Selection and Implementation of the ISO 38500 Governance Framework

Michael Boyle

Glossary

Application Governance: The phrase literally means the management and control of all software programs. For this particular exercise, a reference is being made to the documentation created to manage the bespoke software

Application Portfolio: An inventory of all deployed enterprise software, including a high-level description of the content which is to be found within the respective governance agreements.

CAB: Change Advisory Board, one or more individuals who either assist with approval or prioritization or actually perform the actions therein.

CCTA: Acronym for the Central Computer and Telecommunications Agency, this British government ministry who were assigned the task of creating the ITIL framework.

CMS: Acronym for Content Management System

COBIT: Acronym for Control Objectives for Information and Related Technology, the term refers to the framework established by the ISACA to manage IT governance.

Framework: The literal definition concerns a skeletal structure designed to support or enclose something. Within this document, one is referring to the foundation by which application governance agreements are to be constructed.

ICT: Acronym for Information and Communication Technology

Interface: The interaction between components, applicable to either software or hardware

ITIL: Acronym for IT Infrastructure Library, this framework was created by the CCTA to create the ITIL framework

ISACA: Originally an acronym for Information System Audit and Control Association, the organization concerns itself with IT Governance and refers to itself solely under the acronym due to the broadened activity scope.

ISO: Acronym for International Organization for Standardization, this global public assembly is the largest developer and publisher of international standards

ISO38500: The official name of this framework is ISO/IEC 38500:2008 and involves the standard applied to information technology corporate governance.

KPI: Acronym for Key Performance Indicator, one refers to the items which allow for metrics to be measured in a quantifiable manner.

Methodology: Organizational business rules and postulates applied to the governance framework selected.

RACI: Acronym For Responsible, Accountable, Consulted and Informed. This terminology is used to determine the roles individuals hold within a responsibility matrix

SaaS: Acronym for Software as a Service, one refers to software applications accessible via the internet

Service Catalogue: A catalogue of services performed for either internal or external customers.

SLA: Acronym for Service Level Agreement. This term denotes the commitment made by ICT to adhere to certain levels of performance.

Third-party suppliers: An external software house creating applications being utilized within the enterprise.

Table of Contents

Glossary 2
Introduction: 4
What is Portfolio Management? 5
Goals and Objectives 6
Goals 6
Objectives 9
Analysis and Selection Process 10
Framework Interpretation 12
Standard Content 13
Application Content 17
Deployment 22
Lessons Learned 24

Introduction:

One of the most challenging assignments within an organization is establishing of a maturity model structure in order to optimize enterprise effectiveness. The contents of this paper concern such an assignment. The objective of this mission entailed the establishment of an application governance model and the corresponding documentation therein.

This document should provide a high-level description of the goals and objectives of the exercise performed, the analysis methodology applied and the corresponding selection criteria chosen. In addition, the methodology deployed within the framework selected, a description of deployment and post-deployment actions and the lessons learned throughout this project will also be described.

What is Portfolio Management?

Depending on the operational domain, the term Portfolio Management can be used to describe disparate functions. Considering such, it is worthwhile to describe the authority of activities as such in order to understand the context of this undertaking. In context of this paper, major activities of this department include

- Business requests for automated functionality to fulfill particular business needs. Such requests can be for internal or external (e.g. client-based) purposes.
- A review of the existing application inventory to ensure that the portfolio is optimized
- An assessment of the existing application governance agreements to determine if indeed an application within the portfolio has the technical capability to cover the functionality requirements through additional development.
- If no application exists within the portfolio meeting the bespoke requirements, the business is required to provide a validated business need in alignment with the enterprise goals. A corresponding business case is supplied at a later stage.
- Analysis is performed in order to determine whether the application should either be purchased or internally developed (build or buy).
- The inclusion of the application within the portfolio with the corresponding governance agreement.
- A periodic comparison between the service catalogue and the supporting portfolio applications in order to ensure optimization.

The underlying goal of the Portfolio Management department is financial in nature. Unneeded development, a reduction and eventual elimination of redundant applications, an emphasis on standardization and a concentration on the total cost of ownership (e.g. infrastructure, resources, licenses, etc.) are all actions that add to the overall financial viability of an organization.

A streamlined application portfolio directly relates in:

- lower costs (support, license, training, documentation, servers)
- better applications through a focus on quality
- better requirements through alignment with enterprise goals
- Better documentation as this element becomes a major tenet of the organization.

Goals and Objectives

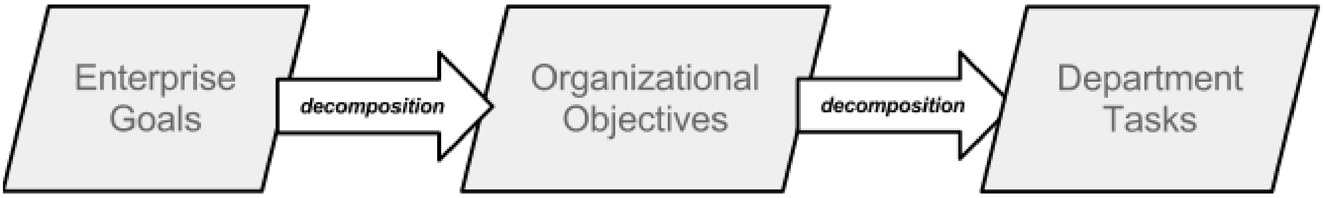
Goals

The goal from a Portfolio Management perspective was to ensure that the department could properly fulfill the duties assigned.

Establishment of a clear understanding of the roles and responsibilities between the business and ICT was the first priority. Upper management was very keen to profess an unambiguous statement tied to ICT's role in how it would support the organization as well as ensure that and all activities should be focused in this direction.

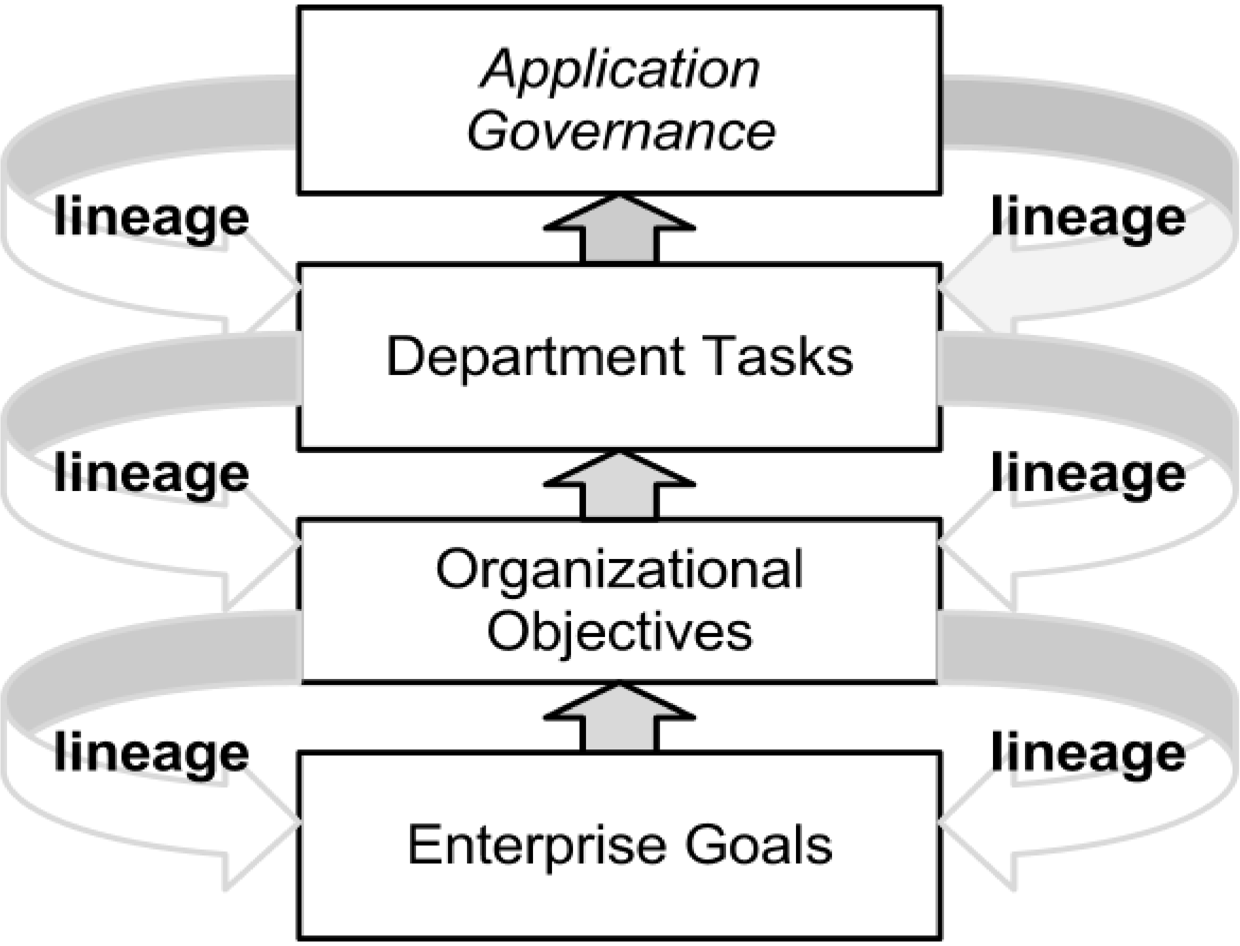
The ability to trace all services and their corresponding processes needed to be established in order to ensure adherence of the organizational goals enterprise-wide.

Figure 1 - Enterprise Goal Traceability



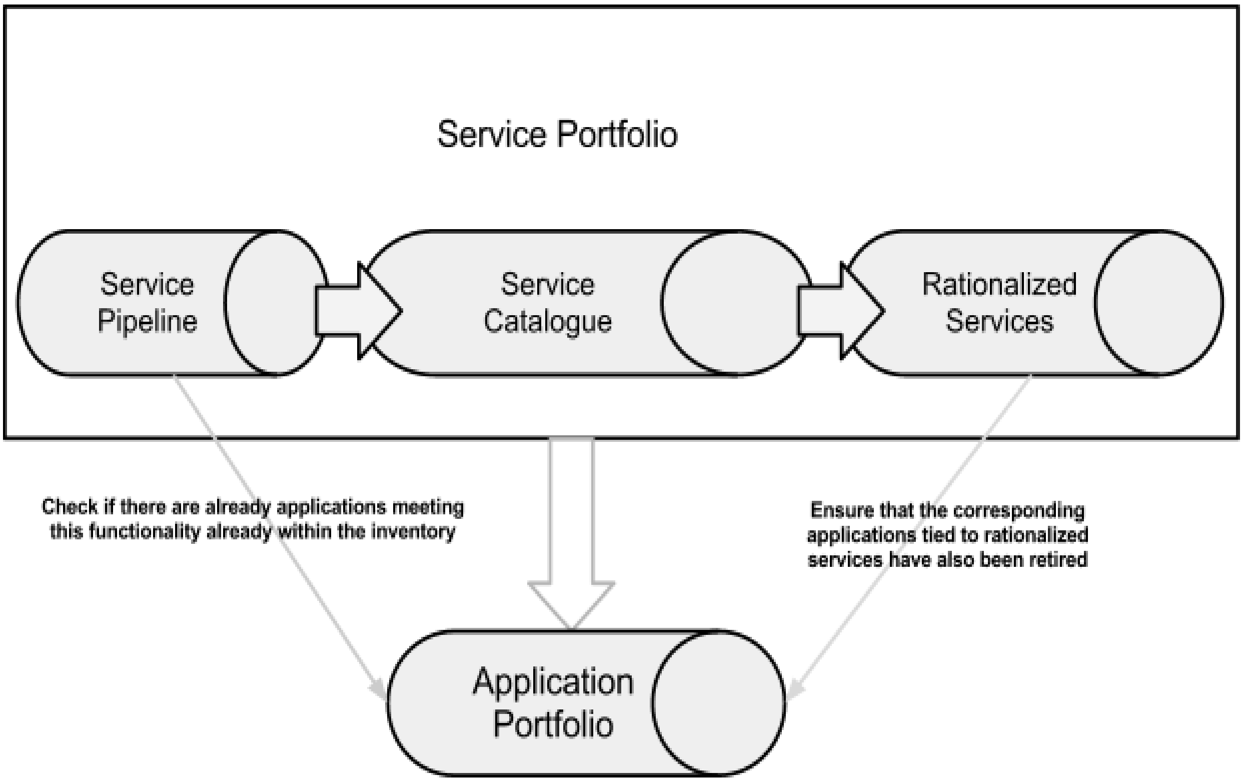
In the figure below, one can follow the lineage between between application governance and the bespoke goals. The described is an indispensable business rule ensuring the highest probability of reaching alignment.

Figure 2 - Relation of Application Governance to Enterprise Goals



One finds a similar lineage professed by ITIL, where the application portfolio is associated with the corresponding enterprise services.

Figure 3 - Relation between the Service and Application Portfolio


Service Portfolio
Service Pipeline
Service Catalogue
Rationalized Services
Check if there are already applications meeting this functionality already within the inventory
Ensure that the corresponding applications tied to rationalized services have also been retired
Application Portfolio

No application portfolio content should exist without a corresponding service catalogue equivalent. This concept is in clear alignment with two clear positions to be found within the organization:

1. Technology is only a tool to support business needs
2. Alignment between the service catalogue and application portfolio functionality is imperative.

Objectives

The Portfolio Management department objectives were very clear:

- Procedural standardization: a uniform procedure was critical if the goals in question were to be achieved.
- Unambiguous responsibility definitions.
- A clear depiction of all technical components tied to an application: The contents should include the application architecture, infrastructure configuration, operating system, programming language, rights and role management, security provisions among others.
- A well-formed listing of each application’s functionality following a business vetting and validation. Alone the argument tied to an application offering a specific functionality does not infer its inclusion to be in the organization’s best interest.
- A thorough listing of all the technical interfaces relating to the application in question
- An exact definition of the configuration standard per application
- A proper requirements management process that takes into consideration any of the process deviations due to the involvement of third party suppliers.
- Clear-cut procedures tied to all issues tied to application performance
- Establishment of proactive business rules to properly react to regulatory, contractual, competitive or supplier-based requirements that are directly related both the service catalogue and the supporting application portfolio.
- A clearly defined implementation and release-based deployment process. Due to the use of 3rd parties and the reliance of customer procedural requirements, one could possibly be required to make differentiations per application.

The deployment of a standardized application governance agreement allows the organization to classify their process assets in a systematic fashion, allowing for Portfolio Management to properly align the service catalogue with the content to be found within the application portfolio.

Analysis and Selection Process

The methodology deployed for this undertaking was comprised of the following tasks:

- Research and collect all pertinent frameworks applicable
- Analyze the frameworks in question; looking for similarities, contradictions, duplications as well as identify any lack of clarity therein
- Group the data based on the categories listed
- Establish priorities based on the actual business need and purpose of the exercise

Based on the tasks listed above, the following reference documentation was selected for review

ITIL v3
COBIT 4.1
ISO 38500:2008

One can find basic similarities between the three frameworks in question. The overarching framework objectives were deemed to be comparable, but the underlying needs as listed under the organizational goals became the critical selection indicators.

ITIL v3

This framework had already been deployed as a base within the organization, but it was clear from the outset that it was not sufficient as a governance framework. ITIL's credo is based on viewing all actions from the customer perspective, but the the framework was too limiting for that what was to be accomplished.

COBIT 4.1

Again, the focus of this framework was sound, but the overriding need to ensure that documentation be depicted from the business perspective eliminated the viability of this option.

During our research, the following description provided by ISACA lead credence to the departments convictions

"ISO 38500 Vs. COBIT Vs. ITIL
ISO 385001 looks down from the top, much like a roof on a house. COBIT (the what) is the walls, and process frameworks such as ITIL and Projects in Controlled Environments 2 (PRINCE2) (the how) are the foundation. Using the house analogy, if the board tried to implement the roof, ISO 38500, without the foundation or walls, it would collapse. Furthermore, without the roof, enterprises would be exposed to the elements. ISO 38500 is not one size fits all. It does not replace COBIT, ITIL, or other standards or frameworks, but, rather, it complements them by providing a demand-side-of-IT-use focus."

In addition, both the ITIL and COBIT frameworks were found to be focused on an overall approach, and our need was to focus solely on the the applications.

Another prevailing factor was the actual source of the frameworks. The organization professed the desire to adhere to ISO standards when and where possible. For this reason, the selection of ISO38500 was seen as being complementary.

The following statement from ISO38500 described very well the intention of this initiative.

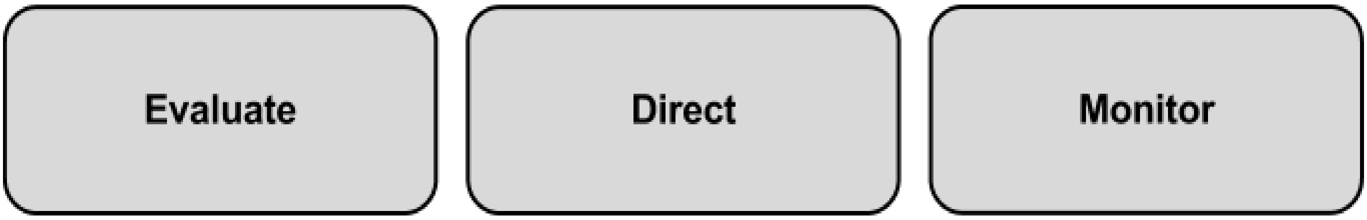
“The ISO has depicted ISO38500 to be a high-level, principled-based advisory standard in nature with the intention of providing guidance for organizations to underpin the governance of IT. The objective of this undertaking is to provide a framework for Enterprise Directors for use in evaluating, directing and monitoring the use of IT within their corporations (ISO/IEC 38500:2008 p. IV-V). “

Our framework interpretation was intended to establish a methodology which would allow for the coverage of all internally and externally-produced software. Such documentation should be applicable, regardless whether the use is within the corporation, applied by external clients, our suppliers or by our client’s suppliers where our organization has established an interface.

Framework Interpretation

After the framework selection was made, it was of utmost importance to concentrate on the transformation from a framework-based to a methodology-based, business rules driven template.

Figure 4 - Governance Model



Evaluate the current setup in order to determine what needs to change and how. The exercise was, first of all, intended to provide transparency.
Direct the preparation and perform the implementation of that what was agreed-upon.
Monitor that of what was agreed-upon and deployed and ensure it is working as intended.

One should not discount the importance between

- The process tied to the original production, code correction, functionality change request and the corresponding release management required
- The interaction between the various stakeholders tied to the usage of the bespoke application
- The roles and responsibilities of all stakeholders identified
- The relation that one application has to numerous other pieces of software and the potential complications which can result through any possible code or configuration changes
- any legal, contractual, market-based or supplier-based requirements and the measures required by an organization
- The deployment requirements and the speed and manpower required to complete the endeavour

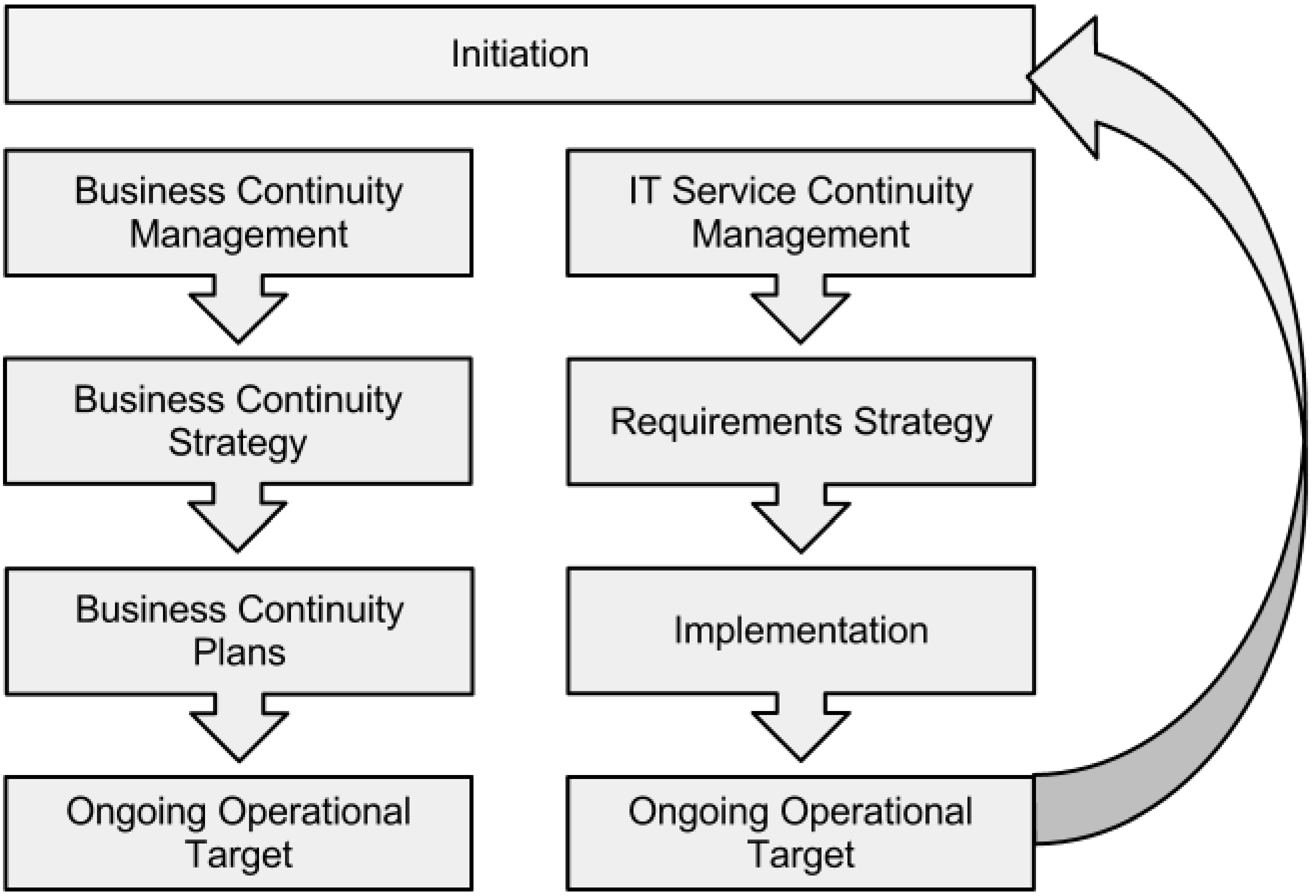
Standard Content

The following content was seen to be standard from the start of the exercise:

- Business Rules pertaining to the exercise ‘build or buy’
- The prioritization criteria established for development change requests
- A common Incident classification for all applications
- Application conformance objectives tied to environmental factors such as government or industry standards, client commitment, etc.
- Business Continuity Strategy

Due to the fact that the applications within the portfolio rely without exception to a proper IT service continuity management, it is important to review both domains, including their relationship to each other

Figure 5 - Business Continuity Model

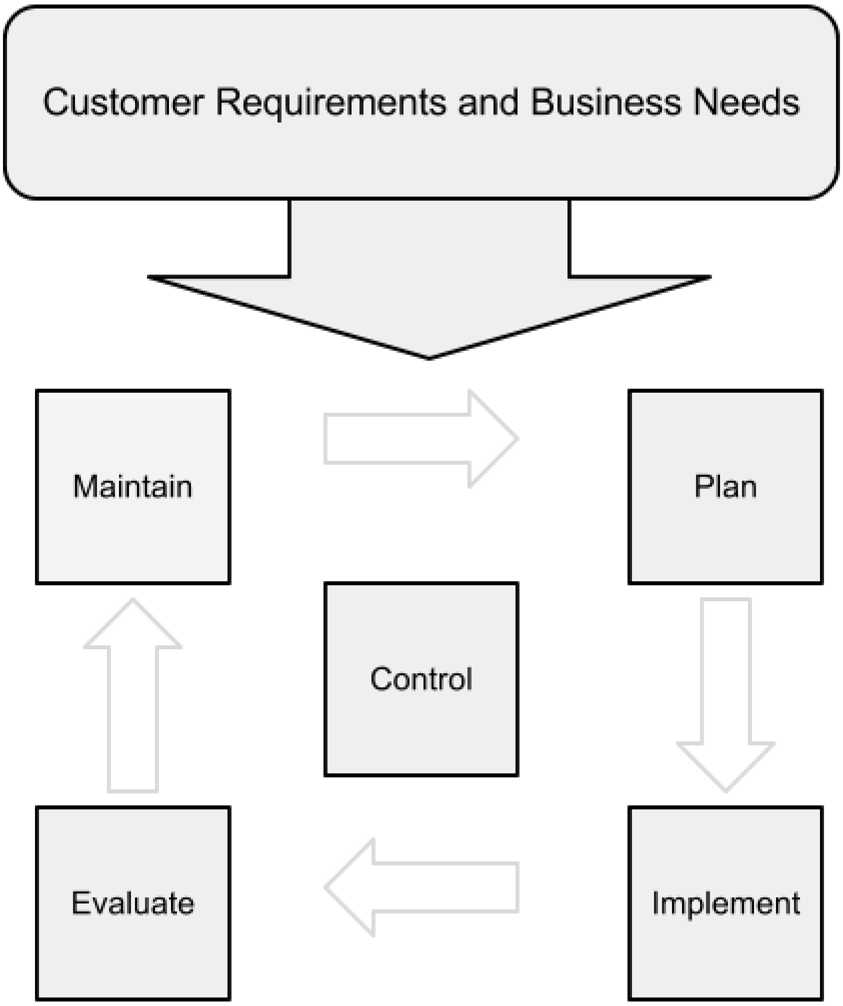

Initiation
Business Continuity Management
IT Service Continuity Management
Business Continuity Strategy
Requirements Strategy
Business Continuity Plans
Implementation
Ongoing Operational Target
Ongoing Operational Target

- Application Security

The major tenet of application security was to concentrate on the following elements

  - Data Confidentiality: Safeguards were required inside and outside the enterprise
  - Data Integrity: A clear priority was established to ensure that data not be corrupted
  - Application Availability: Depending on the application in question, clear SLA's needed to be established and adhered to
  - Application Authenticity: The organization needed to ensure that content be displayed based on the correct rights and roles prescribed by the business

Figure 6 - Application Security Model



The figure depicted above is a standard procedure to be found within a typical application security model.

- Requirements Management

The tasks listed below were found to be applicable to all applications

- *Process for Requirements Gathering*
    - a. Is this the right application for such functionality?
    - b. Who needs to approve changes? Depending on the application, there might be numerous parties who need to be included in such a decision.
    - c. How is the data to be documented?
        - i. Requirement Identifier: a unique number should be assigned to each requirement for reference purposes
        - ii. Who placed the requirement request?
        - iii. From whom did the request come from? Who originated the request. The person placing the request could be different
    - d. Complexity and scale of the request
        - i. Ownership – who requires the change?
        - ii. Requirement Priority
        - iii. Requirement Status: proposed, accepted, verified, postponed, cancelled, implemented
    - e. Business Need Business need needs to be before the business case as there is no need to build a case if there is no need
        - i. define the problem or opportunity
        - ii. describe the desired outcome
        - iii. solution scope
    - f. Capability Gaps:
        - i. What is currently missing within the application
        - ii. What effort is required – work estimate
    - g. Impact Analysis
        - i. Application architecture
        - ii. Interfaces
        - iii. Organizational readiness
    - h. Define Assumptions and Constraints
    - i. Business Case: there is a clear difference between business need and business case. The former concerns the necessity. The latter covers the justification.
    - j. Requirement Priority results out of this?
    - k. Business Objectives
        - i. Documentation needs to be SMART
            1. Specific: describing something that has an observable outcome
            2. Measurable: tracking and measuring the outcome
            3. Achievable: testing the feasibility of the effort
            4. Relevant: in alignment with the organization's key vision, mission, goals
            5. Time-bounded: the objective has a defined timeframe that is consistent with the business need
    - l. Verify requirements: were the statements made in the requirements correct?

m. Validate requirements: Did the requirements properly define the need?

After the change has been approved, the transition requirements needed to be defined.

- Communication Management

Below the standard communication process is depicted:

1. Identify Stakeholders
    a. Use of RACI Matrix
        i. Who is responsible for the application release?
        ii. Who is accountable for the application release?
        iii. Who needs to be consulted within an application release cycle?
        iv. Who needs to be informed within an application release cycle?
2. Define communication structure and scheduling
3. Define types of communication: Ideally, communication is formulated in a certain way to convey only the pertinent information relevant to a particular stakeholder.
4. Influencing factors in communication deployed
    a. Geography
    b. Culture
    c. Frequency required
    d. Formality necessitated
5. Communication tied to the application release
    a. Requirements gathering and documentation
    b. Prioritization
    c. Change request approval process
    d. Development
    e. Testing
    f. Production

As previously mentioned, ICT had already set up ITIL v3 as an operational standard. It was therefore expedient to use that of what had already been established.

Application Content

The elements listed below were deemed to be too application-specific to be standardized due to

- The actors involved in the respective sessions
- The level of detail required by the application per se
- The scope of the application deployment, be it country, regional or global deployment

Responsibility Matrix

Below is a general listing of the positions that could be included under an extended responsibility matrix:

Planning
Investment Planning and Market Strategy
Portfolio Management
Release Management
Business Requirements
Product Communication

Development
Design
Coding

Testing
Quality Assurance

Implementation
Rollout
Configuration
Training (internal and external)

Post-Implementation Support
1st Level
2nd Level
3rd Level

ICT Operations Manual

The content of this section should include a clear depiction of all technical components tied to an application, including the application architecture, infrastructure configuration, operating systems, programming language, rights and role management, security provisions and the like.
Application Catalogue

Intended is not a listing of all functionality an application can offer, but rather that what the business has decided to deploy. All content modifications would require a corresponding change request process to be followed.

Application Interfaces

This section should entail a thorough listing of all the technical interfaces relating to the application in question.

Configuration Standard

This area must include an exact depiction of the application configuration standard.

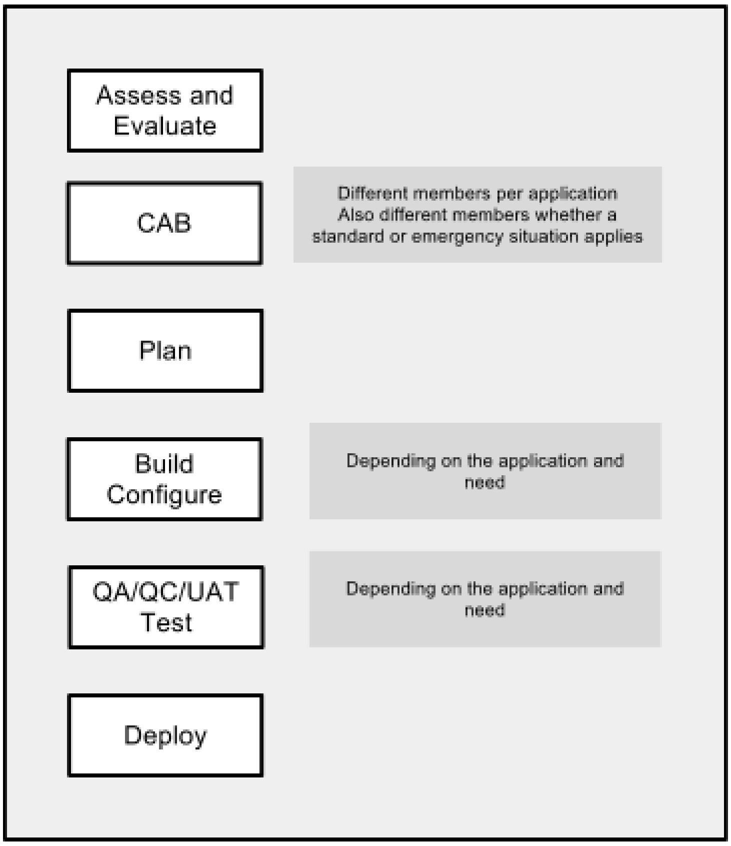
Change Management

Here a clear differentiation between development and configuration change management was made. Such a configuration entails various elements, such as:

- A Configuration Standard modification.
- Exception Management
- Patch Management
- Problem Management

to name just a few

Figure 7 - Change Management Model


Assess and Evaluate
CAB
Different members per application Also different members whether a standard or emergency situation applies
Plan
Build Configure
Depending on the application and need
QA/QC/UAT Test
Depending on the application and need
Deploy

The figure above characterizes the general process to be followed. Depending on the application in question, different actors and/or different steps could be added or deleted.

Application escalation process

Although an overall four-level escalation process would be adhered to, the actors could be very different depending on whether a 3rd party supplier is involved. External factors also affect the means by which the escalation is performed.

Conformance

This section should include a research of legal and contractual requirements. Sources for such information should be Legal, Controlling and Account Management. Depending on the issue at hand, a process needs to be established in order to perform conformance.

Due to the necessity to be proactive towards all matters tied to regulatory, legal and commercial obligations, Portfolio Management had been defined as being responsible for reaching out to the necessary internal departments (e.g. legal, controlling) as well as outside sources (e.g. Technology Business Research Units such as Gartner) in order to stay abreast of possible issues in advance.

As any application in question could be affected by a number of conformance issues, the following governance model definition would apply:

Evaluate: Describe the issue and how the application is affected. A characterization of the measures taken to counteract the issue will be catalogued, including any and all supporting documentation necessary.

Direct: An actions registry comprising the evaluation elements performed must be compiled. This registry should include a validity time frame if so applicable.

Monitor: The processes to be followed must also be documented in order to periodically validate the effectiveness of the measurements deployed.

Application implementation process

Again, the actors could be very different depending whether a 3rd party supplier is involved. Very often, the actual implementation is being maintained by the external vendors. This infers that the processes could be different with every application.

Release and deployment management

Depending on the application in question, the three deployment concepts are specified for categorization purposes. The actual process as such should be clearly stated:

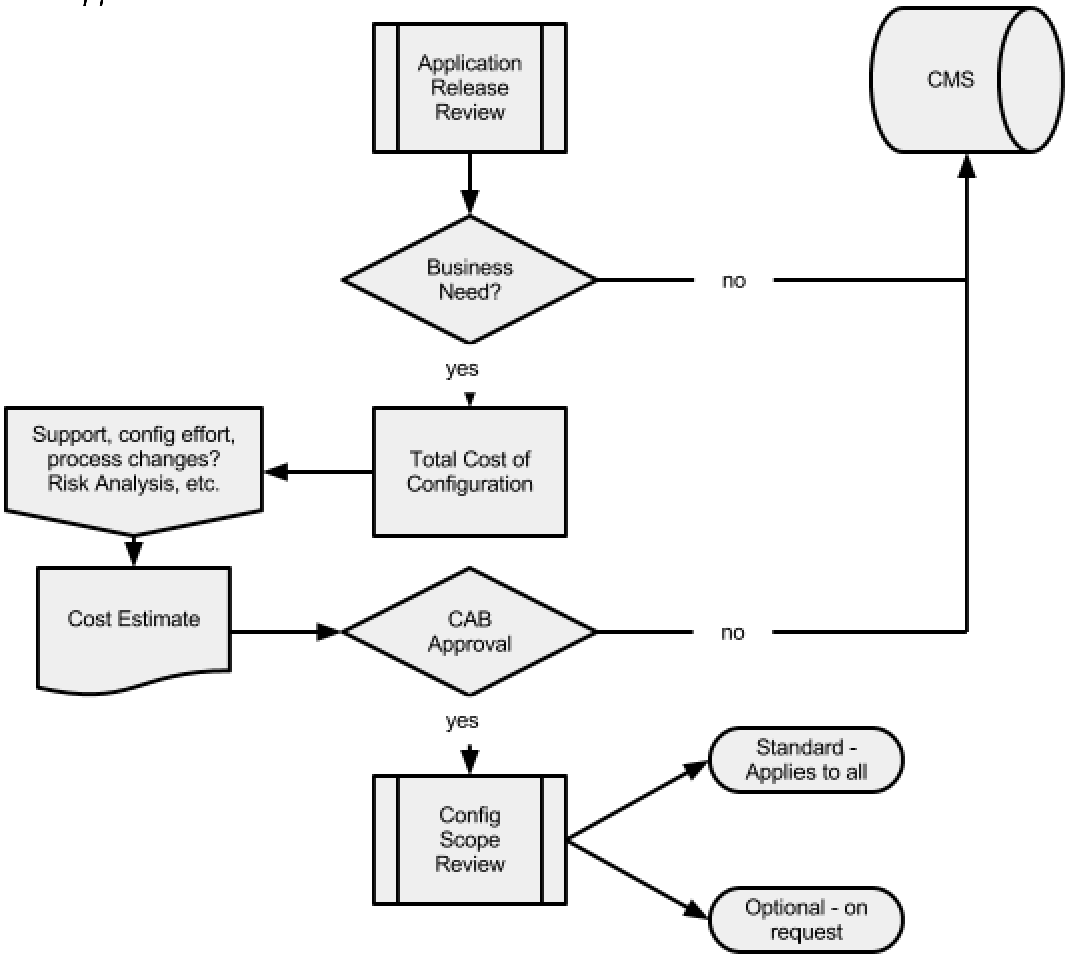
- Automated vs. Manual: Depending on the application in question, either an automatic or a manual installation to all qualified end users will be deployed.
- Push vs. Pull: In certain cases, an end user will be empowered to retrieve the software in question from a portal (pull) and perform the deployment directly. Otherwise, ICT resources will be required to push the data to the respective end users via an automated or manual deployment.
- Phased vs. Big Bang: Assuming the software installation will be managed by ICT services, a decision must be made as to whether the deployment must take place in stages (phased) or can be completed at once (big bang).

Application Release Deployment

The vast majority of the applications in question are managed by 3rd party software houses that work under their own release schedule. It is very seldom that the organization has the ability to pass on requirements. More often than not, a new version of a software is simply released. In those cases where the software is to be deployed on an end-user's desktop, IT Services manages the deployment directly. The depiction below is tied solely to internet-based applications.

Software Upgrades: For SaaS applications, more often than not an upgrade option does not exist. If the 3rd party supplier upgrades their software, the end user automatically has access to the newest version. Regardless, the deployment of particular functionality within a release should always be optional. Once the new release has taken place, the standard configuration setting for the bespoke functionality should automatically be set on *NO* with the option to activate at a later stage.

Figure 8 - Application Release Model


Application Release Review
CMS
Business Need?
no
yes
Support, config effort, process changes? Risk Analysis, etc.
Total Cost of Configuration
Cost Estimate
CAB Approval
no
yes
Standard - Applies to all
Config Scope Review
Optional - on request

Deployment

Within the initial application governance agreement submitted, the ISO38500 principle names were used with one notable exception. Principle 6 - Human Behaviour was replaced with the title *Implementation*. The reasons for this decision were two-fold:

- It was felt that the subject matter (human behaviour) was not directly relevant to the application governance agreement intent.
- Due to the complexity of certain application deployments, the department felt the subject of implementation should be categorized separately.

The application governance agreement template index was presented as follows:

- Preamble
- Responsibility
    - Responsibility Matrix
- Strategy
    - ICT Operations Manual
    - Application Catalogue
    - Application Interfaces
    - Application Configuration Standard
- Acquisition
    - Application Requirements Management Process
    - Application Communications Management Process
    - Business Case Template
    - Prioritization Matrix for Development Releases
    - Change Request Process - Standards Change
- Performance
    - Application Support Process
    - Incident Management Matrix
    - Application Escalation Process
    - Application Security
    - Business Continuity
- Conformance
- Implementation
    - Application Implementation Process
    - Application Release Management Process

Within the bespoke index, the governance model Evaluate - Direct - Monitor was clearly applied under each item.

Example: Responsibility Matrix

Evaluate:

- Identify all parties responsible for an application.
- Verify that the individuals/departments are responsible for the tasks recognized.
- Ensure that all necessary documentation is validated.
- Establish metrics and the corresponding KPIs in order to properly gauge the effectiveness of the responsibility matrix.

Direct:

- Validate with executive management that the individuals/groups denoted hold the responsibility to complete the actions as stated. With this action, the executive management declare themselves accountable for the respective workings of the application in question.

Monitor:

- A periodic governance review would be scheduled with all important stakeholders.
- The KPIs would be reviewed to measure the viability of that of what was agreed.
- The KPIs should include the ability to trace application relevance to the enterprise goals.

The application governance agreement was validated by all relevant stakeholders after completion and was swiftly earmarked for deployment. Various means of communication were distributed throughout the organization, and application governance training sessions were performed for those individuals who would be completing documentation.

It was decided that specific user groups be established within the governance repository. Both overall application governance awareness and data confidentiality needed to be achieved, and content rights management was deployed as the vehicle to accommodate this need.

Lessons Learned

As is often the case, one is confronted with unique, unforeseeable experiences throughout such a project. Fortunately, none were negative by nature, and the organization, by and large, found the initiative to be beneficial.

Below are listed some of the lessons learned from this initiative:

- Once documentation was being collected for the respective applications, it was apparent that further process standardization was easily achievable. Many of the process differences per application were either minimal or not required.
- The resistance of 3rd party suppliers to provide the requested information was not a complete surprise, but the vehemence in certain cases was not expected.
- Application governance agreement completion took much longer than expected. The responses collected begat other organizational initiatives, which invariably caused delays to the agreements. Regardless, the 'ripple effect' of the undertaking was overall a positive one.
- One should not underestimate the politics associated with such an initiative. The transparency provided by this effort was not in everyone's interest, and this feeling was made known in very clear terms.
- The completion of such an agreement was a change in organizational approach, and consequently the amount of change management required was underestimated. Portfolio Management looked at the agreement documentation as an exercise, but in fact the exercise held more the attributes of a project.
- For fear this assertion might be taken as being an understatement, the support of executive management was crucial towards the success of this endeavour. Certain pockets of resistance were not expected, and enterprise backing was required on numerous occasions.