GEST-H510 Gourvernance of entreprise IT

> *The following is a desperate attempt to extract information from the course material.*

1. Digital transformation drivers

Organizational barriers to digital transformation in terms of:

1. Entreprise architecture
2. Program management / Project delivery
3. Vision and strategy

1.1 Enterprise architecture

Managing entreprise architecture

Systems get more complex and sophisticated

Some examples of complex systems [...]

Data pipeline

Components of entreprise architecture:

1. Business process
2. Information
3. Services
4. Applications
5. Infrastructure

Impact of IT on business operations: from fragmentation, wasted information, vulnerability, etc to integration, streamlined processes, lower costs and security.

1.2 Program management

Program management and agility

The typical transformation challenge:

- Long standing set of unfulfilled requirements
- Huge amount of stakeholders to please
- Very strong division between business and operations

- FNAO (Failure is Not An Option) culture
- No track record in innovation
- Standards seen as non-commercial

Waterfall model: big design up front

Agility: ability of firms to sense environmental changes and react to them in a timely and readily manner

Traditional approach: requirements, resources and time are plan driven.

Agile approach: ... are value driven.

A manifesto for business agility

- Clear operating model – how will we grow?
- Leadership setting vision and building capabilities
- Simple and clear Governance — strong core then innovate at edge
- Portfolio management
- Mature and modular enterprise architecture
- More IT savvy—set of practices and competencies that drive more business value (including agility) for each dollar invested

1.3 Vision and strategy

Stakeholders needs drive the value creation objective of the governance (benefits realisatin, risk optimization, resource optimization).

From aspirational through achievable to specific & tangible:

- Values: what do we stand for?
- Vision: where are we going?
- Mission: what do we do / who do we do it for?
- Strategic objectives: how are we going to progress?
- Actions and KPI (Key Performance Indicator): what do we have to do?

1.4 Key concepts and major landmarks in IT governance research

IT governance is the responsibility of the board of directors and executive management.

It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.

Goal cascade method: from management questions, to entreprise goals, to IT goals, to IT processes.

Case study 1: Seven years after the merge of two commercial banks, both organizations continued to possess two parallel data centers with virtually two IT Departments. Eventually, a TO-BE IT organization was conceived based on COBIT description of domains and processes and detailed RACI charts (Responsible, Accountable, Communicated and Informed). The team also identified new essential activities that were not previously carried out.

Case study 2: An Internet banking provider relied on a one of the largest worldwide IT services company for its 24/7 client operations. Services to clients suffered two major interruptions of 3 and 18 hours respectively. A comprehensive investigation based on COBIT highlighted major shortcomings both on the client and on the supplier level

Case study 3: A leading Financial Services organization launched two strategic projects aimed at changing the landscape of bank clearing activities on a full continent level in an outsourcing to two major systems integrators. When projects were eventually abandoned many years later, findings highlighted absence of essential processes including the oversight of the supplier as COBIT 5 would recommend.

2. Enterprise architecture

Reminders on S1 - Components of entreprise architecture:

- Business processes
- Information
- Services
- Applications (payment mgmt, inventory mgmt, etc)
- Infrastructure (on-site or cloud-based storage)

Build & run activities:

- Build include projects, software development, etc
- Run include help desks, etc

Sub-departments of IT (on avg, 5% of companies' budget, increasing):

- Data mgmt
- Security
- Software development
- Projects
- IT HR (specific HR for specific skills)
- Help desk
- IT finance
- Technical services, infrastructure, operations, etc

2.1 Business and IT pain points

- Business pain points
    - Business process outsourcing: pain because lack of supervision
    - Innovation process: where to start? How to identify some company's abilities, etc? Meetings, brainstormings -> identify IT related pain points and trigger events (positive opportunities)
- IT pain points:
    - Globalization
    - Economic pressure

2.2 Structure

An organisation has a structure

Definition of Architecture:

- "The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time"
- Entreprise architects
- IT architects (with different flavours: information, software, infrastructure, etc) Why don’t organizations have the right architecture?
- Change in environment
- M&A or other strategic actions
- Architectural degradation
- No plan

How do architectures get designed:

- Example of the Winchester house (which is visual, yet an application's architecture is trickier to judge)
- Without a plan, IT and business projects stack on top of each other and the organisation becomes silo-ed

To support your strategy, define your operating model:

1. What are the core activities in your organization
2. How standardized and integrated do they need to be?

2.3 The operating model

It focuses on the “sacred transactions” of the organization – the core activities that should be second nature, provides a stable view of the organization and is more useful for guiding IT efforts

Standardization:

- simplifies operations, reduces costs, and increases efficiency
- allows measurement, comparison, and improvement
- can accelerate innovation

But:

- can limit local flexibility
- may require that local units replace perfectly good systems and processes with new standards
- may be politically difficult to implement

Integration

- links efforts through shared data
- provides transparency across the organization, and the seamless flow of information across activities
- allows an organization to present a single face to a customer, supplier, or partner

But:

- requires common data definitions
- can be time-consuming and difficult to implement
- unnecessary if units are organized around unique customer groups

2.4 Key findings

- The transition from one stage to the next is difficult and time consuming.
- Moving from one stage to the next requires a business transformation as well as a technical one. Companies that try to skip a stage are usually unsuccessful.
- Each stage involves a very different view of the value of IT and the role of IT in the organization.
- The leadership challenges are very different for each transition

The role of the CIO changes as organizations move through the stages

2.4 Conclusions

- Enterprise architecture is the organizing logic for the foundation of the organization: work processes and IT systems
- In most organizations, architecture is hindering execution and preventing innovation
- Defining the operating model is the first step in choosing the right architecture for an organization
- Transforming architecture is a difficult and time-consuming process, but the benefits begin immediately

3. Gouvernance and cascading strategy

Objectives:

- understand what is Governance of Enterprise IT
- know what COBIT is and it can support good governance
- understand the COBIT process map
- understand the Business/IT Goals cascade mechanism, and be able to use it

Simply stated, COBIT 5 helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use.

3.1 COBIT principles

1. Meeting stakeholders needs
2. Covering the entreprise end-to-end:

   COBIT 5 addresses all the relevant internal and external IT services, as well as internal and external business processes.)

3. Applying a single integrated framework

4. Enabling a holistic (global) approach - the enablers*

   Any enterprise must always consider an interconnected set of enablers (capabilities, forces, and resources that contribute to the success of an entity, program, or project). That is, each enabler:

   - Needs the input of other enablers to be fully effective, e.g., processes need information, organisational structures need skills and behaviour.
   - Delivers output to the benefit of other enablers, e.g., processes deliver information, skills and behaviour make processes efficient.

5. Separating governance from management**

   Governance ensures that stakeholders needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives (EDM). • Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives (PBRM).

Quizz (with my answer attempts):

1. Governance is about negotiating and deciding amongst different stakeholders' value interests. **True**
2. Creating value for a stakeholder means delivering benefits at the lowest cost possible. **False**
3. Management sets the direction for the Company. **False**
4. Once a Company uses COBIT, it should not use ITIL or PII anymore (T/F) **True**
5. The enablers are a set of independent topics **False**

3.2 COBIT processes

> See COBIT reference for process. Processes are enablers.

Example attributes: Process identification, description, purpose statement, IT related goals and metrics, process goals and metrics, etc.

Quizz (with my answer attempts):

1. IT Goals metrics are generic. **False**
2. Process goals are generic. **False**
3. There is more Governance processes than Management processes. **True**
4. To which Domain belong “Manage requirements” – “Manage suppliers” ? “Manage continuity” ? “Manage service agreements” ? “Ensure resource optimization” ? **Management (?)**
5. In the process model, governance and management activities are distinct, and there is no output of one that serves as input for the other. **False**
6. RACI charts maps to internal and external stakeholders. **False**
7. Processes are broken down in Governance practices, which are broken down in activities (T/F) **Processes > Management practices > Activities**
8. Process goals are defined as ‘a statement describing the desired outcome of a process’. An outcome must be a tangible artefact. **False, can be high-level description / vision**
9. Inputs and Outputs are defined at the level of activities. **True (?)**
10. The COBIT5 Process Reference Model is prescriptive. **False (?)**

3.3 Business / IT goal cascade

Back on COBIT principles:

1. Meeting stakeholders needs
    - Stakeholder needs have to be transformed into an enterprise’s pracCcal strategy.
    - The COBIT 5 goals cascade translates stakeholder needs into specific, pracCcal and customised goals within the context of the enterprise, IT-related goals and enabler goals.

> See fancy charts in the slides for information on how to map Enterprise Goals with IT Goals, then IT Goals and IT processes.

Inpractice, the goals cascade:

- Defines relevant and tangible goals and objecCves at various levels of responsibility.
- Filters the knowledge base of COBIT 5, based on enterprise goals to extract relevant guidance for inclusion in specific implementaCon, improvement or assurance projects.
- Clearly identifies and communicates how (sometimes very operaConal) enablers are important to achieve enterprise goals.

Quiz (with my answer attemps):

1. To which COBIT principle belongs the goal cascading mechanism? **2. Covering the entreprise e2e or 4. Applying a holistic approach**
2. Each process is mapped towards one or several Enterprise Goals. **False. Processes are mapped to IT goals which are themselves related to Entreprise goals**.

> See the exercise on bpost strategy

6. Système d'Information Transeuropéen

Intégration de systèmes à grande échelle ou Construire l'Europe du partage de données

6.1 Contexte

Pourquoi des SI Transeuropéen ? Pour partager des informations entre de nombreux acteurs différents.

Un SI Transeuropéen est un système de systèmes répartis dans toute l'UE dont le but est de partager des données afin d'atteindre des objectifs politiques ou opérationnels.

6.2 Exposé du problème

- Complexité organisationnelle et décisionnelle: aspects politique, stratégique et opérationnel.
- Intervenants: insitutions, EM, pays tiers, entreprises
- Interfaces
- Processus de Décision: comités de décision
- Diversité d'Environnements Informatiques: harmonisation inenvisageable
- Diversité d'Organisations: hiérarchies, stratégies de sous-traitance, méthodologies, politiques de sécurité

"Le SIT est aussi manoeuvrable qu'un super tanker."

6.3 Principes de solution

- Décision: minimiser les changements
- Organisation: subsidiarité (action revient à l'entité compétente la plus proche de ceux qui en sont directement concernés)
- Diversité: implémentation d'**interfaces** techniques, organisationnelles et de sécurité.

6.4 Domaines de responsabilité

- Subsidiarité: cohérence d'ensemble non garantie, responsabilité aux interfaces non définie
- Domaine Commun

- Domaine National
- Domaine Externe

Pour tous les domaines:

- Chacun est maître chez lui
- Chaque fournisseur
    - coordonne
    - définit ses interfaces avec ses clients

6.5 Gestion de projet

Chacun gère son propre plan et communique les "points de rendez-vous". La COM (Commission Européenne) consolide le plan du Domaine Commun et chaque EM consolide le plan de son Domaine National.

Les clés de réussite sont l'organisation, la gestion de projet et surtout le facteur humain.

6.6 Architecture

/

6.7 Interopérabilité

Le but est de spécifier les interfaces. On parle de spécifications système (business, techniques et tests), de sécurité et organisationnelles.

Pour interopérer, il nous faut spécifier des interfaces, plein d'interfaces, produisant une grande quantité de documents selon la complexité du SIT.

Réutiliser un cadre existant réduit coût et délai

6.8 Conclusions

Un SI transeuropéen, c'est:

- intégré avec des milliers d'êtres humains
- respectueux de la diversité
- international et multiculturel
- varié et concret
- passionnant
- une expérience fantastique et enrichissante

6.10 Annexes et backup

/

10. Certification of application security

Learning objectives

- Introduce a new paradigm to build and verify software security based on new ISO/IEC Standard
- Understand how to create a Security Design pattern which can be tracked through the development process
- Describe methods to certify application security through the review of Application Security Controls (ASC)

10.1 Introduction

Definitions

- Information security: Preservation of confidentiality, integrity and availability of information
- Validation: The assurance that a product, service, or system meets the needs of the customer and other identified stakeholders
- Verification: The evaluation of whether or not a product, service, or system complies with a regulation, requirement, specification, or imposed condition. It is often an internal process
- Audit: Systematic, independent and documented process for obtaining audit evidence [records, statements of fact or other information which are relevant and verifiable] and evaluating it objectively to determine the extent to which the audit criteria [set of policies, procedures or requirements] are fulfilled

Scenario

Phases:

1. Requirements
2. Design
3. Implementation
4. Verification
5. Release (including server hardening: firewalls etc)

Security is critical for organizations. Some questions arise:

- Can we trust third parties framework used inside our applications ?
- Can we use logs or other evidences in front of court in case of security incident ?
- Can we assure the board that everything is under control ?
- Do we effectively respect Data privacy of our clients ?
- Could we prove our PCI-DSS* compliance ?

*: PCI-DSS is required for interacting with VISA.

Principle: what cannot be measured cannot be managed. Need to create trut between business and IT, security software must be assessed with evidences.

ISO 27034 principles:

1. Security is a requirement
2. Application security should be managed
3. Application security is context-dependent
4. Appropriate investment for application security
5. Application security must be demonstrated

10.2 Certifying security inside an application

Phase 1: Risk Assessment

1. Where do risks come from? (in terms of people, processes, technology)
2. Determine risks, security requirements and level of trust

Example: security during transmission: low (http), medium (https), high (https + data encryption).

Security control (control in the sense of device, tool) "controls" the required level of trust and the security requirements.

> See slide 26 for examples of security controls

Phase 2: Application Security Controls

Objectives:

1. Security Design Pattern (Knowledge documentation)

   Security activities -> evidence -> verification process -> verification outcome

2. Translate the Security Requirements into a concrete set of tasks

   Risk -> security requirement -> task with some time and some cost

3. Use by the project to implement a Security Control
4. Use by the business to estimate the cost
5. Use by the project manager to estimate the time
6. Use by the quality manager to verify the implementation

7. Use by the auditor to certify the application

8. Improve the organization's Application Security Maturity

What are the advantages of the Application Security Life Cycle Model ?

- Create a Helicopter view of different disciplines under the scope of Application Security
- Allow to identify what are missing areas within the organization
- Allow different disciplines to communicate in an effective way
- Allow to choose the right place for an Application Security Control

10.3 Conclusion

In 2016, Application Security cannot be a feeling:

- A security control cannot be taken in account if there is no evidence it fulfills his purpose.
- It provides a way to demonstrate that an application reaches a specific level of trust within the organization.
- It provides a way to evaluate the application security cost.