs to be part of the third party service level agreement/contract:

- The supervised institution should remain the owner of its own data;
- Data must be stored encrypted;
- Encryption key is only known to the supervised institution, where the third party cannot access the data in a readable format[21];
- If the supervised institution whishes to terminate the contract with the third party, it must has the right to a copy of their data in a format that can be re-used elsewhere and with the certainty that the third party destroys all copies of the data of the supervised institution in its possession;
- The Bank should have the right to audit the third party's IT infrastructure (including computer facilities, hardware, operating environment, application and database);
- For critical outsourced financial systems, an independent audit firm should annually review the third party's IT service management. The audit should be in accordance with the International Standard on Assurance Engagements ("ISAE") 3402; "Assurance Reports on Control at a Service Organization", issued by the International Auditing and Assurance Standard Board and in accordance with the Statement on Standards for Attestation engagements ("SSAE") 16; "Reporting on Controls at a Service Organization", issued by the American Institute of Certified Public Accountants. Furthermore, the third party should comply with all relevant regulations issued by the Bank, including all 'Provisions and guidelines'.

### 8.3 Monitoring and review of third party services

Monitoring and review of third party services should ensure that the terms and conditions of the agreements are being adhered to, and that IT incidents and problems are properly managed. Therefore, the supervised institutions and their respective third party should agree on:

- Monitoring service performance levels to check adherence to the agreements;
- Reviewing service reports produced by the third party and arrange regular meetings for discussions thereon;
- Providing information about IT incidents and operational problems; and
- Resolving and managing any identified problems.

Supervised institutions are ultimately responsible for the work performed by third parties. As a result, supervised institutions should maintain sufficient overall control and visibility into all IT aspects managed by a third party. The reporting process, format and structure by the third party should be clearly defined. Appropriate actions should be taken when deficiencies in the service delivery are observed.

[21] For maintenance reasons third parties might need access to the data in an unencrypted format. The supervised institution need to assure that sufficient compensating controls will be in place to prevent information leakage.

**Principle 9.**

**Supervised institutions should standardize IT financial management.**

The objective of IT financial management is to accurately predict, account for, and optimize costs of required resources to deliver cost effective and reliable end-to-end IT services.

### 9.1 Financial Management Framework

Supervised institutions should establish and maintain a financial framework to manage the investment and cost of IT assets and services through portfolios of IT enabled investments, business cases and IT budgets. The accounting system and sub systems should provide timely and accurate information to feed the decision making processes to manage IT finances.

### 9.2 Preparing the IT Budgeting

Supervised institutions should establish and implement practices to prepare a budget for investment programs, education, and the ongoing costs of operating and maintaining the current IT infrastructure. The IT budget should have at least the following items accounted for:

- Replacement of depreciated assets;
- Additional assets for new systems, business continuity and new personnel;
- License and maintenance fees and other fees from contracts;
- Insurance fees, if not accounted for on a company level;
- IT project portfolio;
- Training costs;
- Hiring costs; and
- Outsourcing costs.

### 9.3 Cost Management

Supervised institutions should implement a cost management process comparing actual costs to budgets. Costs should be monitored and reported upon.

### 9.4 Prioritization within the IT Budget

Supervised institutions should implement a decision-making process to prioritize the allocation of IT resources for operations, projects, and maintenance. The practices should allow for ongoing review, refinement and approval of the overall budget and the budgets for the IT project portfolio during the year. Management should meet quarterly to review the financial performance of the company, and the performance of the IT project portfolio and other IT investments, in order to decide to enlarge, cut down, or shift resources.

When deviations from the original timelines, cost or resource usage are noted, the impact of those deviations on IT project portfolio should be assessed. Together with the business functions affected, appropriate remedial actions should be taken and, if necessary, business cases should be updated and re-evaluated.

**Principle 10.**

**Supervised institutions should continuously educate and train IT personnel and users**

The objective is to provide IT personnel and internal users with ongoing training to maintain their knowledge, skills, abilities, and security awareness at the level required to achieve organizational goals.

Supervised institutions shall:

- Determine the competence needed to perform daily duties;
- Where applicable, provide training or take other actions to acquire the necessary competence;
- Provide cross-training and create a knowledge sharing culture to mitigate the risk that a single person has the sole knowledge in specific areas;
- Motivate personnel by creating personal development plans and career paths, including training needs;
- Train personnel for general and specific information security tasks[22];
- Maintain records of education, training, skills and experience; and
- Determine yearly if employees require training as a result of the evolvement of IT in the company.

In the case of third party services, it is also important to determine that third parties remain competent to deliver the required level of services.

Large supervised institutions are encouraged to implement the ISO 20000-series, COBIT version 5 or ITIL version 3, and train personnel accordingly.

[22] See also "Provisions and Guidelines for Information Security Management – Principle 7"

**Principle 11.**

**Supervised Institutions should ensure the quality of all aspects of ITSM through independent audits.**

Audits should provide independent, objective assurance, and consulting service designed to add value and improve the institution's IT Service Management.

The auditor should review whether the IT Service Management and plans are adequate and effective, and if the institution operates accordingly in a manner to ensure that:

- The institution's IT strategy is executed and in accordance with business requirements and applicable laws and regulations;
- There is a collective understanding of the institution's threat, vulnerability and risk profile;
- Risks are appropriately identified and managed;
- Interactions with the various stakeholders occur as needed;
- Important financial, managerial, and operating information is accurate, reliable, and timely;
- IT Service Management practices are standardized;
- Policies, standards and procedures are continuously updated;
- Employees' actions are in compliance with policies, standards and procedures, and tested for effectiveness;
- IT Service Management roles have sufficient and competent back-up staffing;
- Resources are acquired economically, used efficiently, and are adequately protected;
- Programs, plans and objectives are achieved;
- Quality and continuous improvement are accomplished; and
- Opportunities for improving the IT Service Management processes or the organization as a whole are recognized and addressed appropriately.

**Principle 12.**

**Supervised institutions should inform the Bank when critical IT systems are being replaced or innovative products will be introduced.**

Supervised institutions must inform the Bank of their plans to replace a critical IT system or to introduce an innovative product to the current critical business systems.

A few examples are:
- A supervised institution is planning to change its Financial application
- An insurance company is planning to migrate its current general insurance system to a new general insurance system.
- A commercial bank is planning to implement a new service for customers to interact with their current account via a smart phone.
- A supervised institution is planning to build a new data center and move all its IT operations.

Changes to critical IT systems as mentioned above introduce new risks and the Bank needs to know up front that sufficient measures will be taken to mitigate these risks.

All test scripts should be thoroughly tested and the test results documented. The Project Manager and the Internal Auditor have to verify that all functions have been tested according to the test scripts, that the project is signed-off by all stakeholders and that the new product is moved into production only after receiving written approval from management.

# Appendix 1: Glossary/Definitions

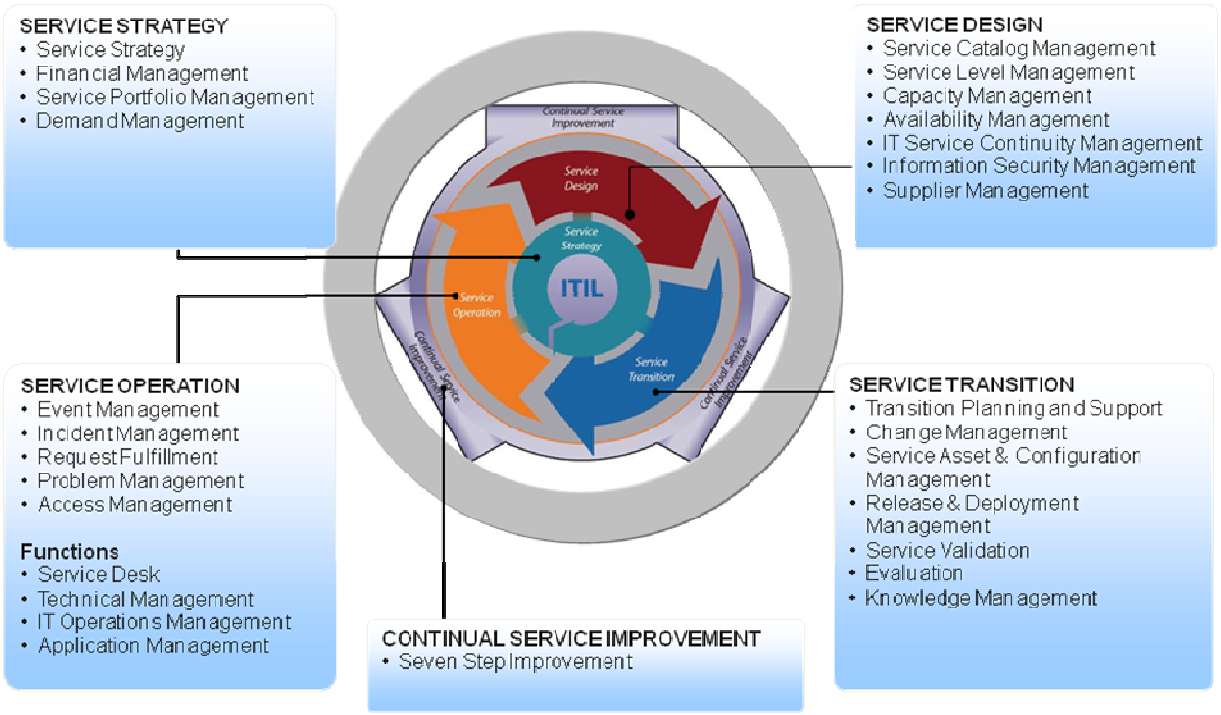
| | |
|---|---|
| **Audit** | A systematic and independent examination of data, statements, records, operations and performances (financial or otherwise) of an enterprise for a stated purpose. In any auditing the auditor perceives and recognizes the propositions before him for examination, collects evidence, evaluates the same and on this basis formulates his judgment which is communicated through his audit report. |
| **Availability** | Ensuring timely and reliable access to information sources. |
| **Backup** | A process, by which data, electronic or paper based, is copied in some form to be available in case the original data is lost, destroyed or corrupted. |
| **Change request** | Proposal for a change to be made to a service, service component or the service management system. |
| **Cloud computing** | Network-based services using virtual servers over the internet. |
| **Control Objectives for Information and Related Technology (COBIT)** | Framework created by ISACA for IT management and IT governance. |
| **Confidentiality** | Preventing disclosure of information to unauthorized individuals or systems. |
| **Configuration baseline** | A formal record of the configuration of a device obtained at a certain point in time. |
| **Configuration item** | Element that needs to be controlled in order to deliver a service or services |
| **Configuration management database (CMDB)** | Data store used to record attributes of configuration items, and the relationships between configuration items, throughout their lifecycle. |
| **Incident** | Unplanned interruption to a service, a reduction in the quality of a service or an event that has not yet impacted the service to the end user. |
| **Information security** | Preservation of confidentiality, integrity and availability of information. |
| **Information security incident** | Single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. |
| **Infrastructure as a Service (IaaS)** | In the most basic cloud-service model, providers of IaaS offer computers – physical or (more often) virtual machines – and other resources. |

| | |
|---|---|
| **Integrity** | The assurance that data is consistent, correct, not manipulated, and includes ensuring information on non-repudiation and authenticity. |
| **Key Goal Indicator** | Helps an organization define and measure progress toward organizational goals. Once an organization has analyzed its mission, identified all its stakeholders, and defined its goals, it needs a way to measure progress toward those goals.<br>Key goal indicators are a measure of "what" has to be accomplished. |
| **Key Performance Indicator** | Key Performance Indicators are measures that tell management that an IT process is achieving its business requirements by monitoring the performance of that IT process.<br>It is a measure of "how well" the process is performing. |
| **Known error** | Problem that has an identified root cause or a method of reducing or eliminating its impact on a service by working around it. |
| **Patch management** | A patch is a piece of software designed to fix problems. Patch management is the process of using a strategy and plan of what patches should be applied to which systems at a specified time. |
| **Platform as a Service (PaaS)** | In the PaaS model, cloud providers deliver a computing platform, typically including operating system, programming language execution environment, database, and web server. |
| **Problem** | Root cause of one or more incidents. |
| **Procedure** | Specific way to carry out an activity or a process. |
| **Recovery Time Objective (RTO)** | The duration of time required to resume a specified business operation. It has two components, the duration of time from activation of the business continuity plan and the recovery of business operations. |
| **Recovery Point Objective (RPO)** | A point in time to which data, should be restored from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a disruption. |
| **Risk** | Effect on uncertainty on objectives. |
| **Risk Assessment** | Steps in the assessment include:<br>- Identification of assets;<br>- Identification of threats and vulnerabilities;<br>- Identification of controls;<br>- Analyzing risk (probability/impact);<br>- Evaluate risk (assessing residual risk). |

| | |
|---|---|
| **Risk Management** | A structured approach to managing uncertainty related to a threat. It includes a sequence of human activities to manage risk namely: risk assessment, strategies development to manage it, and mitigation of risk using managerial resources.<br>The strategies include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk. |
| **Sarbanes–Oxley Act 'SOX'** | A United States federal law that set new or enhanced standards for all U.S. public company boards, management and public accounting firms. |
| **Service** | Means of delivering value for the customer by facilitating results the customer wants to achieve. |
| **Service Level Agreement** | Documented agreement between the service provider and customer that identifies services and service targets. |
| **Service Management** | Set of capabilities and processes to direct and control the service provider's activities and resources for the design, transition, delivery and improvement of services to fulfill the service requirements. |
| **Single point of failure** | A unique source of a service, activity, and/or process, where there is no alternative and whose loss could lead to the failure of a critical function. |
| **Software as a Service (SaaS)** | In the business model using software as a service (SaaS), users are provided access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. |
| **Third party** | An external organization that supplies services to the organization. |

# Appendix 2: ITIL v3 Life Cycle Processes

http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library



# Appendix 3: Legislation[23]

**Book 2 of the Civil Code of Curaçao states in article 15:**
1. The management must, for administrative purposes, keep a record of the financial condition and of everything related to the activities of the legal person according to the requirements to which such activities give rise, and it must keep the books, documents and other data-carriers in respect thereof in such manner that the rights and obligations of the legal person can be ascertained therefore at any time.
2. Without prejudice to the provisions elsewhere in the law, the management must annually, within eight month from the end of the financial year, prepare a written annual account, comprising at least a balance sheet and a statement of income and expenditure.
3. The management must keep the books, documents and other data-carriers referred to in paragraphs 1 and 2 for ten years.
4. All data recorded on a data-carrier, except for the written balance sheet and statement of income and expenditure, may be transmitted to and kept on any other data-carrier, provided the data are rendered correctly and completely when such transmission is made and these will be available during the entire period that these must be kept and can be rendered legible within a reasonable time.

**National Ordinance on the supervision of banking and credit institutions (NOSBCI 1994, N.G. 1994, No. 4) article 42:**
Credit institutions are obliged to keep for at least ten (10) years all letters, supporting documents and other data carriers (media) with regard to the institution and also all records regarding mutations on personal and other persons accounts with accompanying letters, supporting documents and data carriers (media).

**Privacy Act Curacao - Landsverordening Bescherming Persoonsgegevens, AB 2010, 84:**
The Privacy Acts describe all handling of personal data from the collection to the destruction thereof as data processing. Of significant importance is that the personal data can only be collected for a specific, justified objective. Personal data shall be supplied, processed and used in accordance with the laws and shall at all time be subject to principles of fairness and due care.

**Provisions and Guidelines for Safe and Sound Electronic Banking (2011**):
Recordkeeping: All e-banking transactions should generate clear audit trails, which should be archived and kept for 10 years. ATM video surveillance recordings should be archived for at least six months. It is also vital to generate and protect records of customer instructions in a legally acceptable format. Credit institutions should strengthen information security controls to preserve the confidentiality and integrity of customer data. Firewalls, ethical hacking tests, physical and logical access controls are some of the methods available. Recordkeeping requirements should be based upon the level of activity and risk.

[23] Disclaimer: Please refer to the authentic sources for genuine text.

# Appendix 4: Risks for Cloud Computing

| | | |
|---|---|---|
| **Organizational risks** | | |
| 1 | Lock-in | Risk of not being able to migrate easily from one provider to another. |
| 2 | Loss of Governance | Control and influence on the cloud providers to implement supervised institution's specific requirements. |
| 3 | Compliance challenges | The risk Cloud Providers can not comply with legislation and regulatory requirements. |
| 4 | Reputational damage | The risk that the name of the cloud provider is damaged due to unlawful activities carried out by the cloud provider or one of its customers. |
| 5 | Cloud service termination | The risk of providers going out of business. |
| 6 | Cloud provider acquisition | Acquisition of the cloud provider could increase the likelihood of a strategic shift and may put non-binding agreements at risk. |
| 7 | Supply chain failure | A cloud provider can outsource certain specialized tasks of its 'production' chain to third parties. The risk of non-compliancy by subcontractors for regulations, legislation and contract obligations between the main contractor and the supervised institution. |
| 8 | Changing regulations | The risk of changes in legislation and regulations could impact the requirements for both the supervised institution and the cloud provider. |
| 9 | Insufficient skills and knowledge to identify risks related to Outsourcing / Cloud computing | The risk that the supervised institution has insufficient skills and knowledge to identify the risks involved or to assess the operational effectiveness of the controls at the Cloud provider. |
| 10 | Risk of ownership | The risk of unclear data ownership. |
| **IT Operations risks** | | |
| 11 | Resource exhaustion risk | The risk that the cloud provider has not got sufficient control to predict resource usage by customers. |
| 12 | Isolation failure | The risk that the cloud provider has insufficient controls to isolate data, application or database access between customers who share storage, memory, routing in the shared infrastructure. |
| 13 | Cloud provider malicious insider – abuse of high privilege roles | The malicious activities of an insider could potentially have an impact on: the confidentiality, integrity and availability of all kind of data, IP, all kind of services and therefore indirectly on the organization's reputation, customer trust and the experiences of employees. |
| 14 | Intercepting data in transit | Sniffing, spoofing, man-in–the-middle attacks, side channel and replay attacks should be considered as possible threat sources |
| 15 | Illegitimate system access | The risk of Illegitimate system access caused by an improper access and identity management. |
| 16 | Licensing risks | Licensing conditions, such as per-seat agreements, and online licensing checks may become unworkable in a cloud environment. |
| 17 | Data protection risks | It should be clear where data is stored. This applies also for backup data in a vault location and replicated data in a secondary or third datacenter. |

| Compliance risks | | |
|---|---|---|
| 18 | Subpoena and e-Discovery | The risk of disclosure of centralized storage as well as shared physical hardware. |
| 19 | Data protection risks | The risk of not being able to validate if data is handled in a lawful way. Compliant to regulations like privacy laws, as well as encryption standards apply. |
| 20 | Specific local data privacy | The risk that other law and regulations apply at the location where the datacenter is situated compared to where the contract party is situated. |
| 21 | Risk of conflicting regulations | Laws and regulations due change on a regular basis. The risks exist the cloud provider cannot to comply with both regulations. |
| 22 | Unable to recover after a disaster | Insufficient testing for Disaster Recovery. Non compliance to Provisions and Guidelines for Business Continuity Management. |
| 23 | Unable to protect information sufficiently | Non compliance to Provisions and Guidelines for Information Security Management. |
| 24 | Lack of operational procedures | Non compliance to Provisions and Guidelines for IT Service Management |

# Appendix 5: Links to helpful websites

| Organization | Website |
|---|---|
| FFIEC | http://ithandbook.ffiec.gov/it-booklets.aspx |
| ISACA | www.isaca.org/cobit.htm |
| MS MOF | http://technet.microsoft.com/en-us/library/cc506049.aspx |
| ITIL | http://www.itil-officialsite.com/home/home.asp |
| ISO 20000 | http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51986<br>http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41333 |