Business Continuity Management for Airline Operations

Ing. Vijay Hiralall (1895575)

April 2011

Vrije Universiteit Amsterdam

Faculteit der Economische Wetenschappen en Bedrijfskunde (FEWEB)

Postgraduate IT Audit

De Boelelaan 1105

1018 HV Amsterdam

Thesis coach at Vrije Universiteit Amsterdam

- **Dr. Rene Matthijsse RE**
  - Telephone: 06-27159626
  - Mail: matthijsse.rene@gmail.com

Thesis coach at Air France-KLM

- **Jacqueline A.M. Holla RE,** Manager IT Audit
  - Department: AMS/DC – Internal Audit
  - Telephone: 020-6495431
  - Mail: Jacqueline.holla@klm.com

Author – Employee of Air France-KLM

- **Ing.** Vijay Hiralall
  - Department: CIO/IS/Operations - IT Auditing
  - Telephone: 020-6481896
  - Mail: roy.hiralall@klm.com

Summary

Businesses of all sizes heavily depend on their Information Technology Systems for the daily operations. Their dependence is such that any disruption as a result of a fire, system crash, flooding, lightning, employee sabotage or terrorist attack could affect their survival.
Airline operations depend on continuous availability of Information Technology Services for their ticket sales, passenger- and cargo transportation and aircraft maintenance handling in the hangars and at the airport. For continuous availability of Information Technology Systems, airline operations need to implement measures for continuous availability of business processes with almost zero data loss. Before implementing measures it is important to know which businesses processes are mission critical and which methodology should be used for continuous availability of business processes for the daily airline operations.

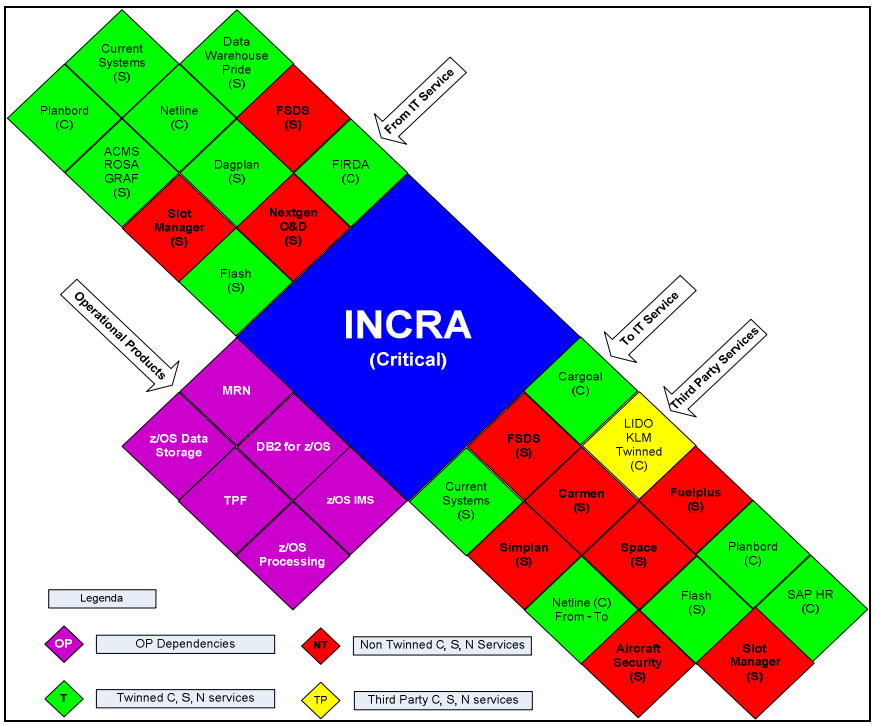
The intention of the research is to investigate which IT Infrastructure components (data, applications, systems and networks) have a primary relationship with airline operations and how major risk areas are managed and controlled for continuous availability of the business processes. The literature review did not reveal such a research in the world focussing on Business Continuity Management for airline operations.

The research is performed within the Air France-KLM division of Passenger Operations and Engineering & Maintenance. The reason that these two divisions were selected is that it represents more than 85% of the Air France-KLM revenues. The research has an exploratory character in a triangulation approach. For the first part, literature is reviewed about airline operations, Information Systems, Infrastructure components, the management of IT risks areas, methods and good practices for BCM and IT General Controls. The second part is performed by open interviews based on a set of pre-selected questions to determine the current BCM implementation. The third part is performed with a set of audit questions from the Business Continuity Institute PAS56 audit Workbook. Questions not clarified by the interviewed, is completed by the author based on available BCM documentation and experience gained during the realization of IT Disaster Recovery Plans for Air France-KLM.

The conducted literature research proposed to implement solutions for uninterrupted availability of business processes based on BCI PAS 56 “good practice” for BCM. The result of the research did not reveal that all parts of PAS 56 stages were implemented. Interviews and documentation persuaded me that parts of the BCM solutions for Critical IT Services for continuous availability of airline operations are in line with known “good practice”. The current implemented BCM is based on BS17799:2005 – Code of Practice for Information Security. The PAS 56 audit Workbook execution shows implementation gaps that can be filled out if IT leaders decide to adopt and implement BS 25999-1 and BS 25999-2 that replaces PAS 56. This could increase the current maturity level of BCM within Air France-KLM.

The conducted audit to benchmark the Air France-KLM Business Continuity Management Process against the BCI PAS56 audit workbook convinced me of the value of the questions within the six stages of PAS56. It gives a usable overview of the controls that must be implemented in a mature Business Continuity Management Process. The design and existence of implemented IT Service Management (ITSM) processes is a prerequisite for a mature Business Continuity Management Process. During the research I concluded that ITSM processes were implemented for the assurance of uninterrupted IT Services. As a result of the case study, a control model is designed for the establishment and auditing of Business Continuity Management for continuous daily airline operations. The control model describes the controls to be implemented for Critical IT Services and related major risk areas.

The intention of the Air France-KLM Business Continuity Management Process is to twin all Critical IT Services and that twinned IT Services must not depend on a non-twinned service. To verify dependencies, I have designed an Integrated E2E IT Service dependencies framework. For the case study, the Critical IT Service INCRA was verified on dependencies on other twinned/not-twinned IT Services. The exercise shows that for example the critical IT service INCRA has dependencies with IT services that are twinned and those that are not twinned. Because of the current design, the functionality in a fallback situation of the critical IT Service INCRA cannot be determined. The outcome of the exercise convinced me that dependencies between critical IT Services need to be investigated in an E2E environment. A critical IT Service must not be seen as standalone but in the IT landscape in which it acts. Twinned Critical IT Services have dependencies on IT Services that rely on Third Party IT Services that are not regularly assessed on their recoverability. This situation might also be relevant for other twinned critical IT Services that has dependencies on non-twinned services.



Source: V. Hiralall – Integrated E2E IT Service dependencies framework

Contents

Preface

The most difficult problem was to choose a subject for my Master thesis that could increase my knowledge. I had two arrows on my arc: Information Technology General Controls for the Financial Year End control or Business Continuity Management. For the first subject I gained experience during my previous ITGC testing work for compliance with the Sarbanes-Oxley Act of 2002 legislation, previously a legal obligation for Air France-KLM as a U.S. publicly listed company. For the second subject I gained experience during my previous role as continuity coordinator at Air France-KLM.

After consulting my thesis coordinator he advised me to choose a subject where I have most knowledge of. I choose Business Continuity Management as my thesis subject. After the approval of the thesis proposal the vacation started and that was a big pitfall for the progress of the thesis. During July and August the progress of the thesis was very low profile. In September I started full swing with the setup of a knowledge base containing literature and publication regarding my thesis subject. In September the period of ITGC audit test work FY2010_11 started at Air France-KLM and it also mend a period of long days at work and late at home. When at home I was “total lost” but had to spend hours till after midnight to move forward in the establishment of my Master thesis for the graduation. After five months of struggling and hard working, I have managed to handover the draft version of my Master thesis, to be completed end of March 2011.

I’d like to thank the following persons that made it possible for me to access the course of IT Auditing at the VU University Amsterdam. Mr. Eric Schutte – Director Transversal NL my current Senior Manager and Mr. Norbert van der Hoek my former Manager of PIM (Process Implementation Management). I also like to thank Mrs. Jacqueline Holla RE – Manager IT Auditing at Air France-KLM, who coached me with my thesis subject and Mr. Dr. Rene Matthijsse RE, my VU coach that directed me during the writing process. I also like to thanks the colleagues of the Information Management Organization of Passenger Operations and Engineering & Maintenance that made time for me for the interviews and helped me with information regarding the status of Business Continuity Management.

Special thanks to my mother were I stayed several weekends to read through the massive Business Continuity Management information downloaded from Internet. Her aim during my studying at her home was only to pamper me with food & beverage on a continual basis without a Service Level Agreement. She was very pity with me about the hours that I was constantly busy without stopping for some rest. I also express my sincere gratitude to my wife and children for the time I could not accompany them during weekend shopping and parties.

Vijay Hiralall
Amsterdam, 1 April 2011

1. Introduction to the Thesis

1.1. The reason for the research

Over the past 20 to 30 years, businesses of all sizes have steadily grown more dependent on their expanding IT infrastructures to help them automate, manage, and analyze their business operations and strategy. Whether it's online trading, airline reservations and operations, financial databases, Web sites, or other computing systems, business are more and more dependent on the continuous availability of Information Technology Systems.

Their dependence is such that a failure of its IT infrastructure environment as a result of a fire, system crash, flooding, lightning, employee sabotage or terrorist attack could affect their survival. In the past, it was sufficient enough to restore automated data processing within a period of 24 hours for critical business services. With the current availability requirements of web portals (online and 7x24 hours) that generates major sales and revenues, disruption of Information Technology Systems for some hours can be fatal for the image and survival of the company. They need to shorten their requirements for **R**ecovery **T**ime **O**bjectives and **R**ecovery **P**oint **O**bjectives to stay competitive.

Airline operations heavily depends on continuous availability of Information Services for their ticket sales, Customer Relationship Management, passenger-, cargo- and aircraft maintenance handling in the hangars and airline operations at the airport. Information Technology Infrastructure Components are heavily used for passenger satisfaction and for the fulfilment of an efficient airline operation. IT leaders recognize that IT infrastructures face varying risks of interruption that prevents their business from accessing the data and systems it needs to operate. The objective of the research is to find out if Risk Assessment (RA) or Business Impact Analysis (BIA) can reveal the dependencies of Critical IT Services for a particular business. Once the BIA is done, the next step is to define strategies for recovery, resumption of business and other key activities. From the analysis it can categorize which business processes in which order must be recovered elsewhere.

1.2. Research objective

Given the shrinking timeframes for **R**ecovery **T**ime **O**bjectives and **R**ecovery **P**oint **O**bjectives to stay competitive in the airline operations, there is a need for a framework for the implementation of Business Continuity Management (BCM) for organizations with a strong IT dependency. With Business Continuity Planning (BCP) and IT Disaster Recovery Planning (IT DRP) as components of Business Continuity Management, it can be The Process, to recover from a disaster situation to a controlled return to “business as usual” within the given **R**ecovery **T**ime **O**bjectives. An implemented framework for Business Continuity Management can provide continuous improvement and operational excellence on a varying risk of IT infrastructure interruptions.

1.3. Problem definition

To determine whether a “Best Practice” framework is used for the realization of Business Continuity Management at Air France-KLM, the following central research question and sub question were asked.

Central research question:

Which IT Infrastructure components (data, applications, systems and networks) have a primary relationship with airline operations and how can major risk areas made manageable and controllable for continuous availability of business processes?

To give an answer to the central main question, the following three (3) sub questions will be answered by analyzing the implemented Information Technology management processes within Passenger Operations and Engineering & Maintenance at Air France-KLM.

Sub question (1) – Describe

What do the business processes and underlying Information Technology Systems for airline operations look like?

Sub question (2) – Analyze

Which major treats and risk areas can be identified and how can appropriate mitigation measures be taken?

Sub question (3) – Consider

Which elements and characteristics are included in the control framework for the establishment and auditing of Business Continuity Management for continuous daily airline operations?

Can the use of International adopted “Good Practice for Business Continuity Management” frameworks, and the formulated central main and sub questions, give answer on the following questions:

- Where does Air France-KLM stand with the realization of Business Continuity Management?
    - What level of Business Continuity Management maturity is currently achieved?
- What is the Business Continuity Management goal of Air France-KLM?
    - What level of Business Continuity Management maturity is the ultimate goal of Air France-KLM?
- What roadmap has to be followed by Air France-KLM to achieve her BCM goal?
    - What is the most effective way to achieve this goal?

During the interviews, parts of the PAS 56 audit Workbook are used to undertake a self assessment to benchmark Business Continuity Management within Passenger Operations and Engineering & Maintenance against the British Standards Institute's Good Practice Guide

to Business Continuity Management. The assessment questions not filled by the interviewed will be completed by the author on basis of available Business Continuity Management documentation and experience gained during the realization of IT Disaster Recovery Plans.

After completion of the case study, conclusions can be made about the reached Business Continuity Management maturity. The recommendation will indicate which evolutionary path may / must be followed to achieve the desired maturity goal.

1.4. Structure of the research report

The study has an exploratory character in a triangulation approach. The research is divided into three parts: a literature review, open interviews and conducting a pre-selected set of questions from the Business Continuity Institute PAS 56 audit Workbook for Business Continuity Management.

If during the writing of the thesis, references to academic literature and publications are made, it will be mentioned with the indication **[x]**, where **x** stands for the number referring to the publication. The title of the used documents will be included in the reference list.

Chapter 2 describes the Air France KLM Group, their foundation, partners and the Sky Team Alliance and the Organization Structure.

Chapter 3 describes the following aspects of the research based on academic literature and publications.

- Airline Operations
- Information Systems;
- Infrastructure components
- Managing risk areas
- Business Continuity Management
- Crisis Management
- Information Technology General Controls

Chapter 4 describes the research methodology (case study) based on interviews with the Management of Passenger Operations and Engineering & Maintenance and standing management processes. To obtain an idea what business processes are relevant to ensure continuous daily airline operations, the following questions has been asked:

- Which IT services are critical or significant to ensure airline operations continuity?
- Which IT Infrastructure components are relevant to these IT services?
- Which risk areas are relevant to the listed IT services?
- Which IT services are already twinned and on what basis twinning was decided?

- Which requirements (classes of recovery) were used twinning these services?

This chapter also describes the Business Continuity Institute PAS 56 Audit workbook, the scores of the self assessment and the control framework for the establishment and auditing of Business Continuity Management to ensure continuous daily airline operations.

Chapter 5 describes the findings of the case study. The results of the interviews, the PAS 56 assessment and the suggested control framework for the establishment and auditing of Business Continuity Management to ensure continuous daily airline operations. It should lead to the findings of the analysis and research on the status of BCM within Passenger Operations and Engineering & Maintenance. Differences between the "BCM Good Practice Guidelines" theoretically examined in Chapter 3 and benchmarked against the Business Continuity Institute PAS 56 Audit workbook will be included in the findings of the case study.

Chapter 6 gives the conclusions on the case study findings. The results of the case study will be drawn about the current level of maturity in respect of BCM. In addition, conclusions and recommendations will be given how the Management of Passenger Operations and Engineering & Maintenance can increase the maturity level of Business Continuity Management for a continuous availability of IT Services for the daily airline operations.

Chapter 7 lists the used references of the Master thesis.

1.5. Standard Framework within Air France-KLM

Within Air France-KLM the following standards frameworks are used to manage Information Technology, Security and their underlying infrastructure:

- ITIL – IT Infrastructure Library
    - ITIL Service Management
    - ITIL Service Delivery
- BS ISO /IEC 17799:2005 – Code of Practice for Information Security Management
- PAS 56: 2003 - Public Available Specification 56 – Published by the British Standards Institution, in conjunction with the Business Continuity Institute and Insight Consulting. Used during the project- and implementation phase of IT Disaster Recovery Planning
- CobiT for SOx, 2nd Edition – Testing of IT General Controls for the financial annual audit
- Prince2 – Project Management
- "Symphony" - Common AFKL development method

2. The Air France-KLM Group

Profile

Before starting with the literature review hereby a sort profile of Air France-KLM and their core businesses. The Air France-KLM Group, born on the merger between Air France and KLM in 2004, is building its development on the complementary between the two airlines in their three principle business: passenger transportation, cargo transportation and aeronautics maintenance and overhaul services. The Group has world-ranking positions in each of its business. Air France-KLM is a European leader in passenger transportation, which represents around 80% of its revenues. The Group is global leader in cargo transportation, its second business with 12% of revenues. On the aeronautics maintenance market (5% of revenues), Air France-KLM ranks number two amongst the multi-product players world-wide. With operations in every continent, the Group has more than 104.000 employees, fly's 71.4 million passengers to 244 destinations, has 594 aircrafts in operation and 21 billion euros in turnover. Both companies benefit from each other's strong points, e.g. customer loyalty, global networks, the Schiphol and Charles de Gaulle hubs. The head offices are located at Amstelveen and at Roissy-Charles the Gaulle Airport near Paris.

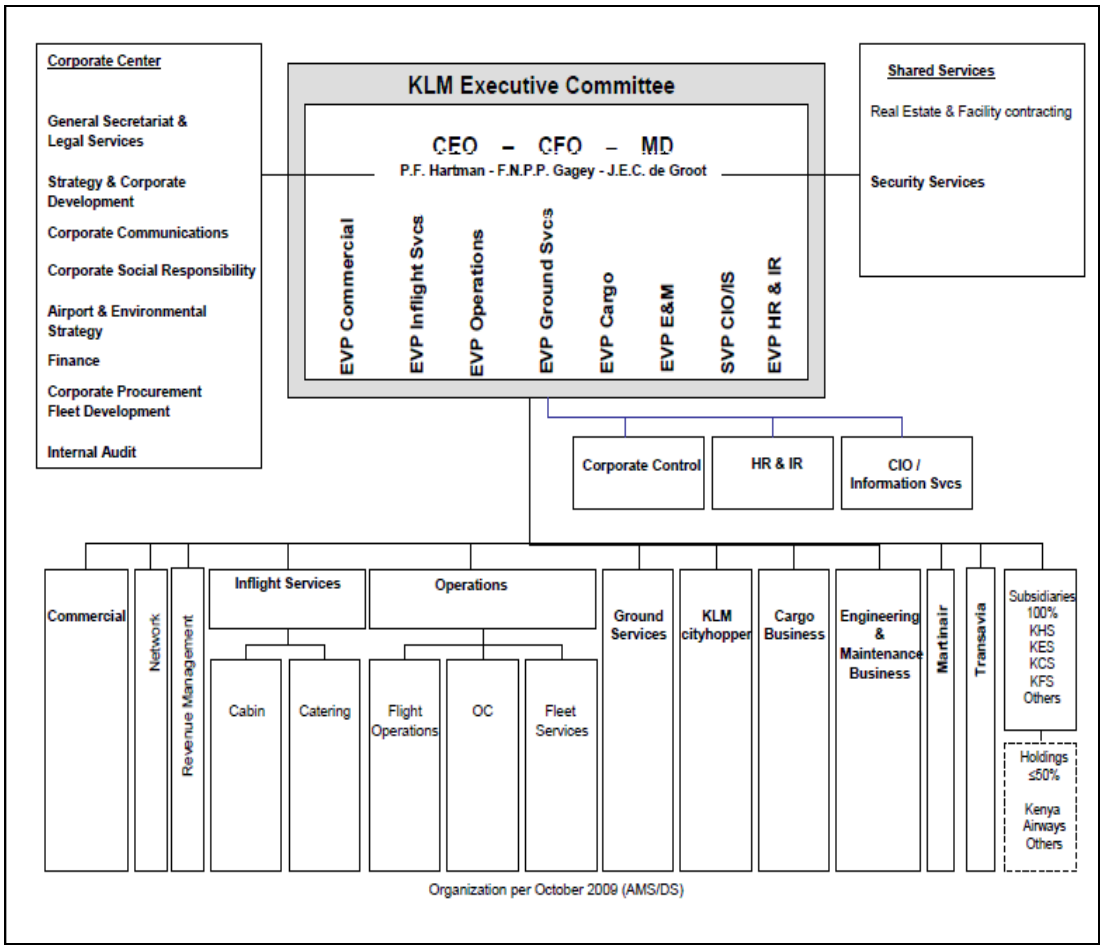
Foundation of KLM, Royal Dutch Airlines and Air France

KLM, Royal Dutch Airlines was founded on October 7, 1919. Air France was founded on August 30, 1933, by a merger of Air Orient, Compagnie Générale Aéropostale, Société Générale de Transport Aérien (SGTA, the first French carrier, founded as Lignes Aériennes Farman in 1919), Air Union and CIDNA (Compagnie Internationale de Navigation).

Partners and the Sky Team alliance

Over the years, Air France-KLM has established cooperative relationships with numerous airlines. The network built up by the Air France-KLM Group and its partners spans the globe, providing access to more than 750 destinations in more than 150 countries on more than 6 continents. Clustering these networks and offering swift transfer options enable travellers to fly to practically any destination in the world, from any one of today's many major hubs.
In 2004, cooperation kicked off between KLM and Air France and KLM joined the global Sky Team alliance which unites other major carriers including Air France, Alitalia, Delta Airlines

KLM Organization Structure



Corporate Information Office / Information Services

KLM CIO/IS Mission Statement

Create business value by delivering reliable ICT-services to the business processes, and innovative ICT-solutions to enable and support business change.

- CIO/Information Services is a world class Information Services provider and will be able to deliver the best value to the company;
- The ICT cost-levels will be at a competitive industry level;
- The ICT architecture and infrastructure enables the growth ambitions of Air France-KLM.

CIO Office

The CIO Office is the staff office of the CIO that supports the Information Officer in governing ICT functions within Air France-KLM on a Strategical and Tactical level (not Operational). The work of the CIO Office focuses on the business (WHAT) and ICT (HOW): turning business and IT policy, ICT investment policy and price/performance of IT services.

3. Literature review

Introduction

A methodological review of past literature (theoretical research) is a crucial endeavor for any academic research work (Webster & Watson, 2002). The need to uncover what is already known in the body of knowledge prior to initiating any research study should not be underestimated (Hart, 1999). Some fields of study have chronically suffered from lack of proper literature review, which in turn has hindered theoretical and conceptual progress (Shaw, 1995a). Webster and Watson (2002) also criticized the Information Systems (IS) field for having very few theories and outlets for quality literature review. Moreover, they noted that the Information Systems field may greatly benefit from an effective methodological literature review in order to strengthen IS as a field of study (Webster & Watson, 2002). [1].

This chapter will review academic literature and publications to explain the following topics:

- Airline Operations
- Information Systems;
- Infrastructure components
- Managing risk areas
- Business Continuity Management
- Crisis Management
- Information Technology General Controls

3.1. Airline Operations

Each day, the airlines achieve the remarkable by safely moving nearly five million people more than 40 million (data from 2003) air miles around the world. Often, however, they fail to deliver on the ordinary. Once the aircraft land, all too many of them taxi to a runway and wait - perhaps for a ground crew to arrive and open a door or for the end of the traffic caused by another plane's maintenance delay. Even standout, low-cost performers lose bags, keep valuable employees idle, depart late, and have billions of dollars in chronically underutilized aircraft and other hugely expensive assets [2].

These extremes coexist because airlines have historically focused on safety, aircraft technology, speed, geographic reach, and in-flight service attributes; on distinctive regulatory constraints and labor issues; and on the unpredictability imposed by weather and rapidly shifting demand. At the same time, issues such as route structures, excess capacity, pricing, and yield management compete with operations for the airlines' attention [2].

Airlines make money only when they match supply and demand [3]. Their yield management objective is to sell the right seat to the right passenger at the right price. Effective planning

and marketing is a continuous process to realize those objectives. To manage that on an effective way there should be continuity in enterprise planning, product planning, tactics and airline operations. [3]

Airline Operational Control centre (AOCC)

The main role of the AOCC is to monitor the conformance of fight activity according to the previously defined schedule. The occurrence of some unexpected events might prevent operations to take place as planned, such as aircraft malfunction, crew delays, and crew member absence [4]. The AOCC is a human decision system composed by teams of experts specialized in solving the described problems. Teams act under the supervision of an operational control manager and their goal is to restore airline operations in the minimum frame and at a minimum cost. According to Castro [5], there are three main AOCC organizations:

- Decision Centre: the aircraft controllers share the same physical space. The other roles or support functions (crew control, maintenance service, etc.) are in a different physical space. In this type of Collective Organization all roles need to cooperate to achieve the common goal.
- Integrated Centre: all roles share the same physical space and are hierarchically dependent of a supervisor. Figure 1 shows the AOCC organization.
- Hub Control Centre: most of the roles are physically separated at the airports where the airline companies operate a hub in this case, if the aircraft controller role stays physically outside the hub we have an organization called Decision Centre with a hub. If both the aircraft controller and crew controller roles are physically outside the hub we have an organization called Integrated Centre with a hub. The main advantage of this kind of organization is to have the roles that are related with airport operations (customer service, catering, cleaning, passengers transfer, etc.) physically closer to the operation.

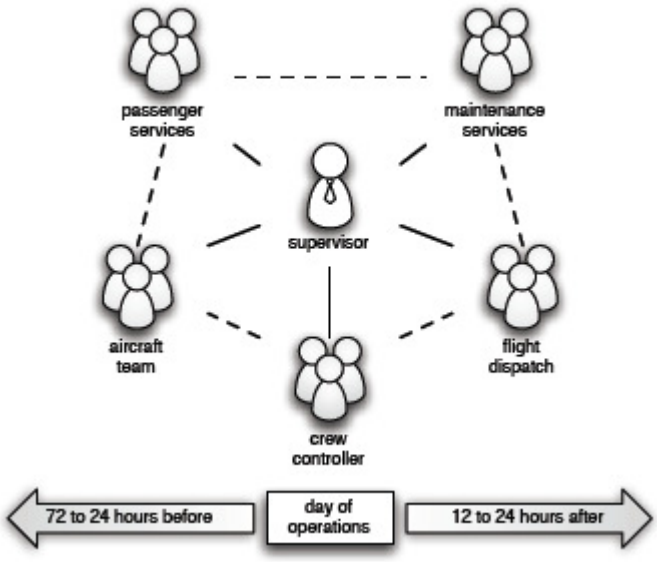


Figure 1: Integrated airline operational control centre (adapted from [6])

As mentioned, figure 1 shows the traditional Integrated Operational Control Centre. As previously stated, the AOCC is composed by groups of workers, each one with its own responsibilities. They must report their activity to a Supervisor, translating a two-level hierarchical system. Figure 1 also represents the activity time-window of the AOCC, it starts 72 to 24 hours before the day of operations and ends 12 to 24 hours after. The roles more common in an AOCC are, according to Kohl [7] and Castro [5]:

- Flight Dispatch: prepares the flight plans and requests new flight slots to the Air Traffic Control (ATC) entities (FAA in North America and EUROCONTROL in Europe, for example).
- Aircraft Control: manages the resource aircraft. It is the central coordination role in the operational control.
- Crew Control: manages the resource crew. Monitors the crew check-in and checkout, updates and changes the crew roster according to the arisen disruptions.
- Maintenance Services: responsible for the unplanned services and for the short-term maintenance scheduling. Changes on aircraft rotations may impact the short-term maintenance (maintenance cannot be done at all stations).
- Passenger Services: decisions taken on the AOCC will have an impact on passengers. The responsibility of this role is to consider and minimize the impact of the decisions on passengers. Typical this role is performed on the airports and for bigger companies is part of the HCC organization.

Disruption Management

The first overview of the state-of-the-practice in operations control centers in the aftermath of irregular operations was provided by Clarke [8]. In his study, besides an extensive review over the subject, he proposes a decision framework that addresses how airlines can re-assign aircraft to scheduled flights after a disruptive situation. Currently, the most thoroughly analysis of the discipline is presented by Kohl et al. [9] where their conclusions are supported by the DESCARTES project, a large-scale airline disruption management research and development study supported by the European Union.

The volume of electronic data for an efficient airline operation is simply too great to be adequately analyzed by simply reading reports or reviewing operations statistics. Even in a small airline, this becomes totally impractical without the support of analytical tools.
The use of Information Systems to manage the airline operation is therefore indispensable. Depending on the size of the airline company, it requires a system with a range of capabilities and outputs to manage their data, In general they require:

a) A system with the capability of transforming large amounts of data into useful information that supports decision making;
b) A system that will reduce workload for managers and personnel;
c) An automated system that is customizable to the companies own culture; and
d) A system that can operate at relatively low cost

3.2. Information Systems and Information Technology

Information Systems applies Information Technologies to accomplish the assimilation, processing, storage, and dissemination of information.

The ever expanding data and information flow across the world would not be manageable without the use of Information Technology and Information Systems.

The distinction between information systems and information technology

On the website of Eindhoven University of Technology we can read that there is a clearly distinction between Information systems and Information Technology. They define these terms as follows:

- An Information Technology transmits, processes, or stores information.
- An Information System is an integrated and cooperating set of software directed information technologies supporting individual, group, organizational, or societal goals.

In other words, Information Systems applies Information Technologies to accomplish the assimilation, processing, storage, and dissemination of information. Thus, PDA's, cellular phones, music players, and digital cameras as information systems use multiple information technologies to create personal information systems. Similarly other information technologies, such as database, networks, and programming languages, are used to created organizational systems.

Modern business organizations become more and more dependent on their information systems to deal with the complexity and changeability of the context (markets) in which they operate and consequently their internal organization structures. Up-to-date, complete and accurate information has become a necessity to survive in an increasingly competitive world. Developments like dynamic cooperation networks, mass customization of products and services, and end-to-end process control require automated means to control operational business processes, for the simple reason that humans cannot oversee the entire operation in an efficient and effective way anymore. Consequently, business requirements to information systems increase at a dazzling pace. (Source: http://is.tm.tue.nl/)

On the other hand, the rapid developments in information technology give way to application types that simply were not feasible just a few years ago. These developments range from basic computing technology via communication technology and a broad spectrum of data and process management technology to complete frameworks for enterprise information systems and e-business systems. (Source: http://is.tm.tue.nl/)

Information Systems defined by UK Academy for Information Systems

UKIAS defines that Information systems are the means by which people and organisations, utilising technologies, gather, process, store, sue and disseminate information. [ukais]

Information System defined by Answer.com

Answer.com defines Information System as a combination of people, hardware, software, communication devices, network and data resources that processes (can be storing, retrieving, transforming information) data and information for a specific purpose. The operation theory is just similar to any other system, which needs inputs from user (key in instructions and commands, typing, scanning). The inputted data then will be processed (calculating, reporting) using technology devices such as computers, and produce output (printing reports, displaying results) that will be sent to another user or other system via a network and a feedback method that controls the operation. (Source: http://Answer.com).

3.3. Information Technology Infrastructure Components

Definition of Information Technology Infrastructure Components

An Information Technology (IT) Infrastructure is a collection of technologies, people, and processes that facilitates large-scale connectivity and effective interoperations of an organization's IT applications. The technology component of an effective IT infrastructure includes technologies for effective data storage and retrieval (e.g., Storage Area Networks), systems integration (e.g., middleware), connectivity (e.g., networking components), and security technologies (e.g., firewalls). The people component includes infrastructure architects and other employees charged with infrastructure design and support. The process component includes processes for architecture standardization and infrastructure change reviews. [10]

Information Infrastructure

The information infrastructure of an organization is defined as all the IT resources (i.e., infrastructure components) used in the information processes and controlled by IS management. It includes both common and specific IT resources and consists of the following three layers of (sub) infrastructures:

The application infrastructure - The application infrastructure includes all the applications. The development infrastructure or systems development environment (i.e., prescribed development methods, techniques, and tools) are often also included in this infrastructure.

The data infrastructure - The data infrastructure comprises the (multimedia) data and knowledge bases, facilities for data protection, integrity, and consistency, and the organization's data model. The data base management systems belong to the technical infrastructure.

The technical infrastructure - The technical infrastructure consists of the hardware and system software of:

- Computer systems (i.e., mainframes, midrange computers, and PCs). Client-server architecture, a subdivision is made into client (i.e., workstation) components and server components.
- Communications networks or external and internal WANs and LANs. [11]

3.4. Information Technology Risk Areas

ERPANET [12], describes risk as a combination of the probability of an event (usually adverse) and the nature and severity of the event. The main aim in understanding and communicating risk is to identify and impose priorities, and take appropriate actions to minimize risks. Three stages to consider in assessing and managing risk:

- Risk identification **-** resources at risk, type of threats, value of resources, organizational vulnerabilities. Identifying risk scenarios should begin with an understanding of how the system should work.
- Risk analysis **-** levels of acceptable risk, likelihood of risk materializing, direct and indirect costs, consequences of risk materializing, safeguards in place.
- Risk management **-** mitigation options and responses, risk prioritization, management strategies, risk reduction, tradeoffs [12]

According to Steve Elky [13], risk is the potential harm that may arise from some current process or from some future event. Risk is present in every aspect of our lives and many different disciplines focus on risk as it applies to them. From the IT security perspective, risk management is the process of understanding and responding to factors that may lead to a failure in the confidentiality, integrity or availability of an information system. IT security risk is the harm to a process or the related information resulting from some purposeful or accidental event that negatively impacts the process or the related information. *Risk* is a function of the likelihood of a given threat**-**source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. The principle reason for managing risk in an organization is to protect the mission and assets of the organization. Therefore, risk management must be a management function rather than a technical function. It is vital to manage risks to systems. Understanding risk, and in particular, understanding the specific risks to a system allow the system owner to protect the information system commensurate with its value to the organization. Organizations have limited resources and risk can never be reduced to zero. Understanding risk, especially the magnitude of the risk, allows organizations to prioritize scarce resources. [13]

Risk and Information Technology

According to Securance Consulting [14] risk is the potential for loss to an enterprise due to error, fraud, inefficiency, failure to comply with statutory requirements, or actions which bring disrepute to the entity. Risk is a synonym for all the adverse outcomes that the organization wishes to avoid. Risk is a function of the probability that such consequences will occur, their magnitude, and their imminence. [14]

Technology Risk Components:

- Integrity Risk – risks associated with the authorization, completeness and accuracy of transactions as they are entered into, processed by, summarized and reported on by the various application systems deployed by an organization. [14]

- Relevance risk – the usability and timelines of information that is either crested or summarized by an application system is the risk associated with not getting the right data/information to the right person/process/system at the right time to allow the right action to be taken.
- Access Risk – risk associated with inappropriate access to systems, data or information. It encompasses the risks of improper segregation of duties, risks associated with the integrity of data and databases, and risks associated with information confidentiality. [14]

Infrastructure Risk:

- Organization Planning – the definition of how IT will impact the business are clearly defined and articulated. It is important to have adequate executive level support and buy-in to this direction and an adequate organizational (people and process) plan to ensure that IT efforts will be successful. [14]
- Application Deployment – ensuring that application systems meet both business and user needs. This process ensures that any change to a system whether purchased or developed internally it follows a defined process that ensures that critical process/control points are consistently followed. [14]
- Logical Security – ensuring that the organization adequately addresses access risk by establishing, maintaining and monitoring a comprehensive system of internal security that meets management's policies with respect to the integrity and confidentiality of the data and information within the organization. [14]
- Computer Operations – ensuring that information systems and related network environments are operated in a secured and protected environment as intended by management. Additionally, ensuring that information processing responsibilities performed by operations personnel are defined, measured and monitored. [14]
- Disaster Recovery – ensuring that adequate planning has been performed to ensure that information technologies will be available to users when they need them. [14]

Definition of vulnerabilities in measuring risks to infrastructures

According to Haimes [15] it is important to define the following terms, which broadly apply to risk analysis:

- Vulnerability is the manifestation of the inherent states of the system (e.g., physical, technical, organizational, cultural) that can be exploited to adversely affect (cause harm or damage to) that system;
- Intent is the desire or motivation to attack a target and cause adverse effects.
- Capability is the ability and capacity to attack a target and cause adverse effects.
- Threat is the intent and capability to adversely affect (cause harm or damage to) the system by adversely changing its states.
- Risk is the result of a threat with adverse effects to a vulnerable system.

Green, J [16], [17] describes the following risk sources for Information Systems:

- Water,
- Fire
- Service Failure
- Mechanical breakdown or software failure
- Accidental or deliberate destruction of property/assets
- Environmental/facility wide damage
- Personnel problem

Tier rating on data center

There is an industry standard way of describing the availability of the data center facility. Availability, in this case, is referring to the degree to which the facility can support constant uninterrupted operation of the contained data processing systems. The tier classification model provides an objective basis for comparing or describing the functionality, capacity, and cost of a data center's facility architecture. In particular, the tier classification model is focused on the Availability of the facility itself, and is driven by the infrastructure to power and cool the data processing environment. [18]

The American National Standards Institute (ANSI) and the Telecommunications Industry Association (TIA) are examples of organizations that formulate standards for the industry to follow. The TIA developed a specification entitled TIA-942: Telecommunications Infrastructure Standard for Data Centers. The TIA relied upon The Uptime Institute to develop this part of the standard. [18]

Businesses appropriately supported by a Tier-3 Data Center are companies that serve both internal and external customers 24×7 and whose IT resources support automation of business processes, so that the customer impact of short shutdowns due to facility outage are manageable. Tier-3 is appropriate for businesses that span multiple time zones and corresponding geographic diversity of employees and customers. Businesses which have significant financial exposure due to customer quality-of-service issues are well supported by Tier-3 facilities. [18]

Because of the concurrently maintainable characteristic of Tier-3 facilities, no annual shutdowns for routine maintenance are required. The Institute has concluded that Tier-3 Data Centers have unplanned events totalling only 1.6 hours per year. Tier-3 sites then, deliver 99.98% availability. [18]

Overview of an Information Technology System

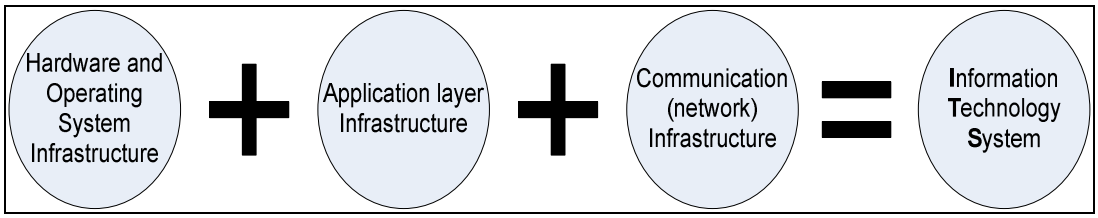
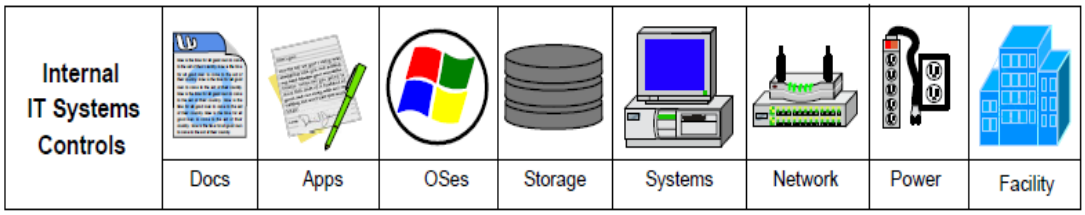
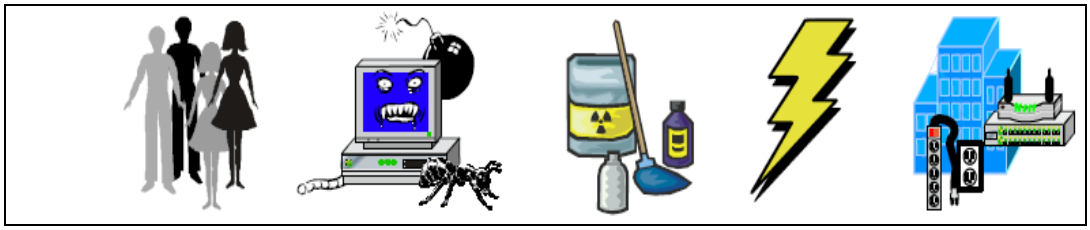


Figure 2: Own Source: Building blocks for an Information Technology System

According to Dorian J. Cougias [19] and the building blocks for an Information Technology System (figure above) it means that we need to protect the following Information Technology Infrastructure components (assets) against threats.



The threats to those IT assets



From the pictures above we can conclude that we need to establish a sound practice of guidelines and controls to protect our IT assets against risks before the threats becoming reality. Summarized it means: **Guidelines + Control Objectives = Protection of Information Assets against Risks**

3.5. Business Continuity Management

Managing an airline operation without the usage of complex Information Technology Systems is impossible. But with complex Information Technology Systems the risks of unplanned disruption arises. The concept of Business Continuity Management that can be a help to implement processes to eliminate, mitigate or reduce the risk of unplanned disruptions in the daily airline operations. Standards for Business Continuity Management that are used around are described in this chapter. The list is not assumed to be complete.

Business Continuity Management Standards

The British Standards Institution (BSI) describes a standard as an agreed, repeatable way of doing something. It is a published document that contains a technical specification or other precise criteria designed to be used consistently as a rule, guideline, or definition.

Werner Verlinden, CIRM, FBCI [20], describes in his article “A short tour of Business Continuity Management Standards” that prior to a standard being elaborated there are usually a series of documents around. Amongst these we can find professional practices (e.g. DRII PP), good practice guidelines (e.g. BCI GPG), guides, principles, circulars, regulatory requirements and others. ISO 22301 - addresses ‘Societal security - Preparedness and Continuity Management Systems – requirements’, an auditable BCM standard.

Global Business Continuity Management Standards

North America: In Canada, the principal business continuity standard is Z1600, which was adopted in 2008 by the Canadian Standards Association. It is based on the U.S. National Fire Prevention Association (NFPA) 1600 standard, and has been adapted to support Canadian interests. The U.S. NIST 800-34 Contingency Planning Guide for Information Technology Systems identifies seven critical steps in developing contingency plans. ITGI (IT Governance Institute) also a U.S. initiative describes in CobiT 4.1 (Control Objectives for Information and related Technology), domain DS4 (Deliver and Support – Ensure Continuous Service) the controls, risks and test approach to audit BCM. [21]

United Kingdom and Europe: In the area of IT disaster recovery, the U.K. has BS 25777. Information Technology Infrastructure (ITIL) also an U.K. initiative that described the aspects of continuity management in IT Service Continuity Management. The British Standards Institution (BSI) is very active in standards development, not only in the U.K., but also worldwide. As such, BS 25999 is widely used as a baseline BC standard by many member countries of the European Union. [21]

International: The International Organization for Standardization (ISO) has been actively working on a global standard for business continuity for several years. There are many opinions as to when the new standard will be approved and released to the global business community. Two documents in particular are worth mentioning: the ISO’s Publicly Available Specification (PAS) 22399, Guideline for Incident Preparedness and Operational Continuity Management and the ISO/IECD (International Electro technical Commission) 24762, Information and Communications Technology Disaster Recovery. The feeling is that these two documents, plus input from many others, will be among the primary foundation documents for the new global standard. [21]

Business Continuity Management - Introduction

Business Continuity Management (BCM) is not just about disaster recovery, crisis management, and risk management control or technology recovery. It is not just a professional specialist discipline but a business owned and driven issue that unifies a broad spectrum of business and management disciplines. BCM provides the strategic and operational framework to both review and where appropriate redesign the way an organization provides its products and services whilst its resilience to disruption, interruption

or loss. BCM has also long been recognised as good business practice and is therefore an integral part of corporate governance. Within this setting BCM takes on a strategic dimension and should not only be seen in a narrow reactive operational context. [22]

Business Continuity Management - Definition

Business Continuity Management is a holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats if realized might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities. [22]

Business Continuity Management - Purpose

Whilst the BCM good practice guidelines do not themselves provide a BCM competency and capability they do provide a generic framework and standardised approach to enable and inform their development. In particular the guidelines are designed to provide assistance in understanding and applying the BCM principles. The guidelines are divided into six sections that are each based upon a stage of the BCM life-cycle and process. Each organisation needs to assess how to apply the good practice contained within the guidelines to their own organisation. With this context they must ensure that their BCM competence and capability meets the nature, sale and complexity of their business, and reflects their individual culture and operating environment. [22]

Business Continuity Management - Scope and audience

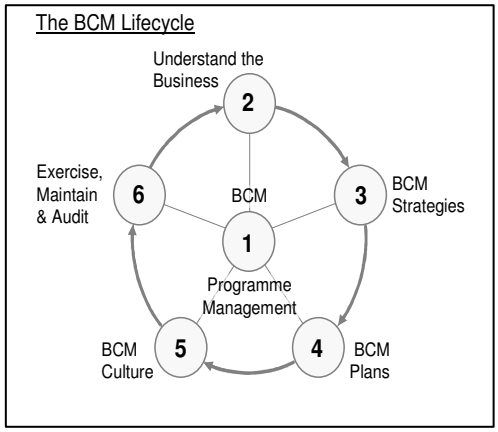
The BCM good practice guidelines establish the process, principles and terminology of Business Continuity Management. They describe the activities and outcomes involved and provide recommendations for good practice. They also describe and provide evaluation criteria and current state assessment (benchmark) workbook. The guidelines are applicable to all organisations, regardless of size or industry sector, and are intended for use by managers, BCM practitioners, auditors and regulators. [22]

The Business Continuity Management “umbrella”

PAS 56, Business Continuity Management is the unifying process which brings together a number of key management disciplines. This concept is shown in the ‘umbrella model’. The management of Risk, Disaster Recovery, Facilities, Supply Chain, Quality, Health and Safety, Knowledge, Emergency, Security, Crisis Communications and Public Relations all sit together under the Business Continuity Management umbrella. It does not imply that BCM is the senior discipline but it is a means of co-ordinating these disparate activities. [23]

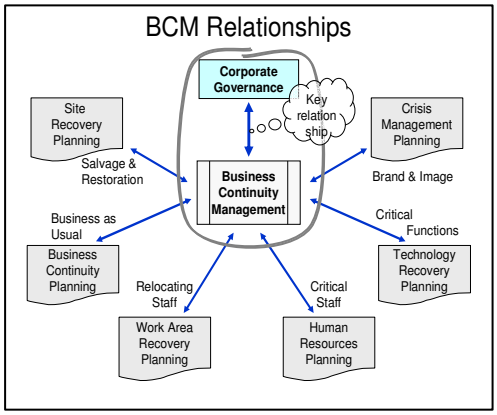
The Business Continuity Management Lifecycle Model

The BCM Lifecycle model suggests the establishment of a BCM programme to manage the ongoing activities as the starting point.
PAS 56 provides some guidance notes about the objectives and deliverable for each of the 6 phases of the BCM life cycle. It also includes a set of benchmarking questions with the implication that a positive answer to each of the questions represents good practice. [23]



BCM Relationships

Business Continuity Management requires planning across many facets of an organisation and therefore depends upon the adoption of a holistic approach. The accompanying diagram shows how the various aspects of BCM relate to each other. It also demonstrates the close link that exists between Corporate Governance and Business Continuity Management. [23]



BCM Strategies

There are 3 levels of strategic planning, which more or less correspond to the Gold, Silver, and Bronze command and control model used by the emergency services:

1. Organizational level BCM strategy is about defining the overall approach to protection, resilience and recovery across the enterprise.
2. Operational level BCM strategy is about organizing the recovery of the key operational processes and controlling the effects of an emergency
3. Resource Recovery BCM strategy is about preparing, recovering and restoring facilities and resources for use in an emergency

The planning at these levels should consider the adoption of one or more of the following basic recovery strategies:

1. Functional Backup which involves relocation of the Mission Critical Activities (MCAs) to a dormant site in an emergency
2. Split Operations which involves redirection of the workload in an emergency
3. Alternate Site which involves relocation to an active site in an emergency
4. Contingency Arrangements which involve the adoption or development of alternate methods of operation for mission critical activities in an emergency [23]

BCM Strategic Options

The choices to be considered when developing the strategy include:

- **Do Nothing**, which is seen as a risky non-strategy
- **Transfer the Operation**, where it is possible and cost effective
- **Terminate the Operation**, which means accepting the loss of a service during an emergency
- **Change the Operation**, which means using alternate methods of delivery or operating as a temporary measure
- **Insurance**, which means transferring the costs in return for some of the profits, although this approach does nothing constructive about the recovery process
- **Loss Mitigation**, which means absorbing the costs of an interruption within the profits although this approach has the same drawbacks as insurance
- **Business Continuity Management**, which means developing pro-active solutions to prevent and resolve the issues [23]

Key Elements for the 6 stages of BCM

PAS 56 [23] describes the objectives and outcomes for the 6 stages of BCM. Some of these are quite specific; others are subject to interpretation, allowing for diversities of scale, industry, areas and styles of operation.

Stage 1 - Programme Management

Stage 2 - Understanding the Business

Stage 3 - BCM Strategies

Stage 4 - BCM Planning

Stage 5 - Embedding a BCM Culture

Stage 6 - Exercise, Maintenance & Audit

Public Available Specification No. 56 - PAS 56

On 24 March 2003 the British Standards Institute (BSI) issued Publicly Available Specification No. 56. PAS 56 is the result of work conducted by the Business Continuity Institute (BCI) and several other organizations. It defines and establishes a framework for implementing Business Continuity Management (BCM). The PAS 56 Audit Workbook has a menu of questions and a good practice compliance analysis tool. The workbook has six stages, adapted from the Business Continuity management Life Cycle model, each with a spreadsheet-based scorecard for capturing results of each benchmark analysis. **[24]**

3.6. Contingency Planning

Introduction

Information Technology (IT) and automated information systems are vital elements in most business processes. Because they are so essential to an organization's success, it is crucial that the services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster. NIST Special Publication (SP) 800-34, Contingency Planning Guide for Information Technology Systems, provides instructions, recommendations, and considerations for government IT contingency planning.

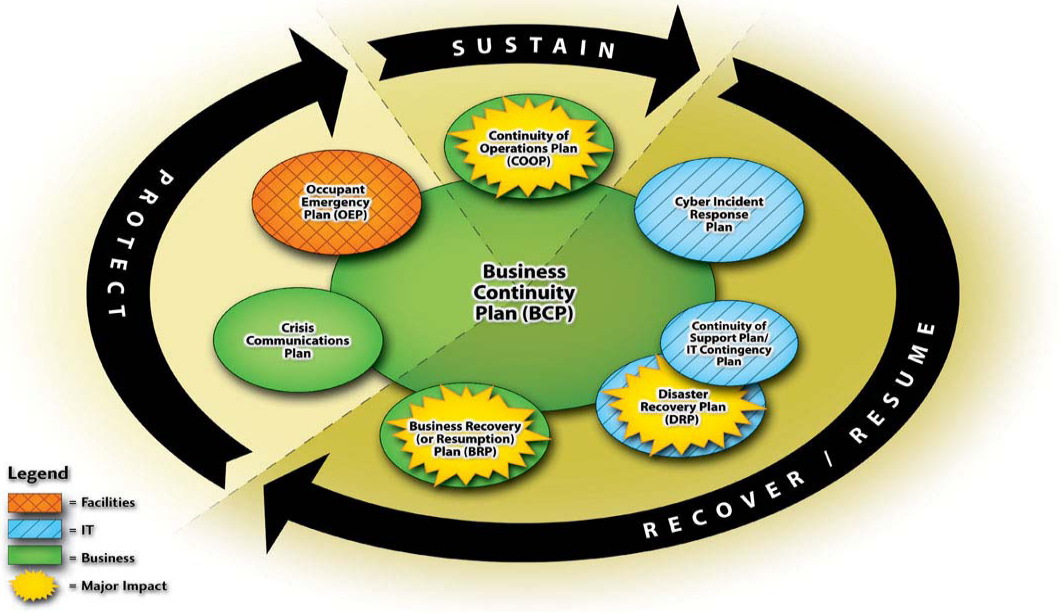


Figure 3: Interrelationships of Emergency Preparedness Plans [25].

Business Continuity Plan (BCP) - BCP focuses on sustaining an organization's business functions during and after a disruption. IT systems are considered in the BCP in terms of their support to the business processes. [25]

IT Contingency Plan - An IT contingency plan should be developed for each major application and general support system; multiple contingency plans may be maintained within the organization's BCP. [25]

Crisis Communications Plan - A crisis communications plan is often developed by the organization responsible for public outreach. The crisis communication plan procedures should be coordinated with all other plans to ensure that only approved statements are released to the public. [25]

Disaster Recovery Plan (DRP) - The DRP applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. Frequently, DRP refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency. The DRP scope may overlap that of an IT contingency plan; however, the DRP is narrower in scope and does not address minor disruptions that do not require relocation. Dependent on the organization's needs, several Disaster Recovery Plans may be appended to the Business Continuity Plan. [25]

Scope of the Contingency Plan

It presents contingency planning principles for the following common IT processing systems:

- Desktop computers and portable systems (laptop and handheld computers)
- Servers
- Websites
- Local area networks (LANs)
- Wide area networks (WANs)
- Distributed systems
- Mainframe systems.

IT Contingency Planning Process

To develop and maintain an effective IT contingency plan, organizations should use the following approach:

1. Develop the contingency planning policy statement
2. Conduct the business impact analysis (BIA)
3. Identify preventive controls
4. Develop recovery strategies
5. Develop an IT contingency plan
6. Plan testing, training, and exercises
7. Plan maintenance

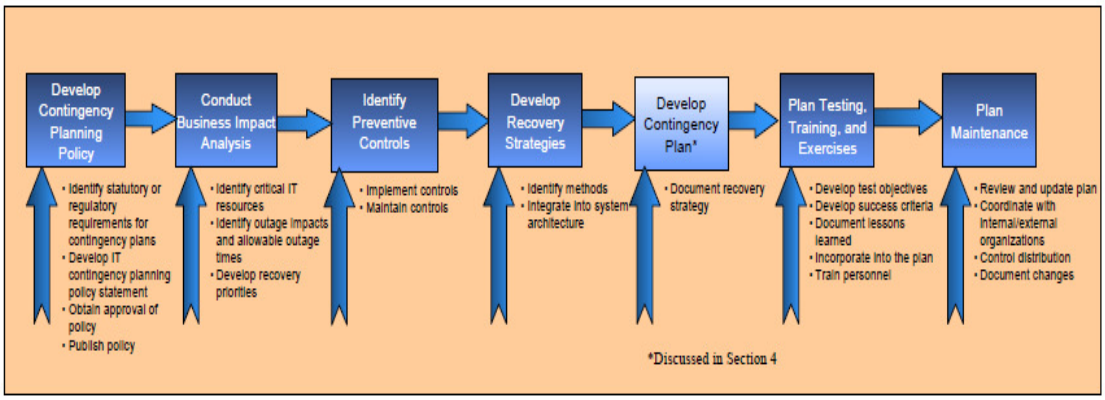


Figure 4: Source NIST SP 800-34: Figure 3-1 Contingency Planning Process

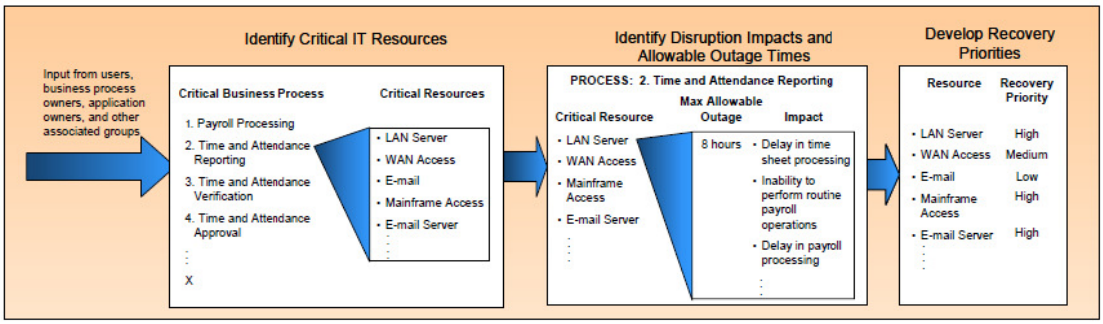


Figure 5: Source NIST SP 800-34: Figure 3-2 Business Impact Analysis Process

3.7 The Changing face of Continuity Planning

Carl B. Jackson, CISSP, CBCP [27] notes that the continuity planning profession continues to evolve from the time when disaster recovery planning (DRP) for mainframe data centers was the primary objective. The last ten year he have seen the industry move from a focus strictly on computer operations and communications recovery planning to one where business functionality and processes are considered the start and end points for proper enterprise wide availability.[26]

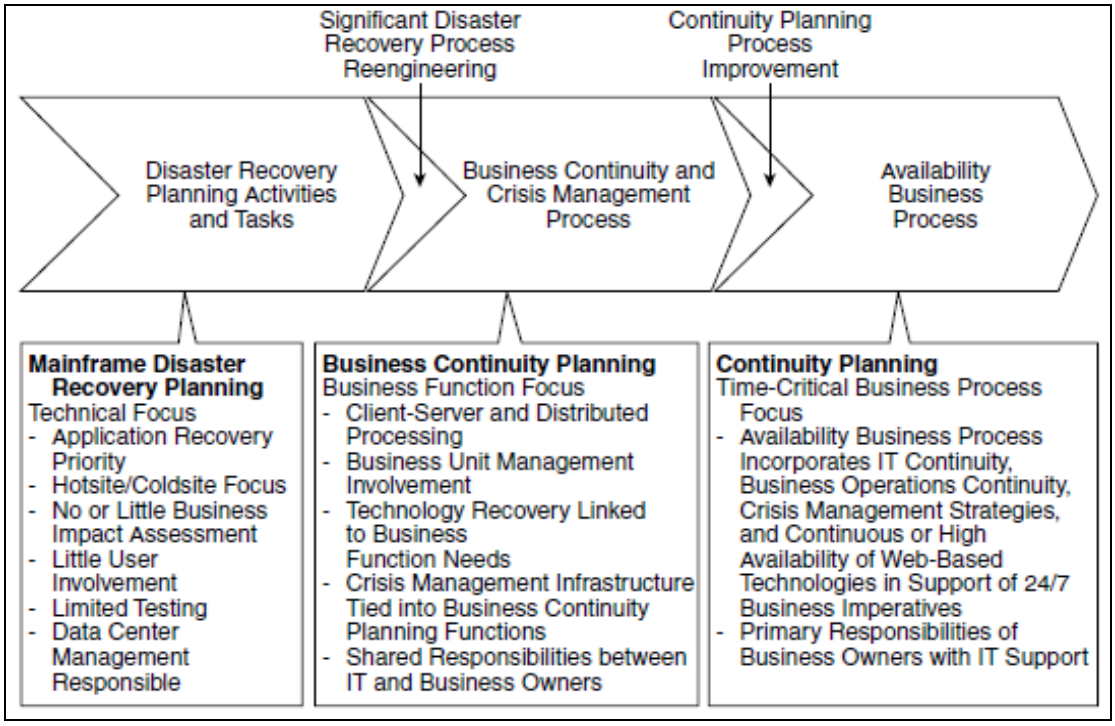


Figure 6: Evolution of Industry Thinking

Figure 6 depicts the evolution of industry thinking relative to the passage from technical recovery to business process recovery. As organizations move operations onto the Web, they must ensure the reliability and availability of Web-based processes and technologies. This includes the assurance that trading partners, vendors, customers, and employees have the ability to access critical B2B and B2C resources. [26]

Continuous availability

The terminology currently being used to describe this Internet-resource-availability focal point is *continuous* or *high availability*. Continuous availability (CA) is a building-block approach to constructing resilient and robust technological infrastructures that support high availability requirements. *Continuous availability* - Acknowledges that the recovery time objective (RTO) for recovery of infrastructure support resources in a 24/7 environment has shrunk to zero time. That is to say that the organization cannot afford to lose operational capabilities for even a very short period of time. [26]. Recovery Point Objective (RPO) is the maximum desired time period prior to a failure or disaster during which changes to data may be lost as a consequence of recovery. Zero is a valid value and is equivalent to a "zero data loss" requirement. Each of these as stated are based on the business model and permissible staleness of the data and can be based on what the customers believe is relevant. (i.e., the recovery point objective of a ticket booking system may be as few as second and the RTO may be based on minutes, not hours. In this case you would have redundant systems with failover but it is still important to include this within the BIA as the recovery priority. [**24**]

Prioritizing the recovery

According to CNT [27] all too often, backup/recovery solutions are devised in a vacuum without much regard for the actual needs of the business. After each business requirement is classified as to the relative impact to the business in the event of an outage, the recovery objectives for each class must be quantified. This needs to be done in terms of recovery time objectives (RTO) and recovery point objectives (RPO). The RTO is the maximum amount of time a business function can be unavailable before it severely impacts the corporation. The RPO is the specific point-in-time the data needs to be restored to in order to affect a successful recovery. [27]

CNT believes that each enterprise should try to categorize their business functions into several Classes of Recovery. Many enterprises use the following general approach:

- **Class 0:** No reason to recover during a disaster recovery
- **Class 1:** Non-vital business functions
- **Class 2:** Business functions that are vital to the company, but are not the most important
- **Class 3:** Critical, “must have” business functions*

* One could also include a Class 4 for business functions which require solutions that are fully fault-tolerant at the hardware level with transaction replication. However, these scenarios are rarely used and are really only practical in mainframe environments. [27]

Breaking down each component into recovery classes makes it easier to determine what the company’s needs are, what the recovery capabilities currently are, and what needs to be done to achieve the desired class of recovery should the current capabilities prove to be inadequate. These requirements can vary per company or industry. [27]

3.8 Crisis Management

According to Caroline Sapriel [28] companies are increasingly emphasizing proactive approaches to crisis communication. Corporations have long understood that they must be prepared to respond effectively to crisis. Communicators are uniquely positioned to integrate crisis communication into the overall business strategy. "Professional communicators understand the environment their organization operates in, which provides them with a keen understanding of emerging discrepancies that can evolve into a crisis," says Dr. Arjen Boin, director of the Leiden University Crisis Research Center in the Netherlands. Because they have their fingers on the public's pulse, Boin continues, "they also have a good grasp of the credit level remaining for an organization hit by crisis. This allows for a smoother transition back to a state of normalcy." [28]

To provide an integrated approach to crisis anticipation, prevention, mitigation and recovery, it is essential to assign ownership of the entire business contingency planning process (see "The Business Continuity Framework,") to a custodian, whether an individual senior staff member or a department, and embed it into corporate management planning. [28]

When the business contingency planning process is not assigned to a custodian in the organization, corporate communication departments are increasingly called on to take on its coordination. [28]

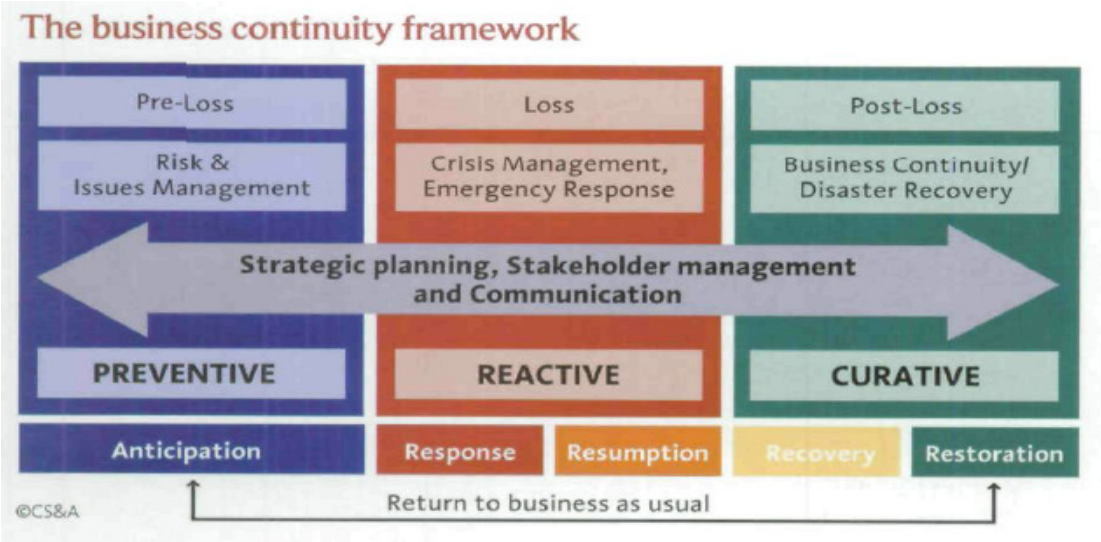


Figure 7: Source: CS&A – International Risk, Crisis & BCM – www.csa-crisis.com

In this integrated model, issues and risk management are loss-prevention functions; emergency response and crisis management planning focus on being prepared to handle adversity, minimize impact and facilitate the management process during chaos; and business continuity planning concentrates on post-loss recovery. Strategic communication planning runs through the full process and provides the glue that facilitates more effective results. [28]

3.9 Information Technology General Controls (ITGCs)

According to Carolyn Strand Norman et al [29], ITGC is fundamental for internal controls. It provides an overall foundation for reliance on any information produced by a system. Since the relation between ITGCs and the information produced by an organization's various application programs is indirect, understanding how ITGCs interact and affect an auditor's risk assessment is often challenging. Assessing the overall ITGC risk within the five ITGC areas of an organization's information systems identifies specific strengths and weaknesses. It provides an organization's overall level of risk within the context of an integrated audit. [29]

IT Management

IT management's key concepts include Information Technology's position within the organization, whether IT goals are aligned with the organization's strategic goals, the use of an IT steering committee, and whether the IT department's structure promotes proper segregation of duties to protect the organization's assets. [29]

Systems Development

The key concepts within systems development include the existence of a new systems implementation methodology, project management, pre- and post-implementation reviews, quality control, adequate testing, and demonstrated compliance with the selected implementation methodology. [29]

Data Security

The critical concepts within data security include adherence to an established information security policy, access approval on a need-to-know basis, periodic rotation or change of access controls, monitoring, exception reporting, and incident response. On the physical side, data security includes physical access and environmental controls over the data center. On the logical side, data security includes policies related to password configuration, change, and history restrictions. Logical security also includes prompt review, modification, or removal of access due to personnel transfers, promotions, and terminations. [29]

Change Management

Change Management's key concepts include documented change procedures, user authorization and approval, separation of duties in implementing changes, management review, quality control, and adequate testing. [29]

Business Continuity Planning

Key concepts of BCP are management's expectations regarding a timely recovery of processing capabilities, the existence of a written plan, the currency of the plan, offsite storage of both the plan and data files, and testing of the plan.

4. Case Study: Description

4.1. Introduction and scope of the Case Study

The aim of the case study is to answer the main-, and sub questions of the Master thesis. The case study verifies whether a Business Continuity Management Process is implemented within Air France-KLM based on a Risk Assessment or Business Impact Assessment and whether an International adopted "Good Practice" for Business Continuity Management such as the PAS 56 was used to do so.

Whilst the Air France-KLM group consist of two airlines and three principal businesses: passenger transportation, cargo transportation and aeronautics and overhaul services, due to limited time the case study focuses only on Passenger Operations and Engineering & Maintenance. The reason that these two principal businesses were selected is that it represents more than 85% of the Air France-KLM revenues. The verification of the implementation of a "Good Practice" has been done by conducting interviews and collecting information about the standing management processes that assures continuous availability of business processes for the daily airline operations. The information collected both from Passenger Operations and Engineering & Maintenance is presented in chapter 6 as an integrated major findings.

The literature review describes that the design and existence of implemented IT Service Management (ITSM) processes is a prerequisite for Business Continuity Management. The following chapter verifies the design and existence of implemented IT Infrastructure management processes in order to determine whether the IT organization is able to deliver IT services on a continual basis and within the agreed Service Levels in case of a disaster.

4.2. IT Service Management

The design, existence and implemented IT Service Management process directly or indirectly mitigate the risk of IT Service disruption and supports Business Continuity Management.

Policies and procedures

Policies and procedures are defined and implemented covering Air France-KLM common systems development, project permits and project management (Prince2). The procedures describe the mandatory documents to be filed for each project. Development has defined and implemented procedures covering functional and corrective application software maintenance by internal- and external service providers. The procedures describe the mandatory documents to be approved for each application software change. An Air France-KLM Information Security Manual (based on BS ISO /IEC 17799:2005 – Code of Practice for Information Security Management), that describes the Air France-KLM security policy.

Release Management

The objective of Release Management is to ensure that only authorized and correct versions of software are made available for operation. The Enterprise Architect verifies that the functional and security requirements including the application controls that support complete, accurate, authorised and valid transaction processing are specified, completed and approved by the Business Executive to ensure that these requirements are adequate and authorised. The Project Manager ensures that a Test and Acceptance Strategy (TAS) document is created before requesting a build permit. The TAS describes the user acceptance of the functional and security requirements, which include the application controls. Approval of the TAS by the Business Executive is mandatory. Granting of the Operate Permit for a significant change to the production IT infrastructure is conditional on the successful completion of the test strategy. Segregation of duties between application development/test and production activities is ensured by organisational design, i.e. by restricting application software deployment to designated and authorized staff, not involved in development work. Requests for application software changes (functional or corrective maintenance) have to be authorised by a representative of the user organisation (i.e., Functional Application Manager). The treatment proposal (including functional specifications) of an application software change must be approved by a representative of the user organisation (i.e., Functional Application Manager). Approval of User Acceptance Test (UAT) by a representative of the user organisation, (i.e., Functional Application Manager), is mandatory for application software changes before being implemented in production.

Third Party Management

Third Party IT Service suppliers are managed by Vendor & License Management to ensure provision of seamless, quality services. Although Vendor & License Management has the right to audit the Third Party about their capability to deliver IT Services as agreed in case of a disaster at their site, it is not always mandated to deliver test reports regarding their reliability of Business Continuity plans. IS-Development manages the Third Party suppliers of application packages. Before Air France-KLM representative signs a contract for the partial or complete outsourcing of relevant IT services, Corporate Information Security Office (CISO) verifies if the third party is properly certified/audited for the relevant controls and security aspects and whether this is appropriately specified in the contract terms. CISO reviews the certification (SAS70)/audit results of relevant third parties annually, including a check that these cover the appropriate scope. Third party performance is monitored by the Product Manager on the basis of a Service Level Report (SLR). Deviations from the agreed performance are discussed with the third party and the ICT Service Managers. For the third party suppliers of application maintenance, Tactical Vendor Managers monitor the performance of the third party and report upon in the Balanced Score Card of Development (explicitly for the most important airline operations relevant third parties).

Change Management

ITIL describes change as an action that results in a new status for one or more CI. A request for change (RFC) is the main input to the Change Management Process. The goal of the Change Management process is to ensure that standardized methods and procedures are applied to realize efficient and prompt handling of all changes in order to minimize the impact of change-related incidents on service quality, thereby improving the day-to-day operations. Change management uses 2 tools. For Office Automation (OA) Vulcain is used as a CMDB and workflow management tool. Non Office Automation (Non OA) uses JIMS. Requests for Change (RfC) are submitted to and verified by the Change officer Agency (OA) on site or the Process Management Team (PMT) (non OA). Non OA changes are registered in JIMS by the Change Initiator in accordance to the Service classification and change Complexity, Impact and Risk. Non standard OA changes are sent to the vendor for a proposal. Non-standard Non OA changes are assessed by a central Change Advisory Board (CAB) in which Component groups of Air France-KLM are represented. The Change initiator assumes responsibility for the completion time of all changes (non-OA) within the defined scope, including time spent by Third Parties. The Change initiator (non-OA) informs the applicant(s) of the completion of a change. Changes resulting from major incidents are registered as emergency (E-) changes in the change management tool, possibly after implementation.

Service Level Management

The goal for SLM is to maintain and improve IT Service quality, through a constant cycle of agreeing, monitoring and reporting upon IT Service achievements and instigation of actions to eradicate poor service – in line with business or cost justification. Service level management has an operational domain and a strategic or tactical domain. The operational domain consists of: i) incident management, ii) problem management, iii) change management and v) Configuration management. ITIL also knows release management, but KL has integrated parts from this operational process in change management. The tactical domain consists of financial management, capacity management, availability management, continuity management and security management. The scope of SLM is confided to all IT services delivered by CIO/IS to Air France-KLM business divisions. Service Level Management also encompasses vendor management. In the case of outsourcing, the service level agreement (SLA) is an essential part of managing relations with third parties. By monitoring the performance of a service the evaluation and management of the service (internally or externally) is made possible. For all the IT Services that are critical and sensitive for the business processes of Air France-KLM, a Service Reference Manual exist that describes the objectives of the IT Services including their Operational Product- and IT Services dependencies. It also gives an overview of IT Infrastructure components (data, applications, systems and networks).

The Business Agreement: 2010 - 2011 between IMO and Air France-KLM Information Services describes the IT services that are used by Passenger Operations and E&M. The IT Services that are part of the Disaster Recovery Plan are indicated with Twinned = (**Y**). For example, the next table shows part of the business agreement that describes the service name, service classification, if it is twinned, the service windows.

Service Name Passenger Operations	Classification	Twinned	Service Windows
INRA	Critical	Y	7 * 24
LIDO	Critical	Y	7 * 24

Service Name Engineering & Maintenance	Classification	Twinned	Service Windows
AUTHORIZATION	Critical	Y	7 * 24
MAINTENIX A330	Critical	Y	7 * 24

It is decided by the Senior Management of Passenger Operations and Engineering & Maintenance that new business processes and applications should be an integral part of the business planning process. Therefore risk-management considerations must be addressed in the business requirements phase of projects. For each project/product the criteria for availability must be filled in the requirement document. It must give answer to the following availability specifications depending on the classification of the service:

- 3 – **Critical** - Downtime cannot exceed 4 hours (impact > € 1M)
- 2 – **Sensitive** / **Significant** - Downtime may exceed 4 hours but is less than a maximum defined in the GOA – General Operating Agreement or specified in chapter 6.
- 1 – **Normal** - Best effort (impact € < 10 K)

The requirement document is part of the common AFKL development method “Symphony” it aims at:

- defining all the business needs related to the new business processes to be defined
- identifying the constraints related to business activities, quality criteria and infrastructures that will support the information system
- prioritizing the requirements in order to help defining deliveries and their contents

Incident Management

ITIL defines an incident as a deviation for the (expected) standard operation of a system or a service. The goal of the Incident Management process is to restore normal service operation as quickly as possible and minimise the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. Incidents are managed with the Incident Management Tool Joint Air France-KLM Information Management System (JIMS). All incidents and questions are reported to the IT-Helpdesk (Single Point of Contact for users). If possible incidents are solved during the first contact with the IT-Helpdesk, using “First Check” instructions. All parties within the incident management process participate in the “Escalation Procedure”.

Major Incidents

Major incidents are those with a significant business impact affecting a Critical, Sensitive or Normal service. There are no quantitative rules for escalation of an incident to major status: the decision is based solely on the judgement of the DMI (Duty Manager ICT) in consultation with all parties involved. The aim of the Major Incident Procedure is to restore services as soon as possible in response to an incident escalation, thereby minimising the impact on business.

An incident can come in through four channels:

1. Duty Manager(s) (e.g. high impact on operation; flight operations; loss of income; image)
2. SoNo's (based on monitoring)
3. Help Desk (information from end users)
4. From a Component Group

Once an incident that has been registered by the System Operators and Network Operators (SoNo's) or the Help Desk has been diagnosed by JIMS (Joint Information Management System) as Severity 1 at a critical or sensitive service, the incident number must be passed on immediately to the DMI. The DMI (and perhaps the OSA) then decide whether the incident should be treated as a Major Incident based on the checklist here below.

In the event that the DM(X) telephones directly with the DMI, the DMI will use a checklist to determine whether the incident should be treated as a Major Incident.

A service is the specific combination of operational products required to provide the agreed ICT functionality in support of a business process, including application and operating system software, database, client workstations, server systems, network connectivity.

Air France-KLM IT Services are classified according to the maximum recovery time and financial impact following a major disruption exceeding normal operations.

Critical	Far reaching impact (>1M€), recovery within 4hrs;
Sensitive	Major impact (<1M€), recovery may be more than 4 hrs;
Normal	Moderate impact (<10k€), no recovery time defined.

Incident resolution times are determined by a combination of Service classification, unavailability of the service and impact on the customer (according to the following classification scheme)

Severity	Service	Level B	Level C	Level D
1	>1 Critical / Sensitive	Immediately	< 1 hour	< 2 hours
1	Critical / Sensitive	< 30 min	< 2 hours	< 4 hours
2	Critical / Sensitive	< 2 hours	< 4 hours	< 8 hours
2	Normal	< 4 hours	< 8 hours	

Information Security Management

Within all IT service activities, logical access management mechanisms are implemented in Information Systems to enforce user authentication by user-id and password. To manage the risk of unauthorized access to Information Systems, all logical access management mechanisms require alphanumeric passwords of at least xx characters, enforce password renewal within xx days, prohibit re-use of the last xx passwords, prohibit password renewal within xx days of the last change, force session time-out after xx minutes idle and lock accounts after xx successive failed login attempts. Access to Information Systems and data, is granted on a need to know basis, by a designated security officer on the basis of an approved standard authorisation matrix and are revoked in a timely manner on employee transfer, resignation or termination. Active logical access rights are checked at least every xx days and timely corrective action taken to maintain compliance with access management policies. Security activity at the operating system and database levels is monitored and logged, including but not limited to failed logical access attempts. Identified security violations are reported to management to take appropriate corrective actions. All incoming mail is scanned for viruses and up-to-date anti-virus software is installed on all xx-based computers. Firewall logs and relevant websites/media are checked daily to identify vulnerabilities and virus threats.

Operations Management

Access to the Data Control Centre and Twin Centre is restricted to a limited number of employees by means of authentication measures. An approval procedure is in place for incidental access. The Twin Centre is appropriately supported by a Tier-3 Data Centre that serve both internal and external customers 24×7 and whose IT resources support automation of business processes, so that the customer impact of short shutdowns due to facility outage are manageable. Back-up copies of software and data are scheduled and retained in accordance with the Air France-KLM Information System Security guidelines and any specific requirements defined in the Servile Level Agreement. 'Point-in-time' recovery (Wintel) and ‘Redo logging’ (Oracle) are enabled for databases of services classified as critical. Restoration of data from backups is tested at least every 6 months and appropriate action taken to correct any deficiencies found. Operations have implemented a set of standard procedures covering computer operations. Procedures and compliance are reviewed at least annually and appropriate corrective action taken.

Problem Management

ITIL defines problem as the unknown root cause of one or more existing or potential Incidents. Problems may sometimes be identified because of multiple Incidents that exhibit common symptoms. Problems can also be identified from a single significant Incident, indicative of a single error, for which the cause is unknown. The goal of the Problem Management process is to minimize the adverse impact of incidents and problems on the

business that are caused by errors within the ICT infrastructure, and to prevent recurrence of incidents related to these errors. Problem Management seeks to get the root cause of incidents and then initiate actions to improve or correct the situation. If a change on the ICT infrastructure is needed to solve the problem, an RfC (Request for Change) is submitted. Problems on shared services are handled by the Air France-KLM service owner, supported by both problem management departments. The provider participates in the Problem Management process and can receive and handle problems defined by Air France-KLM.

Configuration Management

ITILv3 defines Configuration Management as the *Process* responsible for maintaining information about *Configuration Items* required to deliver an *IT Service*, including their *Relationships*. This information is managed throughout the *Lifecycle* of the CI. Configuration Management is part of an overall Service Asset and Configuration Management *Process*. The goal of the Configuration Management process is to provide a logical model of the IT infrastructure by identifying, recording, controlling, maintaining and verifying CI's. Within the scope of the Configuration Management Database (CMDB) are the following components:

- Hardware, including network components where relevant;
- Middleware, including connectivity and databases;
- Physical network;
- Business services, systems and custom-built applications;
- System software, including operating systems;
- Software releases and packages, including commercial off-the-shelf packages and standard products;
- Service management components and records, including capacity plans, IT service continuity plans, incidents, problems, known errors, and requests for change.

The table shows the underlying Information Technology Systems also described as Operational Product that supports the ICT Services of the Information Management Organizations of Passenger Operations and Engineering & Maintenance.

Passenger Operations ICT Services (application)	**Platform**							**Third parties**
	Linux	**Unix**	**Wintel**	**z/OS**	**TPF (*)**	**Wang**	**Service Classification**	
INCRA				**X**	**X**		**C**	
LIDO		**X**	**X**		**X**		**C**	

(*) TPF = Transaction Processing Facility – commonly used in airline operations.

E&M ICT Services (application)	**Platform**							**Third parties**
	Linux	**Unix Oracle**	**Wintel**	**z/OS**	**TPF**	**Wang**	**Service Classification**	
AUTHORIZATION		**X**	**X**	**X**			**S**	
MAINTENIX A330		**X**	**X**				**C**	

IT Continuity Management

IT Continuity Management helps to ensure the availability and rapid restoration of IT services in the event of a disaster. For the IT Services that are Mission Critical for the daily airline operations plans are available to start production activities at the alternate site in case of a disaster in the primary site. The recovery plans are rehearsed on regular bases for in case if. The IT Services that are part of the IT Disaster Recovery Plans (IT DRP) were selected and twinned on basis of a Business Impact Analyses during the realization of the twin-center. Technical Disaster Recovery Plans are designed for the IT Infrastructure components. The procedure applies to an ICT Disaster that effects the daily operation in the “Bunker” or the “Co-location” and describes the actions to be taken in the first hour after the disaster. The IT DRP manual explains the Disaster Recovery Response organization of CIO/Information Services. All CIO/IS departments directly involved are provided with an ICT Disaster Recovery Plan (DRP) which contains detailed instructions, in checklist format, on how to handle the ICT Disaster. During activation of the Disaster Recovery organization, the ICT Disaster Recovery Plan is leading. Local laws, assistance- and fire brigade activities always prevail over the ICT Disaster Recovery Plan. Air France-KLM activities should not interfere with the official investigation unless agreed by the investigating authority. Which action shall be taken will be decided at the discretion of the DMI (Duty Manager ICT).

A procedure has been developed where, after receiving information regarding accidents, serious incidents, DMI will set-up a conference call with the reporting party, the Vice President of Information Services Operations (Pool 5) and Information Services Operations Management (Pool 4).

The situation will be evaluated and determined whether immediate further action is required. They will activate the investigation team to perform a Quick Damage Assessment Report. The input of the Quick Damage Assessment Report will be used to:

- classify the event,
- determine whether other departments will be involved and need to be included in the conference call,
- determine whether local- or Governement authorities need to be notified,
- determine whether Operations Control Center (OCC) needs to be notified.

Three possible outcomes which will activate the ICT Disaster Recovery Plan:

- Serious incident. Together with the participants in the conference call, the DMI will decide if activation of the ICT Disaster Recovery Plan is required.
- ICT Disaster. Air France-KLM ICT Disaster Recovery Plan will be activated.
- ITHANIC. After declaration of the ICT Disaster, the “Ithanic” procedure will be activated.

After the ICT Disaster Recovery plan is activated:

- DMI will activate the internal notification process coordinator who will notify all the internal Information Services parties.
- DMI will activate the external notification process coordinator who will notify all the Business parties about the non-availability of IT servives.
- The DMI will call standby team of DMI, OSA and SONO to go to the co-location and activate the control room.
- The ICT Command Center Locations will be activated. This is a third location (bunker, co-location, Command Center location) in which all employees involved in the recovery process can work if they are not necessary in the co-location.

When it has been decided to activate the ICT Disaster Recovery Plan, the notification process is initiated by the DMI. 3 Notification levels exist:

Level 1 = notification to the ICT departments and persons directly involved.
Level 2 = internal notification of CIO (Chief Information Officer), other CIO/IS Vice Presidents and CIO/IS Communication Consultants.
Level 3 = notification of Business Domains (Ground Services, Passenger Operations, Commercial, Sales, MRN, Engineering & Maintenance, Cargo, Corporate and CIO/IS) and supporting external parties.

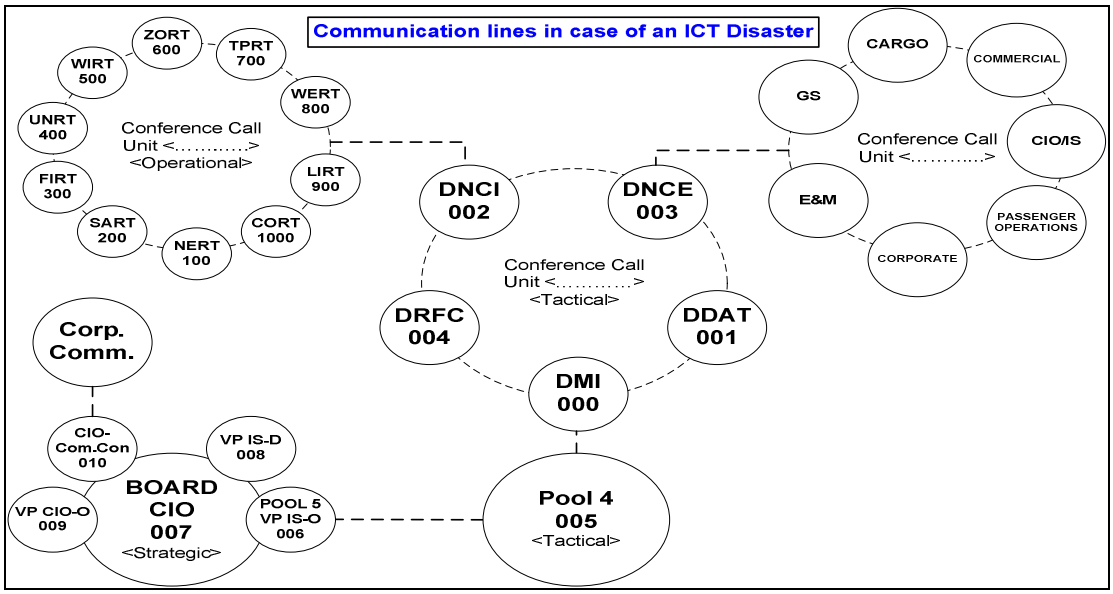


Figure 8: Source: V. Hiralall - Communication lines in case of an ICT Disaster

Scope Twin-Center and Architecture Principles

The Twin-Center design principles documented in the Platform Domain Architecture are valid for the same IT services as within scope of the Twin-Center project:

- All critical IT services to be placed in the Air France-KLM Data Center.
- All sensitive IT services for which the business decided that the service must be twinned.

Twin-Center considerations

To ensure that ICT support can be delivered to Air France-KLM, the data center is split up over two locations, interconnected via dedicated infrastructure components. The systems are divided in such a way that the catastrophic loss of one part of the twinned computer center doesn't result in a loss of service for a long period. The objective of the recovery plans is, to recover from a disaster situation to a controlled return to "business as usual" within the given Recovery Time Objectives

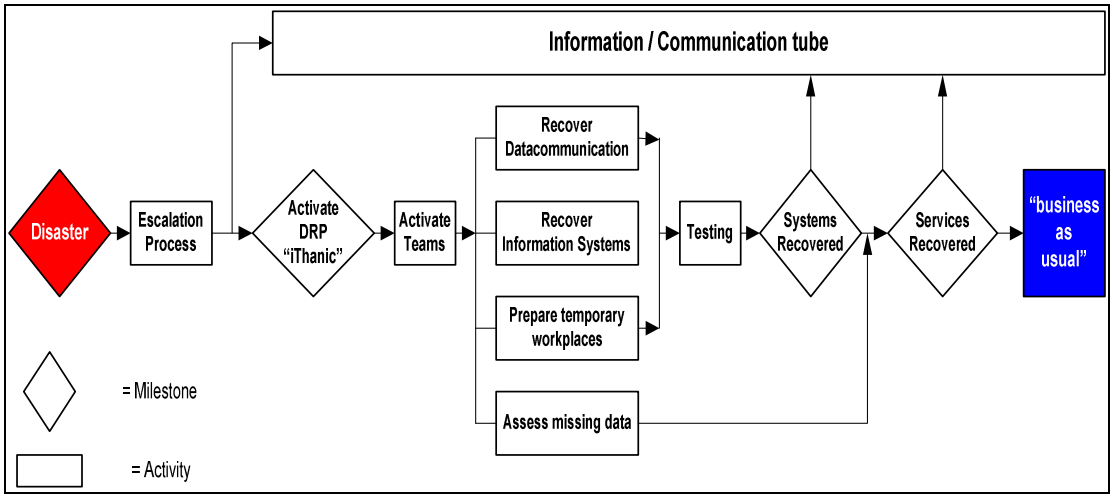


Figure 9: Source V. Hiralall - From disaster to "business as usual"

Requirements for Twin-Center and Architecture Principles

Design principles defined in the Twin-Center project:

- The Recovery Time Objective (RTO) is 4 hours maximum for all critical and (in scope) significant IT services.
- The recovery Point Objective (RPO) is zero data loss for all critical IT services and 24 hours data loss for (in scope) significant IT services
- The design will not take disaster upon disaster into account.

Design Principles related to Twin-Center

- Principle 16: A twinned IS service must not depend on a non-twinned IT service
- Principle 17: Windows and UNIX in twinned services must be based on the high availability options provided by the platform and defined by best practices.
- Principle 18: All twinned IT services should use the shared commodity infrastructure
- Principle 19: For twinned IT services all data necessary for the business operations of the IT service must be present (and up to date) in both Data Centers.
- Principle 20: Actions needed for fall back in case of a disaster must be automatic and/ or through a remote operator.
- Principle 21: Disaster recovery tests must be possible on a component level.

Interview Question / Answer of Passenger Operations and E&M

During the research I have interviewed the Information Management Organisation (IMO) of Passenger Operations and Engineering & Maintenance. The IMO's were interviewed because they support the business to meet their goals with focus on continuous optimization of business process, organization and information systems. The Q/A's are coded as:

- A1-PO = Question - Answer on question 1 by Passenger Operations
- A1-EM = Answer on question 1 by Engineering & Maintenance

Q1 Which IT Services are primary for the daily airline operations?

A1-PO ICT Services supplied by Information Services (main ICT Provider within Air France-KLM) are included in the Business Agreement with Passenger Operations. The services that are primary for the airline operations are classified as "Critical or Significant".

A1-EM Idem answer A1-PO

Q2 How was the IT Services prioritized to sustain that core competency in the face of a disaster or systems interruption are met. That means determining which data, applications, and systems get restored in what sequence and timeframes.

A2-PO IT Service recovery prioritization is based on past business experience and common sense. IT Service recovery is only arranged for Critical and Sensitive services which are twinned. The priority order of services to be recovered in the alternate site is described in the IT DRP.

A2-EM IT Service recovery prioritization is based on at least once a two year performed BIA. IT Service recovery is only arranged for Critical and Sensitive services which are twinned. The priority order of services to be recovered in the alternate site is described in the IT DRP

Q3 On basis of what method (BIA or other), business functions (services) has been classified in Critical, Significant and Normal.

- Is there recently a BIA executed to re-evaluate the classification of the IT Services?
- When was the last BIA carried out?
- Is there a BIA planned to be carry out in the near future?
- Is the BIA used to up-, downgrade the classification of IT Services.
- Or are IT Services classified on basis of common sense from past experience?

A3-PO A Business Impact Analyzes is not performed to classify IT Services.

- Recently no BIA executed to re-evaluate the classification of services
- It is not known when the last BIA was performed
- There is no BIA planned to be executed in the near future
- It is not known if a BIA is used to up-, downgrade the classification of IT Services
- The classifications of the current services are based on common sense from past experience.

A3-EM A Business Impact Analyzes was performed to classify IT Services.

- Recently no BIA executed to re-evaluate the classification of services
- The last BIA was performed 2 years ago.
- There is no BIA planned to be executed in the near future
- A performed BIA could be an entrance to up-, downgrade the classification of IT Services, but did not happened yet.

Q4 What does the loss of Critical IT Services means for Passenger Operations and E&M? Are costs of downtime measured?

A4-PO The loss of Critical IT Services means that the daily airline operation at the airport could be harmed. Scheduled flight could be cancelled due to the absence IT Services for passenger and luggage handling. Loss of income due to loss of IS. Crew assignment can not be performed. There is a standard cost estimation table filled in by IS in case of downtime.

A4-EM The loss of Critical and Significant IT Services does not mean that the daily airline maintenance activity stops in the hangars. There is an IT Fallback plan that covers the loss of network infrastructure in the maintenance area. In case of loss of the IS Data Center, E&M can continue their activities for 24 hours on manual basis. After the 24 hours, manual proceedings are not possible due to backlog. There is a standard cost estimation table filled in by IS in case of downtime.

Q5 What measures have been taken to ensure a continuous availability of core IT services for the daily airline operations?

A5-PO IT Disaster Recovery Plans are implemented for Critical and sensitive services which are twinned.

A5-EM Ditto answer.

Q6 Is a Business Continuity Plan available for facility disaster, power- or network failure?

A6-PO For some of the Critical services fall back procedures are described. That means for the situation that the core IT processes are still running in the data center. There are no Business Continuity Plans in which it is describes how to handle in case of facility or network failure.

A6-EM For the Critical and Sensitive services fall back procedures are described in case of communication network failures. That means for the situation that the core IT processes are still running in the Data Center. Business Continuity Plans also describes how to handle in case of loss of facility (hangars).

Q7 How long is such situation tolerable until it is no longer possible to operate manually and support of IT is indispensable?

A7-PO The critical IT Services of Passenger Operations can not proceed without IT services. The Maximum Allowable Downtime (MOD) is for twinned Critical and Sensitive Services therefore not more than 4 hours. For non-twinned services no measures are taken to recover services after the loss of the data center.

A7-EM The critical and sensitive activities of E&M can proceed 24 hours without IT services. The Maximum Allowable Downtime (MOD) for twinned Critical and Sensitive IT Services therefore is not more than 24 hours. For some of the other sensitive services IT Fallback procedures are implemented to overcome the first 24 hours after an IT disaster. For non-twinned services no measures are taken to recover services after the loss of the data center.

Q8 Are you known with the definition of RTO (Recovery Time Objectives)?

A8-PO RTO – Recovery Time Objectives - represent the maximum allowable downtime that can occur without severely impacting the recovery of operations or the time in which systems, applications, or business functions must be recovered after an outage (e.g. the point in time

that a process can no longer be inoperable). For the Critical services of Flight Operations a RTO of 4 hours is defined (that is the time that is required to reroute and recover the services from the destroyed datacenter in to the co-location). For the sensitive services a RTO of 24 hours is defined (that is due to the RPO of sensitive services)

A8-EM Ditto answer.

Q9 Are you known with the definition of RPO?

A9-PO RPO – Recovery Point Objectives - represents the amount of data that can be lost without severely impacting the recovery of operations or the point in time in which systems and data must be recovered (e.g., the date and time of a business disruption). For the Critical services a RPO of 0 hours is defined (that means no data loss). For the Sensitive services a RPO of 24 hours is defined.

A9-EM Ditto answer.

Q10 Has the management exercised disaster situation in order to rehearse decision-making processes in case this would happen?

- When was the last time an exercise was held?
- What were the results of the exercise?
- Is there an action plan based on the findings to adjust the processes, procedures and manuals?
- Is there management attention for planning and exercising of disaster rehearsals?

A10-PO No management exercises were held in the previous years.

A10 Management exercises are held twice a year (one planned and one unplanned) to rehearse management decision making. Input of independent observers is used to adjust processes and procedures. For the critical business processes a manual procedure is available for use in case of disaster. Results of exercises are used to update recovery procedures

Q11 Are you aware of the fact that a lot of critical twinned IT Services has dependencies on non-twinned IT Services and the workstation environment that is not twinned? Is there a top-management decision to twin all services to eliminate those dependencies?

A11-PO Yes we are aware of the dependencies. There is an ongoing cost estimation study to twin all non-twinned Critical, Sensitive and normal IT Services including the workstation environment.

A11-EM Ditto answer.

	Current		Proposed	
Service	**RTO**	**RPO**	**RTO**	**RPO**
Critical	4 hrs	0 hrs	1 hr	0 hr
Sensitive	4 hrs	24 hrs	24 hr	0 hr
Normal	n.a.	n.a.	>24 hrs < 1 month	0 hr

Q12 Are Crisis Management and Communication Management Plans available and rehearsed?

A12-PO There is plans for two situations; Response A (in case of an aircraft accident) and Response C (for non-aircraft incidents). For Response A is besides the Operational Management responsibility a team of 2000 trained Air France-KLM employees available to help as volunteers.

A12-EM Ditto answer.

IT Infrastructure Components of Passenger Operations

I have extensively exercised the Information Technology Infrastructure Components of one Critical IT Service of Passenger Operations to analyse the dependencies on the Operational Products (the underlying IT Infrastructure components) and the internal- and external twinned and not twinned services. The IT Service that is exercised is classified as “Critical” and it is primary for the daily airline operations.

Example of an Integrated E2E dependencies Framework

The outcome of the exercise shows that the critical IT Service INCRA has dependencies with IT Services that are twinned and those that are not twinned. Because of the current design, the functionality in a fallback situation of the critical IT Service INCRA cannot be determined. This situation is also relevant for other twinned Critical IT Services that has dependencies on non-twinned services.

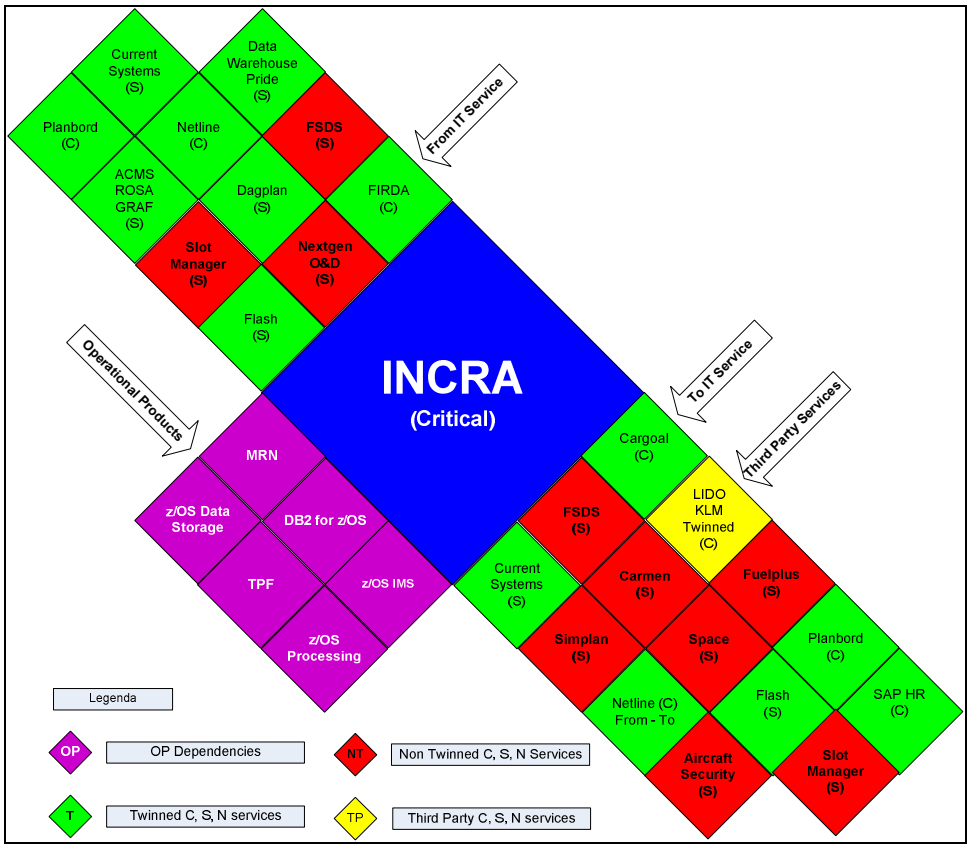


Figure 10: V. Hiralall – Integrated E2E IT Services dependencies framework

4.3. Business Continuity Institute PAS 56 Audit workbook

In addition to the interviews part of the PAS 56 audit Workbook **[30]** has been used to undertake a self-assessment to benchmark the Business Continuity Management status within Air France-KLM Passenger Operations and Engineering & Maintenance against the British Standards Institute's Good Practice Guide to Business Continuity Management. The assessment questions not answered by the interviewed is completed by the thesis author based on available Business Continuity documentation and experience gained during the realization of IT Disaster Recovery Plans for Information Services. The results of the assessment will be drawn about the current level of maturity in respect of BCM. In addition, recommendations will be given how Information Services and the Senior Management of Passenger Operations and Engineering & Maintenance can increase the maturity level of Business Continuity Management.

The workbook provides both a Good Practice Guidelines Process benchmark and a Performance benchmark within each of the six scorecards. The Workbook's mission is to determine if a business is following BCM good practices. The Workbook consists of six scorecards that reflect the BCM lifecycle. The questions and good practice compliance dashboard contained within each stage of the lifecycle enables the assessor to establish if an organisation is using BCM good practice. [24]

The result of the self assessment gives an overview of the weakness and strengths of the current implemented Business Continuity Management Processes against the BCI PAS 56 Audit workbook benchmark.

The scores on the following stages:

Stage 1 - Programme Management -	35
Stage 2 - Understanding the Business -	46
Stage 3 - BCM Strategies -	35
Stage 4 - BCM Planning -	57
Stage 5 - Embedding a BCM Culture -	38
Stage 6 - Exercise, Maintenance & Audit -	31

BCI PAS 56 assessment outcome

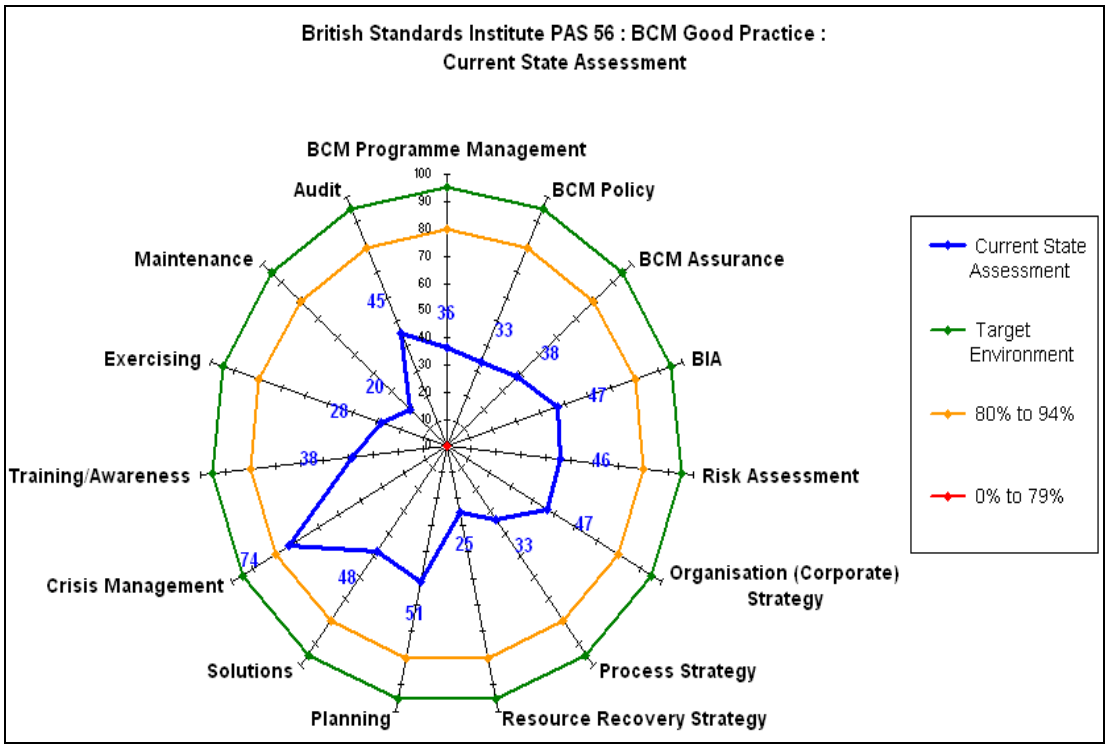


Figure 11: The PAS 56 Components Radar Chart after the workbook execution

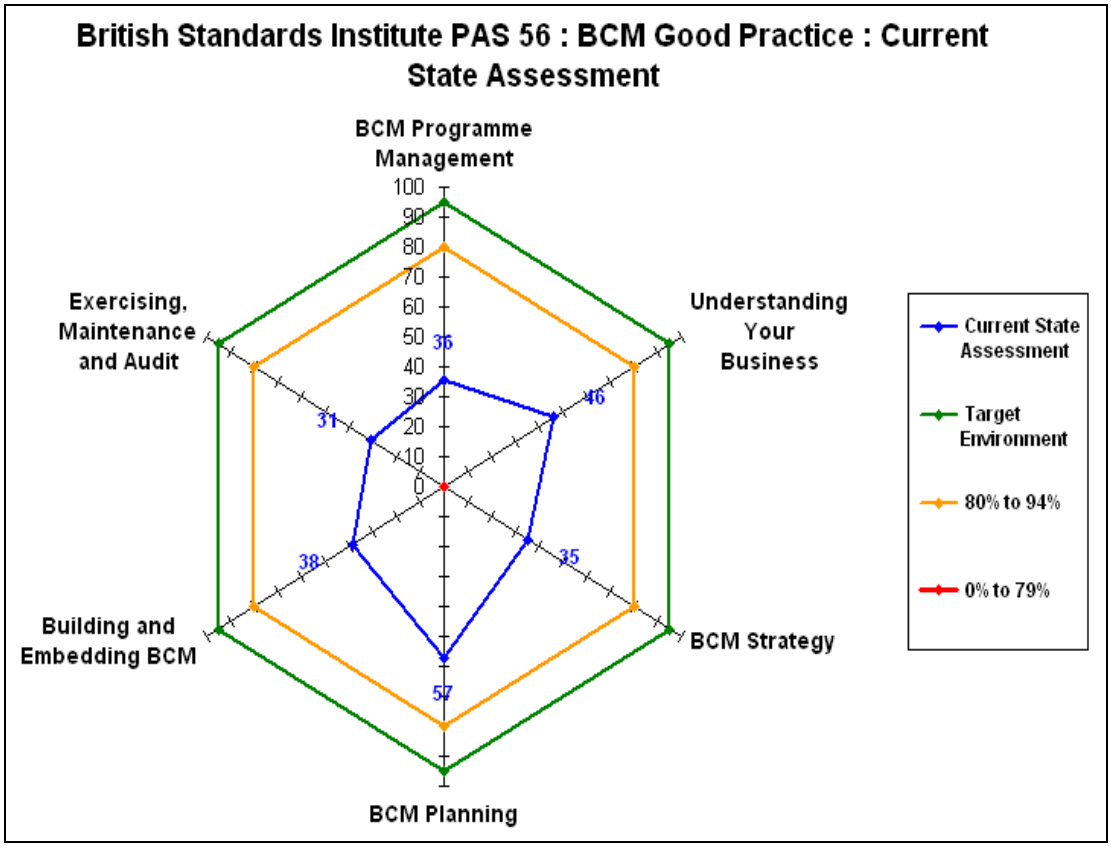


Figure 12: The PAS 56 Total Radar Chart after the workbook execution

5. Findings of the Case Study

5.1 Control Model

It is necessary that the major treats and risk areas that can jeopardise the airline operations are managed to assure continuous availability of the business processes that relies on the Information Technology Infrastructure components (data, applications, systems and networks). The Information Technology related risks can be categorised in relation to the following processes:

- application development, application maintenance, third party management, policies and procedures;
- service management, incident and problem management, change and release management, configuration management, service level management (including third party management), security management, operations management, continuity management;

The control model defines the *IT General Controls* for the business processes that rely on the Information Technology Infrastructure Components.

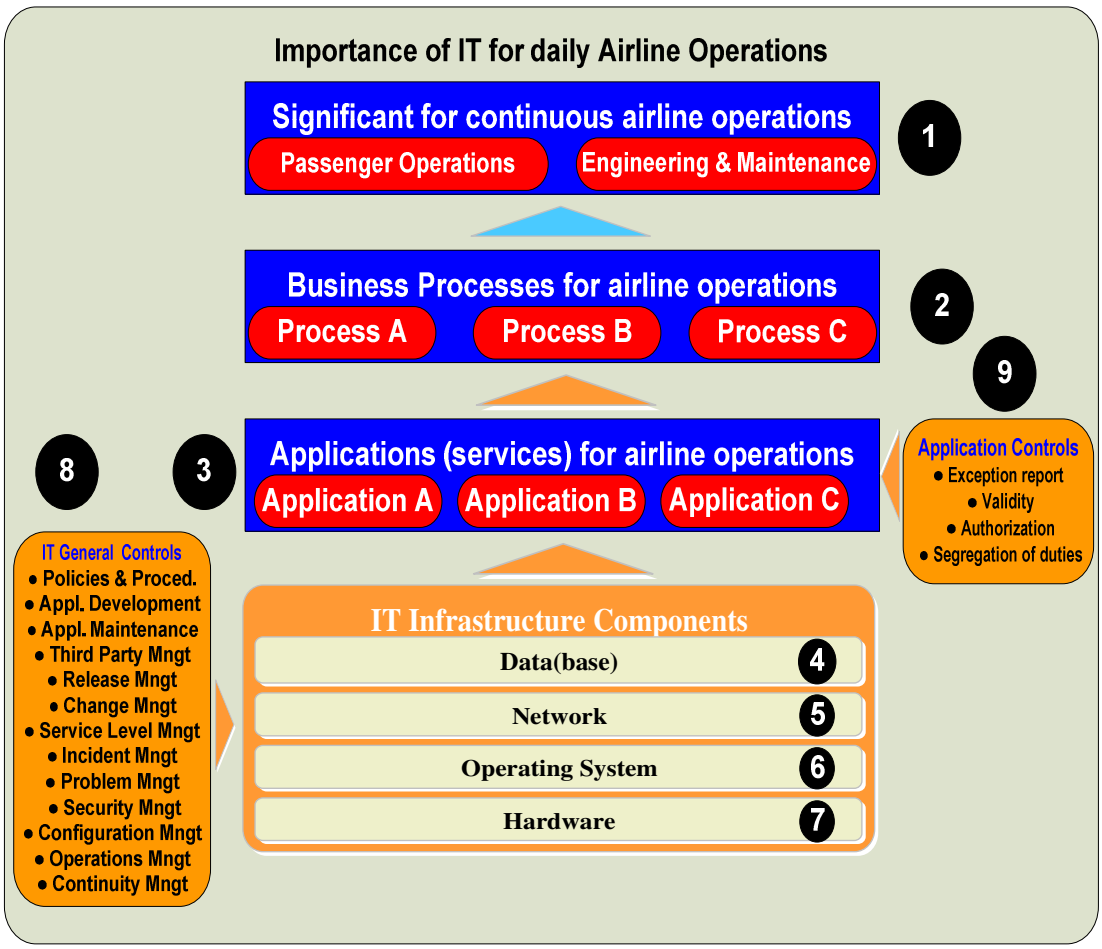


Figure 13: Source originally used for SOx – adapted by V. Hiralall for airline operations scope

Design Principles and Scope of the Control Model

The design of the control model is based on the following principles:

- the controls are applied to ICT services supplied by the IT Department of Air France-KLM and specified by the Senior Management of Passenger Operations and Engineering & Maintenance (E&M) as in scope, including their supporting technical infrastructure and any third parties involved;
- the controls are implemented to mitigate identified risks to the Confidentiality, Integrity and Availability of these services and their data;
- to ensure objective results, the controls must be tested independently by staff not involved in the day to day system development and service management activities.

The control model that has been setup for the establishment and auditing of Business Continuity Management for continuous daily airline operations is in the past introduced for compliance with the Sarbanes-Oxley Act of 2002 legislation [**33**], previously a legal obligation for Air France-KLM as a U.S. publicly listed company. For the aim of the case study the control model is partly reused. The difference between the former developed control model for SOx and the current lies in the fact that SOx does not mandate controls regarding business continuity. In the reshaped version, Business Continuity Management is part of the control model. The controls for Business Continuity Management are based on the "good practice" guidelines as described in the IT Assurance Guide - Using CobiT - 2007 from ITGI [**34**]. The control scope includes the risks to and controls on ICT processes, infrastructure and/or third party services outside CIO/IS control. The main categories are applications/services not supplied by CIO/IS, end-user administration and end-user computing.

Third Parties

The term 'third party' is used in this document in line with the ITGI guidelines to mean companies under contract to CIO/IS, to supply services in support of ICT services in scope or their related technical infrastructure. Equivalent terms in common Air France-KLM use are 'vendor' (IS-Distributed Services and IS-Operations), 'external service provider' (ESP, IS-Development).

Internal control extends to all third parties contracted to supply services in support of ICT services in scope. SAS 70 [35] or ISAE 3402 type II [35] reports[1] covering the relevant application and/or technical scope are preferred. Otherwise third party activities should be tested by exercising the 'right to audit' and extending the relevant controls.

[1] Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognised standard developed by the American Institute of Certified Public Accountants (AICPA) for auditing service organisations. A Type II report contains both the control descriptions and the test results covering at least a 6 month period. SAS 70 was superseded in December 2009 by International Standard on Assurance Engagements (ISAE) No. 3402 "Assurance Reports on Controls at a Service Organization", issued in by the International Auditing and Assurance Standards Board (IAASB), part of the International Federation of Accountants (IFAC). ISAE 3402 will replace SAS 70 for all service auditors' assurance reports covering periods ending on or after 15 June 2011.

Control Set

The control model is designed not to be specific for Passenger Operations and Engineering & Maintenance but can be used within all Business Divisions of Air France-KLM. For the case study I created a roles & responsibilities (RACI) table that is unique, explicit and unambiguous for Passenger Operations and Engineering and Maintenance. Each control is assigned to one or more owners, accountable for the correct application and functioning of the control and remediation of any deficiencies, and the corresponding executor(s), responsible for the operational execution of the control.

Roles and Responsibilities (RACI table)

The table below allocates the roles and responsibilities to Passenger Operations, Engineering & Maintenance, CIO/IS management and staff involved in internal control activities and relevant corporate parties (Internal Audit), based on the following definitions:

- Responsible: the position responsible for performing the activity;
- Accountable: the position ultimately accountable for the results;
- Consulted: position consulted for advice prior to a final decision or action being taken;
- Informed: position informed after a decision or action is taken.

Activity/Role	CIO	CIO/IS Controller E&M Controller Passenger Operations Controller	VPs CIO Office, Development, Operations, Distributed Systems, VP Engineering & Maintenance VP Passenger Operations	CIO Office, IS-D, IS-O and IS-DS Staff,	CISO	IS-D Manager CCC	Director Transversal NL Director Data Center Management	Internal Control Team for CM (ICT – CM) CM = Continuity Management	Internal Audit
Risk Assessment	A	I	R		C	C	C	I	
Control Ownership	A	I	R		C	C	C	I	
Control Execution	A	I		R	C	C	C	I	
Control Design	A	I	I	I	R	R	R	I	C
Control Test	A	I	I	I	R	R	R	I	C
Control Remediation	A	I	R	R	I	I	I	I	I

Documentation set

The documentation/ information set have been maintained only for those IT Services that are supplied by Information Services (main ICT Provider within Air France-KLM), included in the Business Agreement between IS and relevant Business Divisions.

Document	Owner	Document Management
1. CIO/IS ITGC Framework for Continuity Management	MT-XA	By CIO/IS internal control team for CM (ICT– CM); updates to be formally approved by MT-XA
1a. Applications relevant for internal control	Business divisions	The business divisions inform the ICT-CM if any changes occurred that can impact airline operations. The ICT-CM team members who check and update the test plans (platforms and third parties) as appropriate and inform the control owner(s). The ICT-CM documents the changes in the framework.
1b. Risk vs. control matrix	CIO/IS VPs	Following a process change, the CIO/IS ICT-CM team the risk assessment, checks and updates the test plans as appropriate and consults the control owner(s). The CIO/IS ICT-CM documents the changes in the framework.
1c. Control set (Chapter 6.9)	CIO/IS VPs	1. Changes resulting from application or process changes: see 1a and 1b above. 2. Changes resulting from auditors' recommendations: the CIO/IS ICT-CM updates the test plans as appropriate and informs the control owner(s). The CIO/IS ICT-CM internal control team documents the changes in the framework. 3. Changes resulting from CIO/IS management decisions: the ICT-CM obtains the auditors' agreement to significant changes and updates the test plans as appropriate. The CIO/IS ICT-CM documents the changes in the framework.
1d. Third parties	CISO IS-D TLM & Package mgt. IS-O Vendor & Licence mngt	The CIO/IS ICT-CM determines or updates the test approach as appropriate and informs the control owner(s). The CIO/IS ICT-CM documents the changes in the framework.
2. Test plans and results	CISO IS-D. IS-O Transversal NL IS-O DCM IS-DS	The CIO/IS ICT-CM finalises the plan before the start of testing. Subsequent updates: see 1a – 1d above. The test results will also be documented in the test plan.
3. Control issue reports	CISO IS-D. IS-O Transversal NL IS-O DCM IS-DS	The CIO/IS ICT-CM evaluates, classifies and documents each issue and reviews the findings and agrees the remediation plan with the Control Owner. The Control Owner manages resolution and reports progress to the CIO/IS ICT-CM for update of the control issue report. Control issues are closed when the control is proven effective by a retest.

The indicated owners reflect the departments inside Air France-KLM.

5.2 Results of the Control Model

The following table shows the CIO/IS IT processes and their associated risks. The controls associated with the risks (column ITGC) are not inserted in the thesis. CIO/IS can be seen as the IT Service Provider of Air France-KLM. The Information Management Organizations of the Business Divisions of Air France-KLM can be seen as the IT Service User's Organization.

Notes:

1. The process and risk reference codes are for internal control purposes only and have no other significance.
2. The IS-DS and IS-O service and infrastructure management processes, prefixed ODS, are based on the ITIL v2 standard names. The Engineering & Maintenance and Passenger Operations IT Service and infrastructure management processes are respectively prefixed as E&M and PO. For simplicity, Incident Management has been grouped with Problem Management, and Change Management with Release Management. The processes are treated as a single group rather than separate IS-DS and IS-O activities, as the process and service managers' responsibilities in the Combined IT organisation extend over both departments, independent of their individual reporting relationships.
3. The controls are based on the "good practice" guidelines as described in IT Control Objectives for Sarbanes-Oxley (SOx) 2nd edition issued by the ITGI **[31]** and Control Objectives for Information and related Technology 4.1 **[32]**, tailored to the Passenger Operations and E&M organisation;
4. The control groups and control objective statements are taken from the ITGI guidelines (CobiT for SOx 2nd Edition), figures 15 to 26 [30] and ITGI IT Assurance guide 2007 [33]. Specific references in the ITGI objectives to financial reporting have been removed, to ensure that the control framework can be applied to other business processes as and when required.
5. The potential risk impact classification is based on following criteria:
    - High: the risk outcome will threaten the effectiveness of the ICT service and/or IT dependent controls;
    - Medium: the risk outcome will have a significant impact on, but will not threaten the effectiveness of, the ICT service and/or IT dependent controls;
    - Low: the risk outcome is unlikely to have a significant effect on the effectiveness of the ICT service and/or IT dependent controls.

CIO/IS Processes		Associated Risks			Control Group	Control Objective	ITGC
Ref.	Name	Ref.	Description	Impact			
CIO-P1	Policies & Procedures	R1	The integrity of information systems is compromised by the absence of up-to-date policies and procedures defining the required acquisition, development, maintenance, operations, security and data management processes	Low	Ensure Systems Security	Controls provide reasonable assurance that information systems and subsystems are appropriately secured to prevent unauthorised use, disclosure, modification, damage or loss of data	18_11
CIO-P2	Application Development	R14	The integrity of application software is compromised as a result of inadequate design, development and test of the application controls that support complete, accurate, authorised and valid transaction processing	High	Acquire and Maintain Application Software	Controls provide reasonable assurance that application and system software is acquired or developed that effectively supports requirements	11_02
TPM-P1	Third Party Management: Procurement	R2	Third party services do not (sufficiently) support the confidentiality and/or integrity of the information systems and related data	High	Manage Third Party Services	Controls provide reasonable assurance that third party services are secure, accurate and available; support processing integrity; and are defined appropriately in performance contracts	17_03 17_04
ODS-P1		R1	The integrity of information systems is compromised by the absence of up-to-date policies and procedures defining the required acquisition, development, maintenance, operations, security and data management processes	Low	Manage Operations	Controls provide reasonable assurance that authorised programs are executed as planned and deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing and error monitoring	22_03
ODS-P2	Service Support: Incident / Problem Management	R4	Incidents and problems are not detected, are inadequately addressed and/or not resolved	High	Manage Problems and Incidents	Controls provide reasonable assurance that any problems and/or incidents are properly responded to, recorded, resolved or investigated for proper resolution	20_01
ODS-P3	Service Support: Change / Release Management	R5	The integrity of information systems and related data is compromised by the use of unauthorised and/or untested software	High	Install and Accredit Solutions and Changes	Controls provide reasonable assurance that the systems are appropriately tested and validated prior to being placed into production processes and that associated controls operate as intended and support requirements	14_02
		R6	The integrity of information systems and related data is compromised by unauthorised changes made to the ICT production infrastructure	High	Manage Changes	Controls provide reasonable assurance that significant system changes are authorised and appropriately tested before being moved to production	15_01 15_02 15_03 15_04 19_02

CIO/IS Processes		Associated Risks			Control Group	Control Objective	ITGC
Ref.	Name	Ref.	Description	Impact			
ODS-P4	Service Support: Configuration Management	R7	The integrity of information systems is compromised due to deviations between the configuration registration and the actual situation	Low	Manage the Configuration	Controls provide reasonable assurance that IT components, as they relate to security and processing, are well protected, would prevent any unauthorised changes, and assist in the verification and recording of the current configuration	19_05 19_08
ODS-P5	Service Delivery: Service Level Management	R2	Third party services do not (sufficiently) support the confidentiality and/or integrity of the information systems and related data	High	Manage Third Party Services	Controls provide reasonable assurance that third party services are secure, accurate and available; support processing integrity; and are defined appropriately in performance contracts	17_05
ODS-P6	Security Management	R9	The confidentiality, integrity and/or availability of business data are compromised, either intentionally or otherwise, by unauthorised persons gaining logical access to information systems.	High	Ensure Systems Security	Controls provide reasonable assurance that information systems and subsystems are appropriately secured to prevent unauthorised use, disclosure, modification, damage or loss of data.	18_01 18_02 18_03 18_05 20_02
		R10	The confidentiality, integrity and/or availability of information systems and related data are compromised by computer malware (i.e. viruses, trojans, worms and other threats).	Low	Manage the Configuration	Controls provide reasonable assurance that IT components, as they relate to security and processing, are well protected, would prevent any unauthorised changes, and assist in the verification and recording of the current configuration.	19_06 19_07
ODS-P7	ICT Infrastructure Management: Operations Management	R11	The confidentiality, integrity and/or availability of information systems and related data are compromised, either intentionally or otherwise, by unauthorised persons gaining physical access to computing facilities.	Medium	Ensure Systems Security	Controls provide reasonable assurance that information systems and subsystems are appropriately secured to prevent unauthorised use, disclosure, modification, damage or loss of data.	18_09 18_10
		R12	Business data are irretrievably damaged or lost.	High	Manage Data	Controls provide reasonable assurance that data recorded, processed and reported remain complete, accurate and valid throughout the update and storage process.	21_02 21_03

CIO/IS Processes		Associated Risks			Control Group	Control Objective	ITGC
Ref.	Name	Ref.	Description	Impact			
		R13	The confidentiality and/or integrity of business data are compromised by inadequate control of batch transaction processing.	High	Manage Operations	Controls provide reasonable assurance that authorised programs are executed as planned and deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing and error monitoring.	22_02
D-P1	Application Development	R1	The integrity of information systems is compromised by the absence of up-to-date policies and procedures defining the required acquisition, development, maintenance, operations, security and data management processes.	Low	Enable Operations	Controls provide reasonable assurance that policies and procedures that define required acquisition and maintenance processes have been developed and are maintained, and that they define the documentation needed to support the proper use of the applications and the technological solutions put in place.	13_02
		R14	The integrity of application software is compromised as a result of inadequate design, development and test of the application controls that support complete, accurate, authorised and valid transaction processing.	High	Acquire and Maintain Application Software	Controls provide reasonable assurance that application and system software is acquired or developed that effectively supports requirements.	11_02
					Install and Accredit Solutions and Changes	Controls provide reasonable assurance that the systems are appropriately tested and validated prior to being placed into production processes and that associated controls operate as intended and support requirements.	14_01
D-P2	Application Maintenance	R1	The integrity of information systems is compromised by the absence of up-to-date policies and procedures defining the required acquisition, development, maintenance, operations, security and data management processes.	Low	Enable Operations	Controls provide reasonable assurance that policies and procedures that define required acquisition and maintenance processes have been developed and are maintained, and that they define the documentation needed to support the proper use of the applications and the technological solutions put in place.	13_03
		R15	The integrity of the information systems and related data is compromised by unauthorised and/or untested changes made to the application software.	High	Manage Changes	Controls provide reasonable assurance that significant system changes are authorised and appropriately tested before being moved to production.	15_05 15_06 15_07

CIO/IS Processes		Associated Risks			Control Group	Control Objective	ITGC
Ref.	Name	Ref.	Description	Impact			
D-P3	Third Party Management: Performance Management	R2	Third party services do not (sufficiently) support the confidentiality and/or integrity of the information systems and related data.	High	Manage Third Party Services	Controls provide reasonable assurance that third party services are secure, accurate and available; support processing integrity; and are defined appropriately in performance contracts.	17_06
D-P4	Policies & Procedures	R1	The integrity of information systems is compromised by the absence of up-to-date policies and procedures defining the required acquisition, development, maintenance, operations, security and data management processes.	Low	Enable Operations	Controls provide reasonable assurance that policies and procedures that define required acquisition and maintenance processes have been developed and are maintained, and that they define the documentation needed to support the proper use of the applications and the technological solutions put in place.	13_01
ODS-P8	Continuity Management	R16	Lack of the availability of an IT continuity framework that leads to: • Insufficient continuity practices • IT continuity services not managed properly • Increased dependency on key individuals	Medium	Ensure Continuous Service	Controls provide reasonable assurance that a framework is developed for IT continuity to support enterprise-wide business continuity management using a consistent process to assist in determining the required resilience of the infrastructure and to drive the development of disaster recovery and IT contingency plans.	23_01
ODS-P8	Continuity Management	R17	Lack of the availability of IT continuity plans that leads to: • Failure to recover IT systems and services in a timely manner • Failure of alternative decision-making processes • Lack of required recovery resources • Failed communication to internal and external stakeholders	High	Ensure Continuous Service	Controls provide reasonable assurance that IT continuity plans are designed to reduce the impact of a major disruption on key business functions and processes.	23_02
ODS-P8	Continuity Management	R18	Lack of items specified as most critical in the IT continuity plans that leads to: • Unavailability of critical IT resources • Increased costs for continuity management • Prioritisation of services recovery not based on business needs	High	Ensure Continuous Service	Controls provide reasonable assurance that the plans focuses on items specified as most critical in the IT continuity plan to build in resilience and establish priorities in recovery situations in line with prioritised business needs, while ensuring that costs are kept at an acceptable level and complying with regulatory and contractual requirements.	23_03

CIO/IS Processes		Associated Risks			Control Group	Control Objective	ITGC
Ref.	Name	Ref.	Description	Impact			
ODS-P8	Continuity Management	R19	Lack of maintenance of the IT continuity plan that leads to: • Inappropriate recovery plans • Plans failing to reflect changes to business needs and technology • Lack of change control procedures	Medium	Ensure Continuous Service	Controls provide reasonable assurance that IT management defines and executes change control procedures to ensure that the IT continuity plan is kept up to date and continually reflects actual business requirements.	23_04
ODS-P8	Continuity Management	R20	Lack of regular testing of the IT continuity plans that leads to: • Shortcomings in recovery plans • Outdated recovery plans that do not reflect the current architecture • Inappropriate recovery steps and processes • Inability to effectively recover should real disaster occur	Medium	Ensure Continuous Service	Controls provide reasonable assurance that the IT continuity plan is tested on a regular basis to ensure that IT systems can be effectively recovered, shortcomings are addressed and the plan remains relevant.	23_05
ODS-P8	Continuity Management	R21	Lack of regular IT Continuity Plan Training that leads to: • Outdated training schedules • Failure to recover as expected due to inadequate or outdated training	Medium	Ensure Continuous Service	Controls provide reasonable assurances that all concerned parties are provided with regular training sessions regarding the procedures and their roles and responsibilities in case of an incident or disaster.	23_06
ODS-P8	Continuity Management	R22	Lack of timely distribution of the IT Continuity Plan that leads to that: • Confidential information in the plans are compromised • Plans not accessible to all required parties • Upgrades of the plan not performed in a timely manner due to uncontrolled distribution strategies	Medium	Ensure Continuous Service	Controls provide reasonable assurances that a defined and managed distribution strategy exists to ensure that plans are properly and securely distributed and available to appropriately authorised interested parties when and where needed.	23_07
ODS-P8	Continuity Management	R23	Lack of IT Services recovery and resumption planning that leads to: • Shortcomings in recovery plans • Inappropriate recovery steps and processes • Failure to recover business-critical systems and services in a timely manner	Medium	Ensure Continuous Service	Controls provide reasonable assurances that actions are taken for the period when IT is recovering and resuming services. This may include activation of backup sites, initiation of alternative processing, customer and stakeholder communication, and resumption procedures.	23_08

CIO/IS Processes		Associated Risks			Control Group	Control Objective	ITGC
Ref.	**Name**	**Ref.**	**Description**	**Impact**			
ODS-P8	Continuity Management	R24	Lack of well managed Offsite Backup Storage that leads to: • Unavailability of backup data and media due to missing documentation in offsite storage • Loss of data due to disaster • Accidental destruction of backup data • Inability to locate backup tapes when needed	Medium	Ensure Continuous Service	Controls provide reasonable assurances that all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans are stored offsite and that offsite arrangements are periodically assessed, at least annually, for content, environmental protection and security.	23_09
ODS-P8	Continuity Management	R25	Lack of post-resumption review that leads to: • Inappropriate recovery plans • Recovery plans failing to meet business needs • Objectives not met by the recovery plans	Medium	Ensure Continuous Service	Controls provide reasonable assurances that IT management has established procedures for assessing the adequacy of the plan in regard to the successful resumption of the IT function after a disaster, and update the plan accordingly.	23_09

5.3 Findings of Passenger Operations and E&M BCM

The interviews, collecting and analyzing information regarding the status of the current recovery plans confirmed me that the “good practice for Business Continuity Management” such like PAS 56 was not used for the establishment of Business Continuity Management within Passenger Operations and E&M. Although Air France-KLM did not used British Standards Institute's Good Practice Guide to implement Business Continuity Management within their organization, some part of the current implementation are in line with the stages of BCI PAS 56. The filling exercise should be taken into consideration when setting up and managing Business Continuity Management. It helps the Organization to oversee all the aspects of BCM and what to implement that is relevant for a mature BCM.

The established recovery plans are in general implemented as recommended by the Air France-KLM Information Security Manual based on the British Standards BS ISO /IEC 17799:2005 – Code of Practice for Information Security Management.

The Business Agreement: 2010 - 2011 between IMO Passenger Operations, E&M and Air France-KLM Information Services describes the IT services that are used by both IMO’s. The IT Services that are part of the IT Disaster Recovery Plan are indicated with Twinned = (**Y**).

Conducting the case study I found out that the current recovery plans were focused on IT Disaster Recovery Planning (IT DRP). The CIO/IS-Operations department is responsible for the implementation of IT Disaster Recovery Plans for the IT Services that are designated by the Business Divisions IMO’s.

The IT Services that are part of the IT Disaster Recovery Plan (IT DRP) are mostly Critical IT Services. Some of the Sensitive IT Services are also twinned because of their dependencies with other Critical or sensitive IT Services. Normal IT Services are moderately twinned.

Passenger Operations is highly dependant on the uninterrupted availability of IT Services because their business processes can not run in case of an outage that lasts longer than four hours. E&M can run their critical business processes on manual basis for the first 24 hours without the availability of IT. After the 24 hours, manual proceedings are not possible due to backlog.
IT Services are classified in three categories

	Current		Proposed (*)	
Service	**RTO**	**RPO**	**RTO**	**RPO**
Critical	4 hrs	0 hrs	1 hr	0 hr
Sensitive	4 hrs	24 hrs	24 hr	0 hr
Normal	n.a.	n.a.	>24 hrs < 1 month	0 hr

(*) In case of twinning all IT Services

The table shows that for Critical IT Services that are twinned, a RTO of 4 hours is acceptable (Recovery Time Objective: How fast will it work again) and a RPO of 0 hour is acceptable (Recovery Point Objective: to which point in time is the data available again. RPO of 0 hour means no data loss).

For some of the Critical IT Services of Passenger Operations and E&M, extra measures are taken in case of loss of facility due to a disaster (fire, bombs, terrorist attack or power-, network outage). For this kind of disasters, Passenger Operations has manual procedures that are tested on monthly basis in a location more than 3 kilometres of the current facility. The test results are evaluated and actions plans are released to customize the test plans. E&M has manual procedures (ICT Fall Back Plans) that covers the first 24 hours in case of network- or power outage. These plans are tested on a monthly basis in a location more than 800 meters of the current facility. The test results are evaluated and actions plans are released to customize the test plans. Twice a year management testing is organized to involve management in decision rehearsal in case of a real situation. The test has once a year a pre-planned and once an un-planned character.

There are no Business Continuity Plans available that describes manual procedures for the IT Services that are not twinned. There are also no plans for facility relocation or continuity problems that arise in case of Bird Flu, strikes and facility blockades.

Passenger Operations has a Masterplan Contingency Management that describes the criteria for contingency in case multiple flights can not be performed. It also describes the contingency organization, the participants and their roles.

The continuity reliability of Third Parties is not verified on a controlled manner. The right to audit or to receive information regarding continuity test results and follow actions are part of the contract agreement but in general it is not practiced as part of the control function.

6. Conclusions

6.1. Central main question

Central research question:
Which IT Infrastructure components (data, applications, systems and networks) have a primary relationship with airline operations and how can major risk areas made manageable and controllable for continuous availability of business processes?

Sub question (1) – Describe
What do the business processes and underlying Information Technology Systems for airline operations look like?

Sub question (2) – Analyze
Which major treats and risk areas can be identified and how can appropriate mitigation measures be taken?

Sub question (3) – Consider
Which elements and characteristics are included in the control framework for the establishment and auditing of Business Continuity Management for continuous daily airline operations?

6.2. Major findings

The current recovery plans are in general implemented as recommended by the Air France-KLM Information Security Manual based on the British Standards BS ISO /IEC 17799:2005 – Code of Practice for Information Security Management. The BCI "Good practice for Business Continuity Management – PAS 56" was generally not used for the establishment of Business Continuity Management within the scope of the case study.

The major finding of the case study is shown in the outcome of the exercise (Integrated E2E dependencies of INCRA) were the critical IT Service INCRA has dependencies with IT Services that are twinned and those that are not twinned. Because of the dependencies of INCRA on both twinned and non-twinned IT Services it is therefore impossible to determine whether the critical IT Service INCRA will function due to the absence of the incoming data stream from the non-twinned services in a fallback situation. This situation is also relevant for other twinned Critical IT Services that has dependencies on non-twinned services.

There are concerns within the Business Divisions about the reliability of the setup of the Twin-center concept. This concept has a highly focus on twinning the Critical IT Services and some Sensitive services in case they have highly dependencies with other Critical IT

Services. The issue that arises by twinning only Critical Services and a low number of Sensitive services is that in case of a disaster in the Data Center, backup and program of non-twinned services will be lost making recovery impossible.

IT Services that are classified as critical (PAS 56 defines it as – Mission Critical Activities), for the daily airline operations are twinned for a continuous availability of business processes. Classification of the IT Services is based on performed BIA's (exercised before the establishment of the twin center). The Business Divisions in scope of the case study has classified their IT Services for their business processes in three classes; Critical, Sensitive and Normal. In case IT Services are classified as Critical it means that they support Mission Critical Activities within the business. Sometimes services are classified on basis of common sense, or experience from the past. This way of selecting services for twinning has noting to do with treats and risks that can jeopardize the availability of IT Services.

Air France-KLM has setup a second Data Centre (Twin-centre) for uninterrupted business processing in case of a Data Centre disaster on the primary site. The Continuous Operations model provides Data centre facilities at two locations interconnected via Fiber Optics (Dark Fiber). This allows Operations to install systems, belonging to a High Available cluster or farm, across these locations. Doing so provides for quick recovery of critical services in the event of a disaster at the Air France-KLM Data Centre.

Third Parties that deliver IT Services to Air France-KLM are growing. The dependency is therefore a risk for the availability and continuity of airline operations processes in case the Third Party is affected by a disaster. Although Air France-KLM has the right to audit or to receive information about their recovery capabilities as part of the contract agreement, in general it is not practiced as part of the control function.

The business processes and underlying Information Technology Systems of the Critical and sensitive IT Services of Passenger Operations and E&M that are primary for the daily airline operations is described in the Service Reference Manual (SRM).

The elements and characteristics that is included in the control model for the establishment and auditing of Business Continuity Management for continuous daily airline operations gives an overview of the controls that can be established on basis of the risks for the environment in scope.

6.3. Recommendation

I like to recommend the management of CIO/IS to conduct an indebt analyzes for all the Critical IT Services that has inter dependencies with other IT Services. The first step to take is to analyze if the incoming data stream for the processing of Critical IT Services is received from twinned or from non-twinned services. The second step that has to be taken is to twin the non-twinned services that deliver relevant incoming data for the processing of the Critical IT Services. In order of importance for the daily airline operations, a roadmap has to establish for twinning the inventoried not-twinned services. Some can claim that it is cost effective to twin all not twinned classes of IT Services rather than to analyze the dependencies for each critical service before twinning. Due to the current budget constrains it is better to execute the implementation of non-twinned IT Services based on the importance of the IT Service for other already twinned Critical IT Services. By choosing this phased implementation plan it is necessary to implement a process to keep the E2E chain and IT Service dependencies current. After the finalizing of the Configuration Management implementation in JIMS, it can be a great help to aggregate the dependencies of twinned Critical IT Services on non-twinned IT Services.

To mitigate the risk of disasters at the Third Party site that results in non-availability of airline operations business processes, it is important to implement controls to assure that IT Service are delivered within the agreed Service Levels. This can be done by regularly verification of the Third Party recovery capabilities or by requesting for an ISAE 3402 audit report that gives some assurance on the Third Party capability to deliver IT Services in case of disaster.

I would recommend the responsible management of Air France-KLM, to implement or to tune-up Business Continuity Management based on the British Standard Institution BS25999-1 standard for Business Continuity Management. This official standard was published in November 2006 to replace PAS56. BS25999 embraces two standards: BS 25999-1 and BS 25999-2. The former is a code of practice (which is the document based upon PAS56) and the latter is a specification for business continuity management. It is intended to provide assistance to the person responsible for implementing business continuity management within an organization. It describes a framework and process for the Business Continuity Manager to use and offers a range of good practice recommendations. The second part can also be used to assess an organization's ability to meet regulatory and other requirements, and as such is the basis for certification. (Source:www.pas56.com).

7. References

[1] Yair Levy, Timothy J. Ellis. Towards a Framework of Literature Review Process in Support of Information Systems Research – 2006

[2] Stephen J. Doug et al. The hidden value in airline operations - Mckinseyquarterly.com November 2003.doc

[3] Barry C. Smith. Optimization in Airline Planning and Marketing - Institute for Mathematics and Its Applications – November 2002

[4] Numo Machado et al. – Impact of the Organizational Structure on Airline Operations

[5] A. Castro. Centros de controlo operacional: Organizacao e ferramentas. Monograph for Post-graduation in Air Transport Operations, 2008. ISEC - Instituto Superior de Educao e Ciłncias.

[6] Antonio J.M. Castro and Eugenio Oliveira. Disruption management in airline operations control, 2010

[7] N. Kohl and S. Karisch. Airline crew rostering: Problem types, modeling, and optimization. Annals of Operations Research, 127:223-257, 2004.

[8] M. Clarke. Irregular airline operations: A review of the state-of-the practice in airline operations control centre. Journal of Air Transport Management, 4:67-76, 1998.

[9] N. Kohl, A. Larsen, J. Larsen, A. Ross, and S. Tiourine. Airline disruption management perspectives, experiences and outlook. Journal of Air Transport Management, 13:149-62, 2007.

[10] Ram L. Kumar - A Framework for assessing business value of Information Technology Infrastructure - Journal of Management Information Systems / Fail 2004, Vol, 21, No. 2. pp, 11-32.

[11] Djoen S, Tan and Aad A. Uijttenbroek - Information Infrastructure Management - Fall97, vol.14

[12] ERPANET - Electronic Resource Preservation and Access NETwork

[13] Steve Elky - An Introduction to Information System Risk Management - May 31, 2006 - SANS Institute

[14] Securance Consulting 2005 - Technology Risk Matrix

[15] Yacov Y. Haimes - On the definition of vulnerabilities in measuring risks to infrastructures - Risk Analysis, Vol.26 No.2, 2006

[16] Philip L. Powell & Jonathan H. Klein - Risk Management for Information Systems Development - Journal of IT (1996) 11, 309-319

[17] Green, J. (1995) – Business Resumption Planning, Unpublished MSc Thesis, University of Warwick

[18] Bob Landström – A Quick Primer on Data Center Tier Ratings – July 15th, 2008 - http://notesfromtheconsultantsjungle.com

[19] Dorian J. Cougias - Preparing for Disaster or the auditor whichever is worse - SearchDataCenter.com

[20] Werner Verlinden - A short tour of business continuity management standards - principal consultant BCM & director, Ascure

[21] Dr. David J. Smith FBI - Business Continuity Institute - BCM Good Practice guidelines version BCI DJS 1.0 - 01.11.02.pdf

[22] Jim Burtles - PAS 56 - 2003 - An Overview from Automata, January 2005 - adopted from the BSI

[23] James A. Scholz - Securing Critical IT Infrastructure - Information Security Journal: A Global Perspective, 2009 - Copyright © Taylor & Francis Group

[24] Scott W. Ream, The Business Continuity Maturity Model 2003, www.ContingencyPlanning.com

[25] NIST SP 800-34 http://csrc.nist.gov/publications/nistpubs/index.html.

[26] Carl B. Jackson, CISSP, CBCP - The changing face of Continuity Planning – 2002

[27] Classes of recovery - Computer Network Technology - Corporation - www.cnt.com

[28] Caroline Sapriel - Taking the long view - Communications World 2007 - www.iabc.com

[29] C.S. Norman et al - Assessing Information Technology General Control Risk - An Instructional Case - Issue in Accounting Education – Vol. 21 no.1 February

[30] The Business Continuity Institute PAS 56 Audit Workbook 2003

[31] IT Control Objectives for Sarbanes-Oxley - 2nd edition, September 2006 - IT Governance Institute (www.itgi.org)

[32] Control Objectives for Information and related Technology - Version 4.1, 2007 - IT Governance Institute (www.itgi.org)

[33] U.S. House of Representatives. 2002. The Sarbanes-Oxley Act of 2002. Public Law 107-204 [H.R.3763]. Washington, D.C.: Government Printing Office.

[34] IT Assurance Guide - Using CobiT - 2007 - IT Governance Institute (www.itgi.org)

[35] ASAE 3402 – International Standard on Assurance Engagements [ASEA] - Assurance reports on Controls at a Service Organization

[36] Federal Financial Institutions Examination Council [FFIEC] - Business Continuity Planning March 2008 IT Examination Handbook

Appendix A: Business Continuity Management Glossary

Alternate Site Test / Exercise	A business continuity testing activity that tests the capability of staff, systems, and facilities, located at sites other than those generally designated for primary processing and business functions, to effectively support production processing and workloads. During the exercise, business line staff located at recovery site(s) participate in testing business functions and the supporting systems by performing typical production activities, including accessing applications and completing pending transactions. Staff members participate in testing alternate site facilities through the use of PCs, phones, and other equipment needed to perform testing of business activities [36]
Back-up Generations	A tape rotation methodology that creates three sets of back-up tapes: daily incremental sets or “sons,” weekly full sets or “fathers,” and end-of-month tapes or “grandfathers.” This back-up methodology is frequently used to refer to master files for financial applications.
Business Continuity Plan (BCP)	A comprehensive written plan to maintain or resume business in the event of a disruption. BCP includes both the technology recovery capability (often referred to as disaster recovery) and the business unit(s) recovery capability
Business Continuity Strategy	Comprehensive strategies to recover, resume, and maintain all critical business functions.
Business Continuity Test	A test of an institution’s disaster recovery plan or BCP.
Business Impact Analysis (BIA)	The process of identifying the potential impact of uncontrolled, non-specific events on an institution's business processes.
Business Recovery Test / Exercise	An activity that tests an institution’s BCP.
Call Tree	A documented list of employees and external entities that should be contacted in the event of an emergency declaration.
Change Management	The process of ensuring that changes to the IT environment are planned, documented, and authorized. The impact of changes on business continuity and disaster recovery processes should be factored into an institution’s change management processes.
Checklist Review	A preliminary procedure to testing that employs information checklists to

	guide staff activities. For example, checklists can be used to verify staff procedures, hardware and software configurations, or alternate communication mechanisms.
Component	An element or part of a business process.
Component Test / Exercise	A testing activity designed to validate the continuity of individual systems, processes, or functions, in isolation. For example, component tests may focus on recovering specific network devices, application restoration procedures, off-site tape storage, or proving the validity of data for a particular business line.
Connectivity Testing	A testing activity designed to validate the continuity of network communications.
Crisis Management	The process of managing an institution's operations in response to an emergency or event which threatens business continuity. An institution's ability to communicate with employees, customers, and the media, using various communications devices and methods, is a key component of crisis management.
Crisis Management Test / Exercise	A testing exercise that validates the capabilities of crisis management teams to respond to specific events. Crisis management exercises typically test the call tree notification process with employees, vendors, and key clients. Escalation procedures and disaster declaration criteria may also be validated.
Critical Path	The critical path represents the business processes or systems that must receive the highest priority during the recovery phase.
Custom Redirect Service	This service enables control over the location of incoming calls or the redirection of calls to various locations or pre-established phone numbers to ensure customer service continuity.
Database	A database represents the collection of data that is stored on any type of computer storage medium and may be used for more than one purpose.
Data Mirroring	A back-up process that involves writing the same data to two physical disks or servers simultaneously.
Data Replication	The process of copying data, usually with the objective of maintaining identical sets of data in separate locations. Two common data replication processes used for information systems are synchronous and asynchronous mirroring.

Data Synchronization	The comparison and reconciliation of interdependent data files at the same time so that they contain the same information.
Disaster Recovery Exercise	A test of an institution's disaster recovery or BCP.
Disaster Recovery Plan	A plan that describes the process to recover from major processing interruptions.
Disk Shadowing	A back-up process that involves writing images to two physical disks or servers simultaneously.
Electronic Vaulting	A back-up procedure that copies changed files and transmits them to an off-site location using a batch process.
Emergency Plan	The steps to be followed during and immediately after an emergency such as a fire, tornado, bomb threat, etc.
End-to-End Recoverability	The ability of an institution to recover a business process from initiation, such as customer contact, through process finalization, such as transaction closure.
Enterprise-Wide	Encompassing an entire organization, rather than a single business department or function.
Frame Relay	A service provided by telecommunications companies that connects local area networks to regional or national backbone networks.
Full-Interruption/ Full-Scale Test (IT and Staff)	A business continuity test that activates all the components of the disaster recovery plan at the same time. Hardware, software, staff, communications, utilities, and alternate site processing should be thoroughly tested in this type of testing activity. The exercise should include the business line end users and the IT group to ensure that each business line tests its key applications and is prepared to recover and resume its business operations in the event of an emergency. The full test verifies that systems and staff can recover and resume business within established recovery time objectives. End users should verify the integrity of the data at the alternate site after the IT group has restored systems and applications needed for the staff to perform production activities.
Functional Drill/Parallel Test	This test involves the actual mobilization of personnel at other sites in an attempt to establish communications and coordination as set forth in the BCP.

Functionality Testing	A test designed to validate that a business process or activity accomplishes expected results.
Gap Analysis	A comparison that identifies the difference between actual and desired outcomes.
Hierarchical Storage Management (HSM)	HSM is used to dynamically manage the back-up and retrieval of files based on how often they are accessed using storage media and devices that vary in speed and cost.
HVAC	Acronym for heating, ventilation, and air conditioning.
Integrated Test / Exercise	This integrated test/exercise incorporates more than one component or module, as well as external dependencies, to test the effectiveness of the continuity plans for a business line or major function.
Interdependencies	Interdependencies Where two or more departments, processes, functions, and/or third parties support one another in some fashion.
Media	Physical objects that store data, such as paper, hard disk drives, tapes, and compact disks (CDs).
Modeling	The process of abstracting information from tangible processes, systems and/or components to create a paper or computer-based representation of an enterprise-wide or business line activity.
Module	A combination of various components of a business process or supporting system.
Module Test / Exercise	A test designed to verify the functionality of multiple components of a business line or supporting function at the same time.
Network Attached Storage (NAS)	NAS systems usually contain one or more hard disks that are arranged into logical, redundant storage containers much like traditional file servers. NAS provides readily available storage resources and helps alleviate the bottlenecks associated with access to storage devices.
Recovery Point Objectives (RPOs)	RPOs represent the amount of data that can be lost without severely impacting the recovery of operations or the point in time in which systems and data must be recovered (e.g., the date and time of a business disruption).
Recovery Site	An alternate location for processing information (and possibly conducting business) in an emergency. Usually distinguished as “hot” sites that are

	fully configured centers with compatible computer equipment and “cold” sites that are operational computer centers without the computer equipment.
Recovery Time Objectives (RTOs)	RTOs represent the maximum allowable downtime that can occur without severely impacting the recovery of operations or the time in which systems, applications, or business functions must be recovered after an outage (e.g. the point in time that a process can no longer be inoperable).
Recovery Vendors	Organizations that provide recovery sites and support services for a fee.
Remote Access Capabilities	The ability to obtain access to a computer or network from a remote distance.
Remote Control Software	Software that is used to obtain access to a computer or network from a remote distance.
Remote Journaling	Process used to transmit journal or transaction logs in real time to a back-up location
Resiliency	The ability of an organization to recover from a significant disruption and resume critical operations.
Resiliency Testing	Testing of an institution’s business continuity and disaster recovery resumption plans.
Risk Assessment	A prioritization of potential business disruptions based on severity and likelihood of occurrence. The risk assessment includes an analysis of threats based on the impact to the institution, its customers, and financial markets, rather than the nature of the threat.
Routing	The process of moving information from its source to a destination.
SAS 70 Report (from 2011 – ISAE 3402)	An audit report of a servicing organization prepared in accordance with guidance provided in the American Institute of Certified Public Accountants’ Statement of Auditing Standards Number 70.
Simulation	The process of operating a model of an enterprise-wide or business line activity in order to test the functionality of the model. Computer systems may support the simulation of business models to aid in evaluating the BCP.
Simulated Loss of Data Center Site(s) Test / Exercise	A type of disaster recovery test that involves the simulation of the loss of the primary, alternate, and/or tertiary data processing sites to verify that the institution can continue its data processing activities.

Sound Practices	Defined in the “Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System,” which was issued by the Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and Securities and Exchange Commission.
Split Processing	The ongoing operational practice of dividing production processing between two or more geographically dispersed facilities.
Storage Area Network (SAN)	SAN represents several storage systems that are interconnected to form one back-up network, which allows various systems to be connected to any storage device and prevents dependence on a single line of communication.
Sustainability	The period of time for which operations can continue at an alternate processing facility.
Synchronous Data Replication	A process for copying data from one source to another in which an acknowledgement of the receipt of data at the copy location is required for application processing to continue. Consequently, the content of databases stored in alternate facilities is identical to those at the original storage site, and copies of data contain current information at the time of a disruption in processing.
Table Top Exercise/ Structured Walk-Through Test	A preliminary step in the overall testing process that may be used as an effective training tool, but not as a preferred testing method. This is a test in which employees review and discuss the processes to be followed during specific contingency scenarios. Generally, these exercises are conducted with all participants in the same room. Key decision makers may be placed in role playing situations to follow specific steps in the disaster recovery plan. The objective is to test the participant’s knowledge of the procedures, identify any potential gaps in the plan, and evaluate the plans to respond to various events.
Terminal Services	A component of Microsoft Windows operating systems (both client and server versions) that allows a user to access applications or data stored on a remote computer over a network connection.
Test Assumptions	The concepts underlying an institution’s test strategies and plans.
Test Plan	A document that is based on the institution’s test scope and objectives and includes various testing methods.
Test Scenario	A potential event, identified as the operating environment for a business continuity or disaster recovery test, which the institution’s recovery and resumption plan must address.
Test Scripts	Documents that define the specific activities, tasks, and steps that test

	participants will conduct during the testing process.
Test Strategy	Testing strategies establish expectations for individual business lines across the testing life cycle of planning, execution, measurement, reporting, and test process improvement. Testing strategies include the testing scope and objectives, which clearly define what functions, systems, or processes are going to be tested and what will constitute a successful test.
Transaction Testing	A testing activity designed to validate the continuity of business transactions and the replication of associated data.
Two-way Polling	An emergency notification system that allows management to ensure that all employees are contacted and have confirmed delivery of pertinent messages.
UPS	UPS is an acronym for uninterruptible power supply, which typically represents a collection of batteries that provide electrical power for a limited period of time.
Utility programs	A program used to configure or maintain systems, or to make changes to stored or transmitted data.
Virtual Private Network (VPN)	A network where data is transferred over the Internet using security features preventing unauthorized access.
Voice over Internet Protocol (VoIP)	The transmission of voice telephone conversations using the Internet or Internet Protocol networks.
Walk-Through Drill/Simulation Test	This test represents a preliminary step in the overall testing process that may be used for training employees but not as a preferred testing methodology. During this test, participants choose a specific scenario and apply the BCP to it.
Wallet Card	Portable information cards that provide emergency communications information for customers and employees.
Wide-Scale Disruption	An event that disrupts business operations in a broad geographic area.