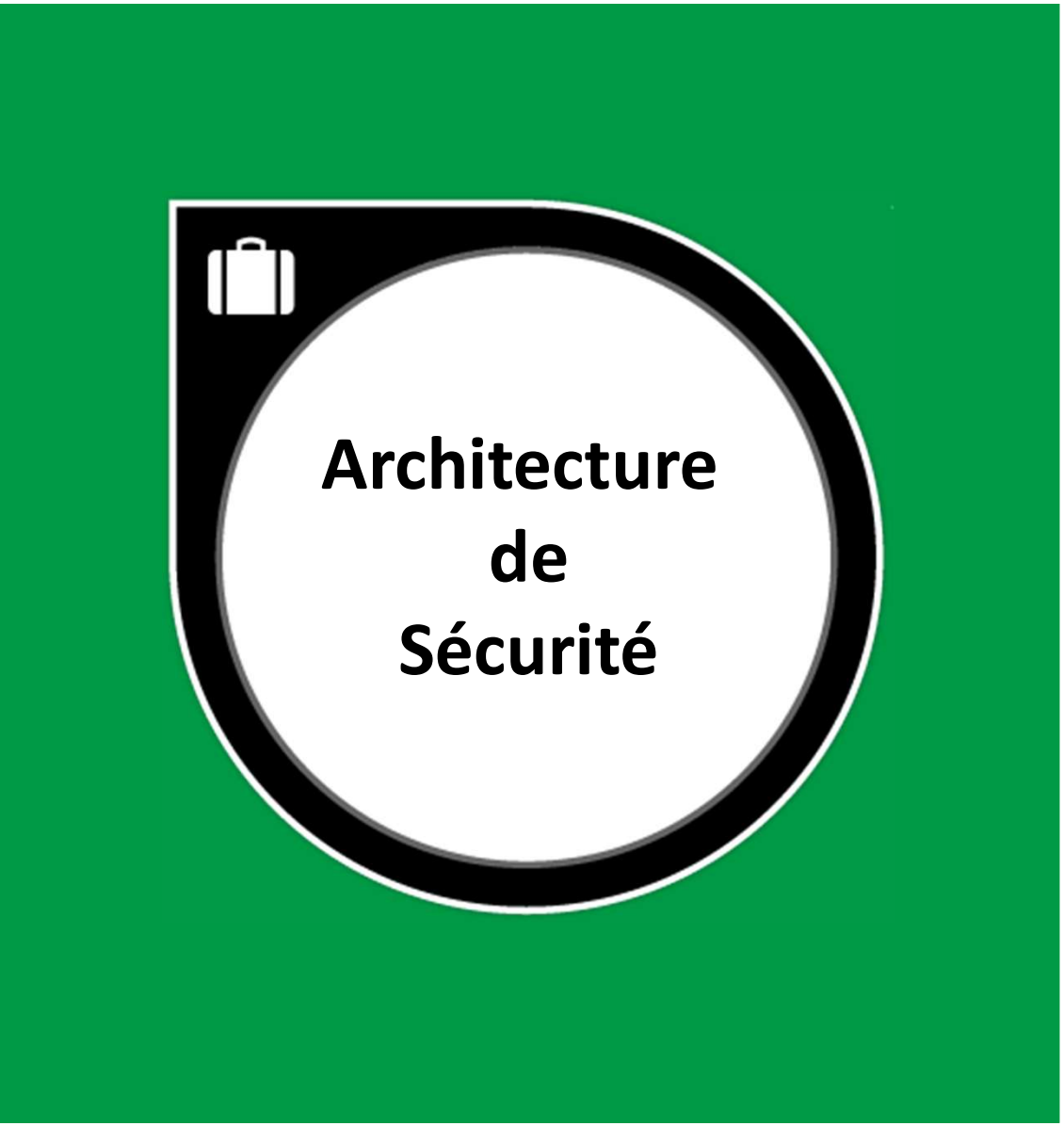


INF 809
Architecture de sécurité

Stratégie

Cours 4
Architecture Contextuelle

UNIVERSITÉ DE SHERBROOKE

PLAN DE LA SÉANCE

- Retour sur les notions de base
- Requis d'affaire (*Business Requirements)*
- Moteur d’affaire (*Business Drivers for security*)
- Attributs SABSA
- Les contraintes
- Scénarios de menaces
- Matrice de risque et priorisation

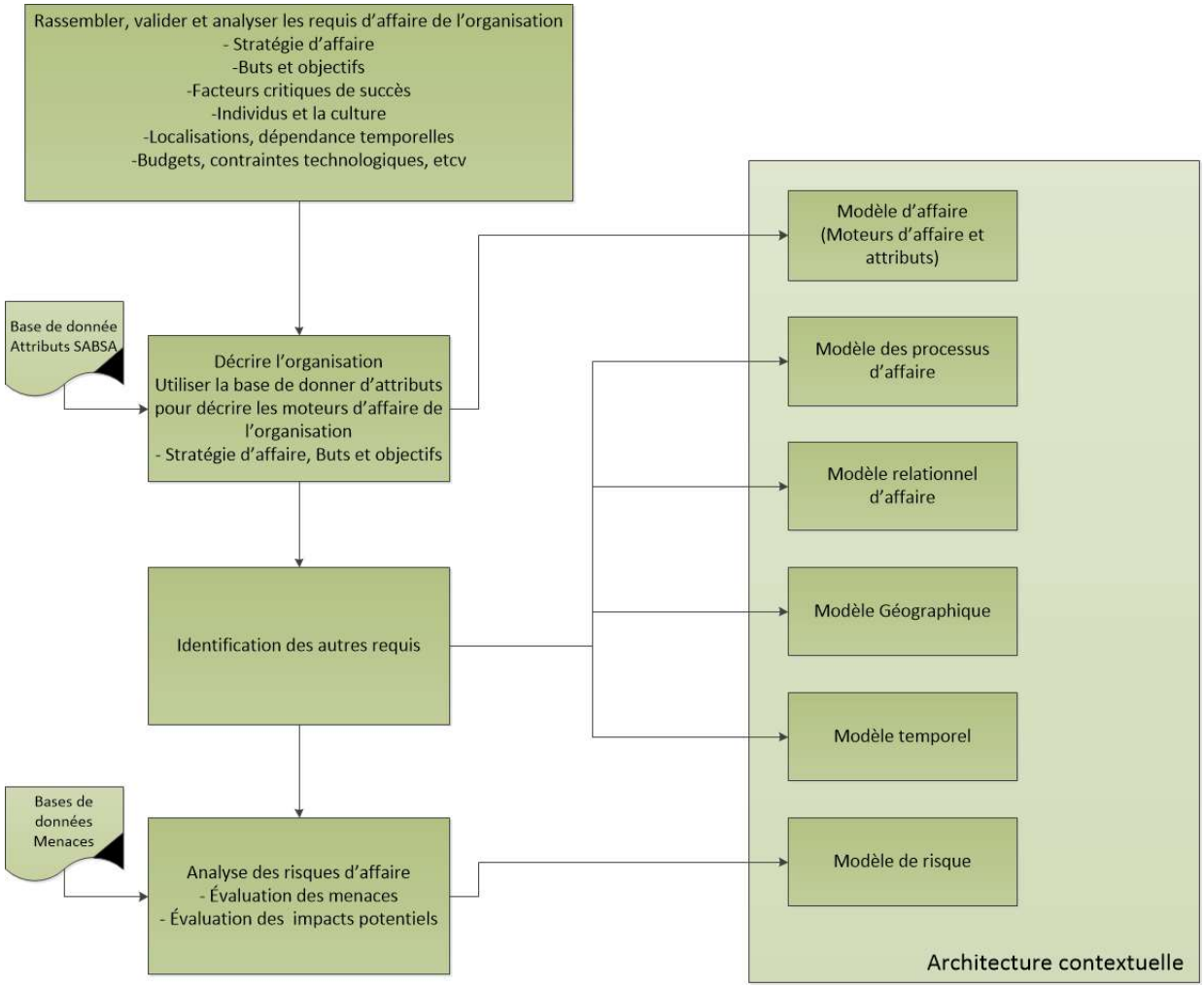
PLAN DE LA SÉANCE

PLAN DE LA SÉANCE

Table 2: SABSA Architecture Matrix™ 2018

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Goals & Decisions	Business Risk	Business Meta-Processes	Business Governance	Business Geography	Business Time Dependence
	Business Value; Taxonomy of Business Assets, including Goals & Objectives , Success Factors, Targets	Opportunities & Threats Inventory	Business Value Chain; Business Capabilities	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of Business Goals and Value Creation
CONCEPTUAL ARCHITECTURE	Business Value & Knowledge Strategy	Risk Management Strategy & Objectives	Strategies for Process Assurance	Security & Risk Governance; Trust Framework	Domain Framework	Time Management Framework
	Business Attributes Taxonomy & Profile (with integrated performance targets)	Enablement & Control Objectives; Policy Architecture; Risk Categories; Risk Management Strategies; Risk Architecture; Risk Modelling Framework; Assurance Framework.	Inventory of all Operational Processes (IT, industrial, & manual); Process Mapping Framework; Architectural strategies for IT used in process support.	Owners, Custodians and Users; Service Providers & Customers; Trust Modelling Framework	Security Domain Concepts & Framework	Through-Life Risk Management Framework; Attribute Performance Targets
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Trust Relationships	Domain Maps	Calendar & Timetable
	Inventory of Information Assets; Information Model of the Business	Risk Models; Domain Policies; Assurance Criteria (populated Assurance Framework).	Information Flows; Functional Transformations; Service Oriented Architecture; Services Catalogue; Application Functionality and Services	Domain Authorities; Entity Schema; Privilege Profiles; Trust Relationship Models	Domain Definitions; Inter-domain Associations & Interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	Infrastructure	Processing Schedule
	Data Dictionary & Data Storage Devices Inventory	Risk Management Rules & Procedures; Risk Metadata	Working Procedures; Application Software; Middleware; Systems; Security Mechanisms; Process Control Points	User Interface to Business Systems; Identity & Access Control Systems	Workspaces; Host Platforms, Layout of Devices & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	Component Assets	Risk Management Components & Standards	Process Components & Standards	Human Entities: Components & Standards	Locator Components & Standards	Step Timing & Sequencing Components and Standards
	Products and Tools, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery; Application Products	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators; Component Configuration	Time Schedules; Clocks, Timers & Interrupts
MANAGEMENT ARCHITECTURE	Delivery and Continuity Management	Operational Risk Management	Process Delivery Management	Governance, Relationship & Personnel Management	Environment Management	Time & Performance Management
	Assurance of Operational Excellence & Continuity	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Management & Support of Enterprise-wide and Extended Enterprise Relationships	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

PLAN DE LA SÉANCE



- ESA p114 Figure 7-4

UNIVERSITÉ DE SHERBROOKE

Abstraction

UNE ABSTRACTION EFFICACE EST REQUISE

- L'abstraction en architecture d'entreprise…
  - Une généralisation d'un ou plusieurs concepts, sans aucun détail sur l'implémentation de celui-ci. Ces généralisations sont obtenues de concepts ayant des similarités évidentes.

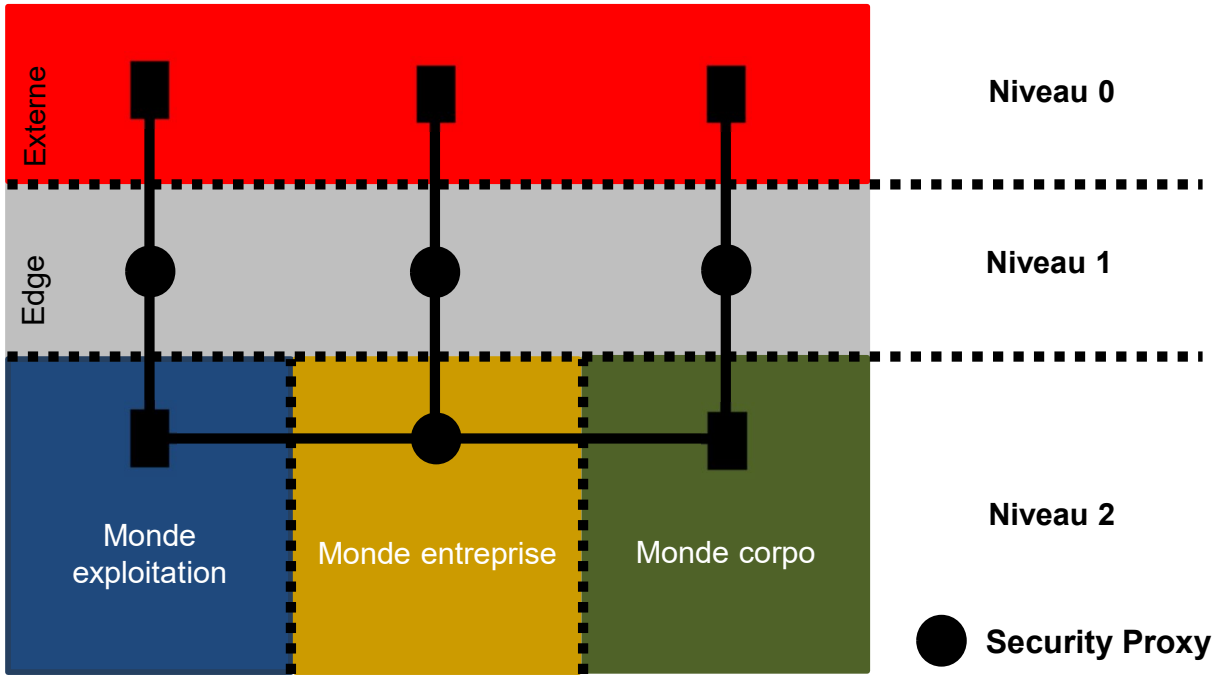
Objets abstrait (sécure)

Concept de sécurité 1
Concept de sécurité 2
Concept de sécurité 3

Sherwood ESA ch.11 p.290

UNE ABSTRACTION EFFICACE EST REQUISE

Modèle abstrait de l'architecture réseau



Architecture de référence

Architecture de référence logique – Sécurité Réseau (155 pages)

UNE ABSTRACTION EFFICACE EST REQUISE

- Afin d'obtenir une traçabilité efficace, il est important de développer dès le départ une bonne abstraction du contexte d'affaire (actifs, buts & objectifs).
- Pour se faire, l'architecture contextuelle doit définir 2 ensembles différents de requis :

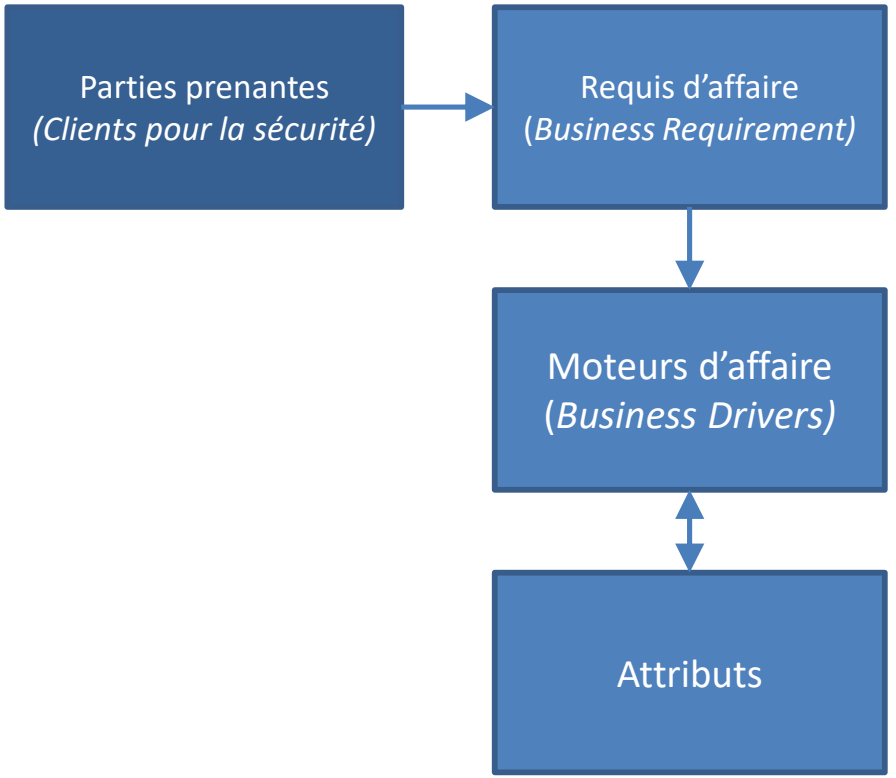
Requis d'affaire	Les actifs, les processus et les objectifs au niveau de la conduite des affaires de l'organisation. (La réputation de l'organisation, ses objectifs de ventes, etc)
Moteurs d'affaire (sécurité)	Les requis d'affaire sur lesquels on applique une abstraction pour la sécurité afin de définir les requis de sécurité nécessaire à la saine conduite des affaires de l'organisation

Moteurs d'affaire
(*Business Drivers for security)*

UNIVERSITÉ DE SHERBROOKE

TOUT COMMENCE EN HAUT DE LA PYRAMIDE

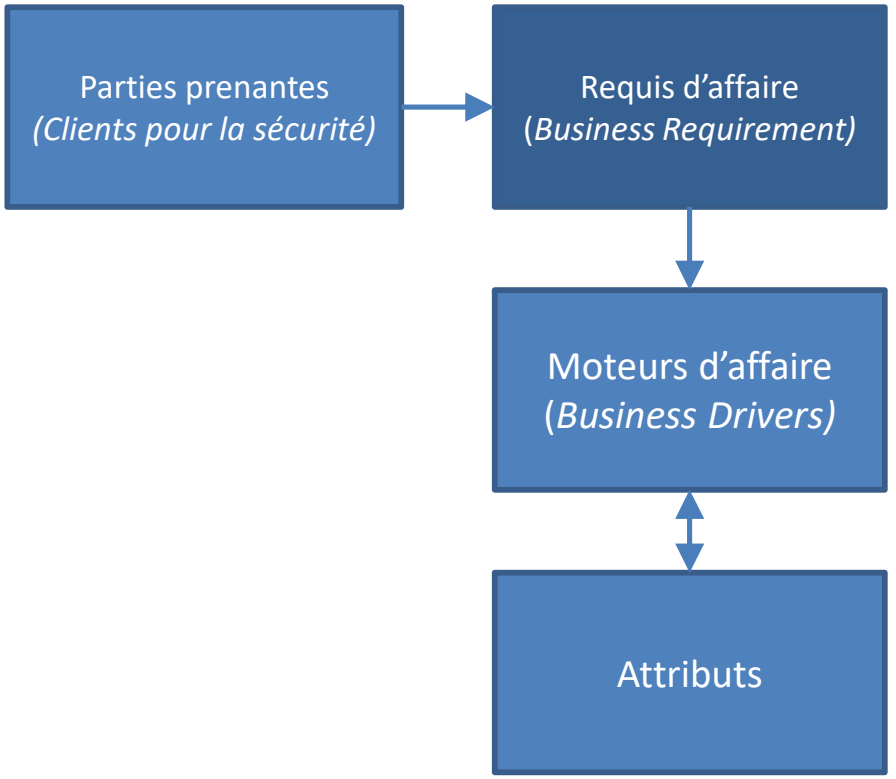
- C-Level (CISO, CTO, CFO, CEO,etc)
- Senior managers
- Leaders d'affaire
- Gestionnaires de programmes
- Gestionnaires de projets



REQUIS D'AFFAIRE

- Stratégie d'affaire
- Buts et objectifs
- Facteurs critiques de succès

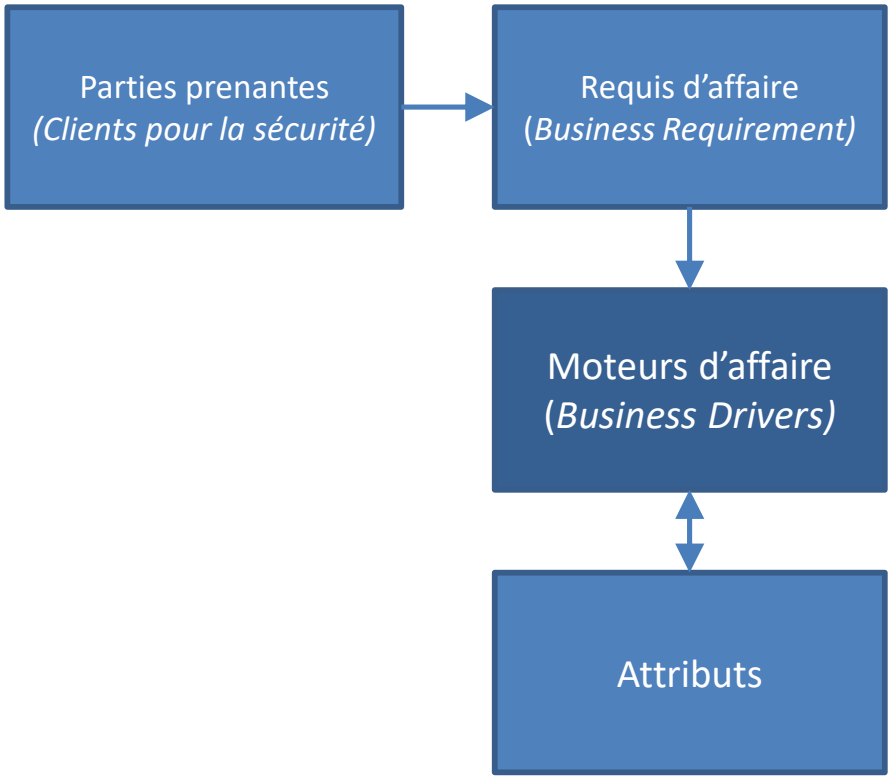
- Ce qui est le plus important pour l'organisation au niveau stratégique (p.169-187)
  - Vendre plus de produit
  - La réputation de l'organisation
  - Mission social
  - L'organisation digital
  - TI comme facilitateur



MOTEUR D'AFFAIRE DE SÉCURITÉ

- Chaque organisation est unique
  - Ce qui implique que chaque organisation aura un profil de sécurité unique
- Afin de pouvoir conduire une bonne évaluation des risques auxquels est exposé une organisation, il faut comprendre quels sont ses besoins en sécurité → Les moteurs d'affaire (*Business Drivers for security)*
- Les moteurs d'affaire doivent découler des requis d'affaire
  - Chaque requis (BR) aura son ensemble de BD
- Artefact clé de l'Architecture Contextuelle

- Qu'est-ce que la sécurité peut faire pour ***protéger, maximiser, supporter l'organisation*** dans le contexte de son besoin d'affaire exprimé ?

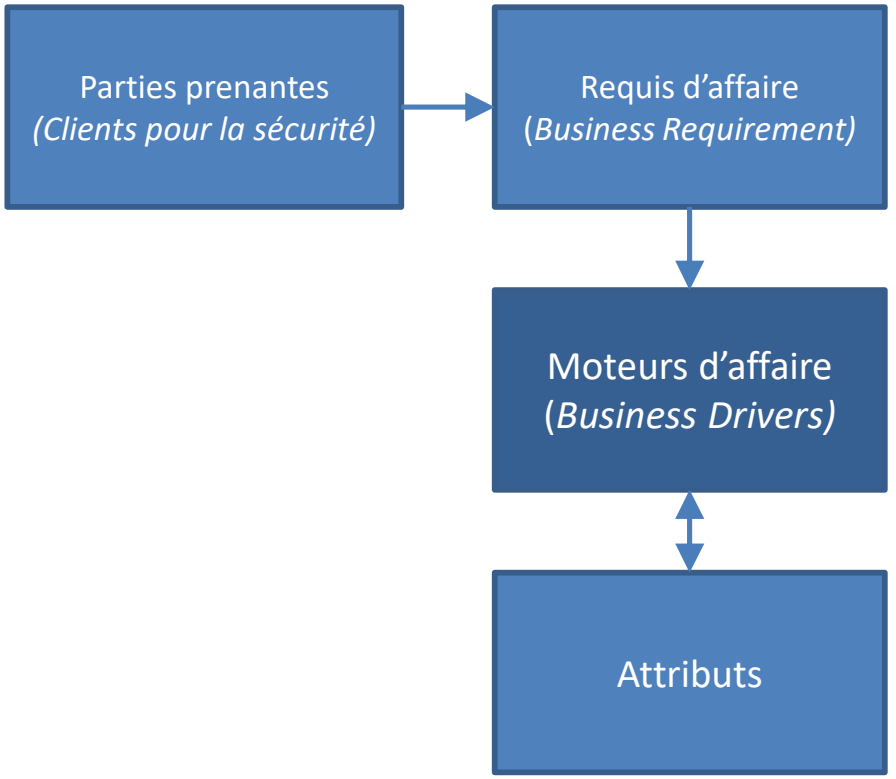


MOTEUR D'AFFAIRE DE SÉCURITÉ

Partie prenante « A » : « Nous devons produire plus de TrucA »

Architecte de sécurité : « Nous pourrons produire plus de TrucA si la sécurité permet d'améliorer la chaîne de production grâce à un plus haut niveau de confiance et à une réduction des pannes évitables »

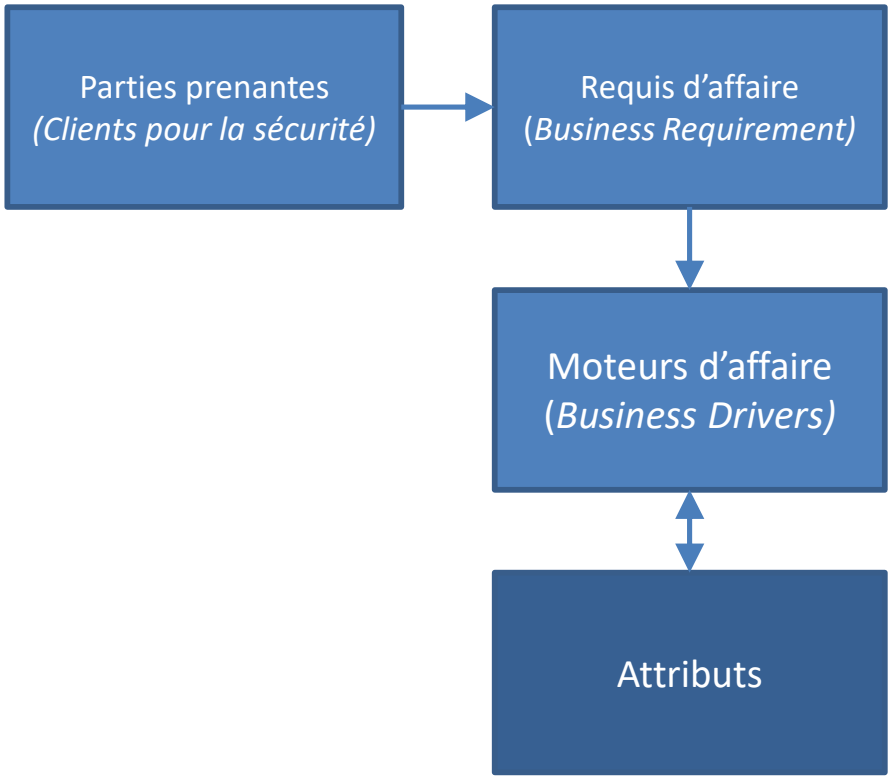
Le moteur d'affaire de sécurité reflète l'importance de la sécurité dans le requis d'affaire.



ATTRIBUTS

- Un attribut est une abstraction conceptuelle d'un ou plusieurs véritable(s) moteur(s) d'affaire

- Les attributs fournis par SABSA on été modélisés dans un langage normalisé qui utilise une taxonomie définie qui permet une mesure de la performance simple et intuitive



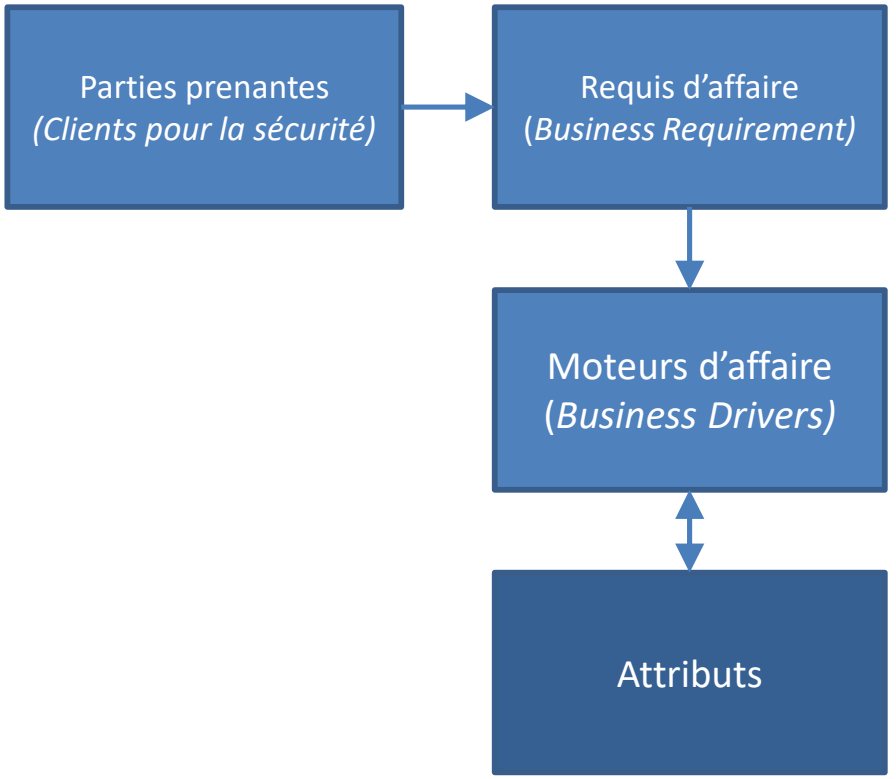
ATTRIBUTS – QUEL EST LA VALEUR DE CET ABSTRACTION ?

- La structure du profil d'attribut permet une organisation et une communication claire des requis de sécurité abstrait de toute complexité et simple à comprendre pour les parties prenante

Attribute	Attribute Classification	Attribute Definition	Owner (Accountable Authority)	Performance Target	Recommended Measurement Category	Recommended Measurement Approach	Recommended Metric Type
"Error-free"	Operational Attribute	*"The system should operate without producing errors."*	System Owner	99.9% of all system output is correct	Performance	Random sample of system output conducted on a daily basis	Percentage

ATTRIBUTS – LA VALEUR DU PROFILAGE

- Le profil des attributs et la technique de création des profils d'attributs permet à n'importe quel ensemble de requis d'être normalisé en un ensemble de spécifications réutilisables (objets réutilisables)
- Assure une traçabilité bidirectionnelle entre le requis d'affaire et la solution
- Procure un lien vital entre les requis d'affaire et le design technologique et le design de processus de sécurité

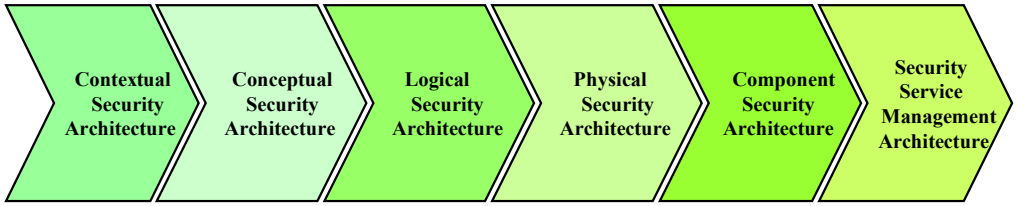


ATTRIBUTS – TRAÇABILITÉ

- Lorsqu'on cherche à comprendre pourquoi les choses sont faite d'une certaines façon dans une organisation, si l'architecture de sécurité a été développé suivant une méthode structuré, il sera toujours possible de tracer la réponse jusqu'au requis d'affaire

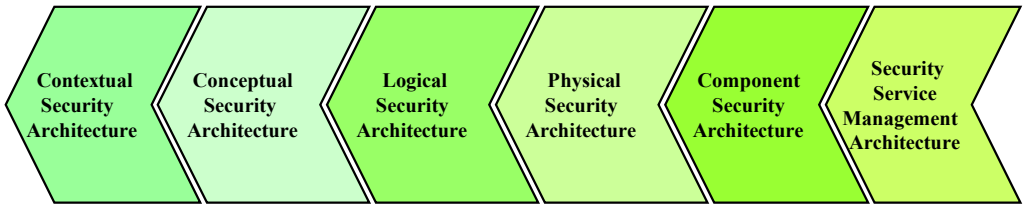
- Permet de suivre la logique des décisions à travers les différentes couches du modèle

Architecture complète



Chaque requis d'affaire pour la sécurité est répondu et le risque résiduel est acceptable pour l'organisation

Traçabilité complète



Chaque éléments opérationnels ou technologiques de sécurité peut être justifié par une référence à un risque touchant un requis d'affaire

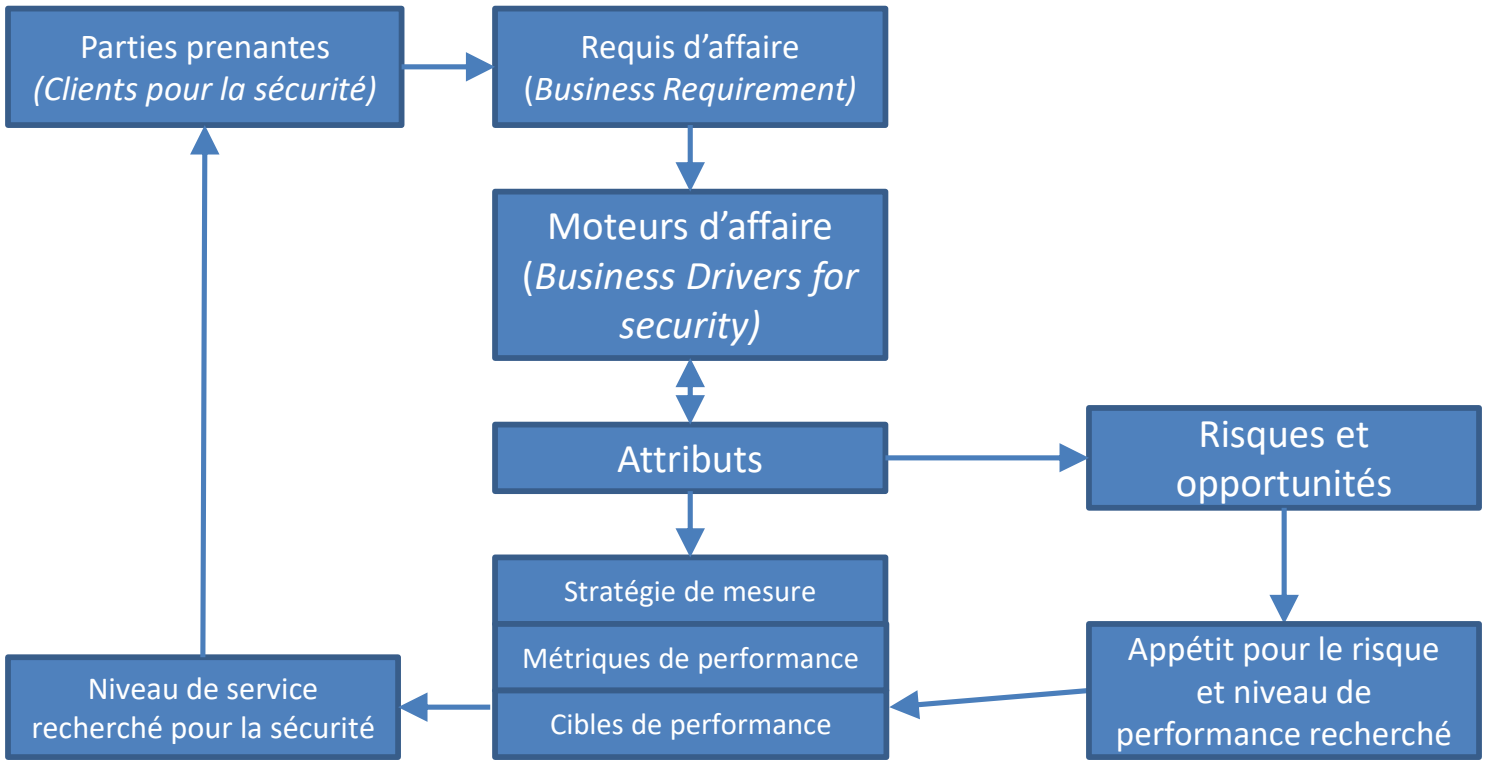
*ESA p.88

ATTRIBUTS – MISE EN PRATIQUE DU PROFILAGE D'ATTRIBUTS

CeFTI

- Facteur clé dans la traçabilité des éléments
- Référence afin de s'assurer d'avoir une architecture complète (*completeness)*
- Évaluation, surveillance et suivi des cyber-risques
- Définition des objectifs de contrôle
- Gestion et mesure de performance des objectifs de contrôle
- Stratégie de surveillance de la performance générale de sécurité
- Pick-list de requis qu'on désire incorporer dans les tests utilisateurs
- Évaluation et opération – contrats, SLA's, objectifs de performances
- Point d'intégration pour n'importe quel standards de sécurité qui requière un barème de mesures
- ROI
- Procurement, Appelle d'offre et évaluation des propositions
- Gouvernance
- Security Assurance grâce aux audit et à la conformité
- Intégration des outils de conformité (base de départ)
- Communication avec les C-level

PROCESSUS DE CRÉATION DE PROFILS DES ATTRIBUTS



ATTRIBUTS – DÉFINITION DE LA TAXONOMIE ET DU PROFIL

SABSA Business Attributes Taxonomy

Nom, Définition, Classification

SABSA Business Attributes Profile

Nom, Définition, Classification**, Cible de performance, Stratégie de mesure, Métriques**

Expérience utilisateur par rapport à la sécurité du système

Requis de sécurité pour la gestion des système

La sécurité qui protège les opérations quotidiennes

Les requis de sécurité pour identifier et gérer les risques

Attribute Classifications	Description
User Attributes	This group of attributes are related to the user's experience of interacting with the business system
Management Attributes	This group of attributes are related to the ease and effectives with which the business system and its services can be managed
Operational Attributes	This group of attributes describes the ease and effectives with which the business system and its services can be operated
Risk Management Attributes	This group of attributes describes the business requirements for mitigating operational risk. ***This group most closely relates to the "security requirements" for protecting the business.***
Legal & Regulatory Attributes	This group of attributes describe the business requirements for mitigating operational risks that have a specific legal or regulatory connection.
Technical Strategy Attributes	This group of attributes describes the needs for fitting into an overall technology strategy
Business Strategy Attributes	This group of attributes describes the needs for fitting into an overall business strategy

Ce que les exécutifs veulent voir

Les requis de conformité

Aspects stratégiques de l'architecture technologique et de sécurité

ATTRIBUTS – RÈGLE À SUIVRE POUR LE PROFILAGE

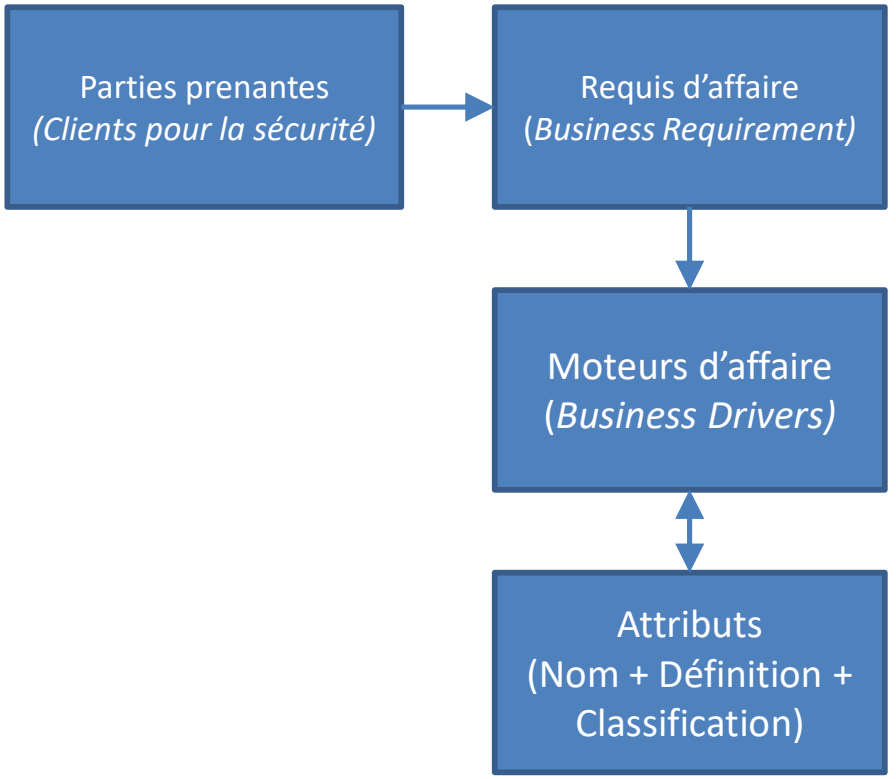
- Les attributs peuvent être tangibles ou intangibles
- Chaque attributs doit être identifié par un nom et avoir une définition détaillé de sa signification ***pour votre organisation***
- Les attributs doivent être validés et endossés par l'exécutif et les parties prenantes de l'organisation
- Chaque attribut doit avoir sa stratégie de mesure et ses métriques pour pouvoir fixer les cibles de performance
- Les cibles de performances peuvent ensuite être utlisés dans les activités de design, d'implémentation, de négociation contractuelles et de KPI

COMMENT CRÉER LES PROFILS

1. Valider avec les différentes parties prenantes quels sont les requis d'affaire

2. Identifier les moteurs d'affaire (*Business drivers for security*) des parties prenantes

3. Construire la taxonomie d'attributs (*Nom + Définition + Classification*)



EXEMPLE – IDENTIFICATION DES REQUIS D'AFFAIRE

1. Entretien au sujet des requis d'affaire avec un exécutif

Entretien avec le PDG de Banque Toto :

«Nous sommes une entreprise mondiale avec une réputation qui c'est construite sur plus d'un siècle. Les clients nous donnent tout leur argent et nous demandent de s'en occuper pour eux. Il n'est pas possible pour un client d'avoir plus confiance en une organisation que la confiance qu'ils nous démontrent? Si, pour une raison ou une autre, ce niveau de confiance qui nous est démontré était brisé, nos relations avec nos clients et notre réputation sur le marché en souffriraient énormément.»

EXEMPLE – IDENTIFICATION DES MOTEURS D'AFFAIRE DE SÉCURITÉ

2 Identifier les moteurs d'affaire (*Business drivers for security*) des parties prenantes

Entretien avec le PDG de Banque Toto :

«Nous sommes une entreprise mondiale avec une réputation qui c'est construite sur plus d'un siècle [BDS1]. Les clients nous donnent tout leur argent et nous demandent de s'en occuper pour eux. Il n'est pas possible pour un client d'avoir plus confiance en une organisation que la confiance qu'ils nous démontrent? [BDS2] [BDS3] Si, pour une raison ou une autre, ce niveau de confiance qui nous est démontré était brisé, nos relations avec nos clients et notre réputation sur le marché en souffriraient énormément. [BDS4] [BDS5]»

Échantillon des BD de sécurité	
BDS1	Protéger la réputation de l'organisation, s'assurer qu'elle est perçue comme compétente dans son domaine
BDS2	Protéger le niveau de confiance des clients envers l'organisation
BDS3	Protéger les différentes parties en relation d'affaire avec nous de pertes financière, de données ou autres due à une mauvaise gouvernance
BDS4	Maintenir le niveau de confiance des différentes parties
BDS5	Réduire le risque de détérioration des relations avec nos clients majeurs

EXEMPLE – IDENTIFICATION DES REQUIS D'AFFAIRE

1. Entretien au sujet des requis d'affaire avec un exécutif

Entretien avec le VP E-Business de Banque Toto :

«Mon plus grand défi consiste à maîtriser la gestion de la relation client dans une entreprise aussi diverse que la notre, où de nombreux projets de développement d'applications sont créés par de nombreuses unités commerciales. Si l'un de ces projets se comporte différemment des autres ou de ce qui est prévu par la stratégie d'entreprise en matière de gestion des informations client, l'initiative de gestion de la relation client à l'échelle de l'entreprise dont je suis le responsable sera sérieusement mise à risque. »

EXEMPLE – IDENTIFICATION DES MOTEURS D'AFFAIRE DE SÉCURITÉ

2 Identifier les moteurs d'affaire (*Business drivers for security*) des parties prenantes

Entretien avec le VP E-Business de Banque Toto :

«Mon plus grand défi consiste à maîtriser la gestion de la relation client dans une entreprise aussi diverse que la notre [BDS6], où de nombreux projets de développement d'applications sont créés par de nombreuses unités commerciales. Si l'un de ces projets se comporte différemment des autres ou de ce qui est prévu par la stratégie d'entreprise en matière de gestion des informations client, l'initiative de gestion de la relation client à l'échelle de l'entreprise dont je suis le responsable sera sérieusement mise à risque. [BDS7] »

Échantillon des BD de sécurité	
BDS6	Besoin d'une politique d'entreprise pour la gestion des données clients, ainsi qu'une surveillance pour assurer la conformité de celle-ci
BDS7	L'architecture de sécurité devrait être indépendante des fournisseurs ou des produits. Elle devrait tracer les lignes directrices pour supporter plusieurs fournisseurs et plusieurs produits.

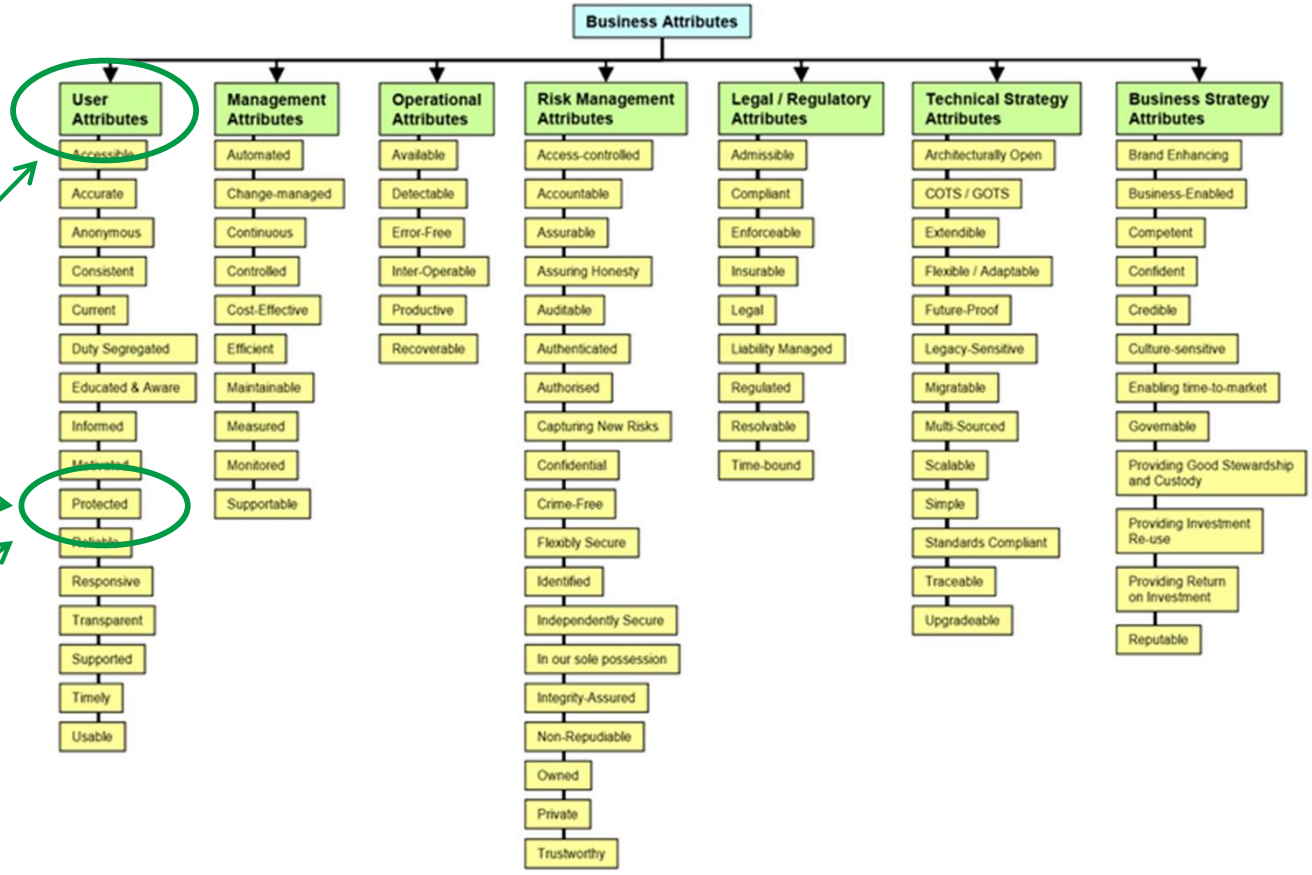
EXEMPLE – COMPLÉTER LA TAXONOMIE

3 Construire la taxonomie des attributs (Nom + Définition + Classification)

Classification : « User Attribute »

Nom : « Protected »

Définition: « Les informations d'un utilisateur ainsi que ses privilèges d'accès doivent être protégés contre les abus d'autres utilisateurs ou d'un intrus. »



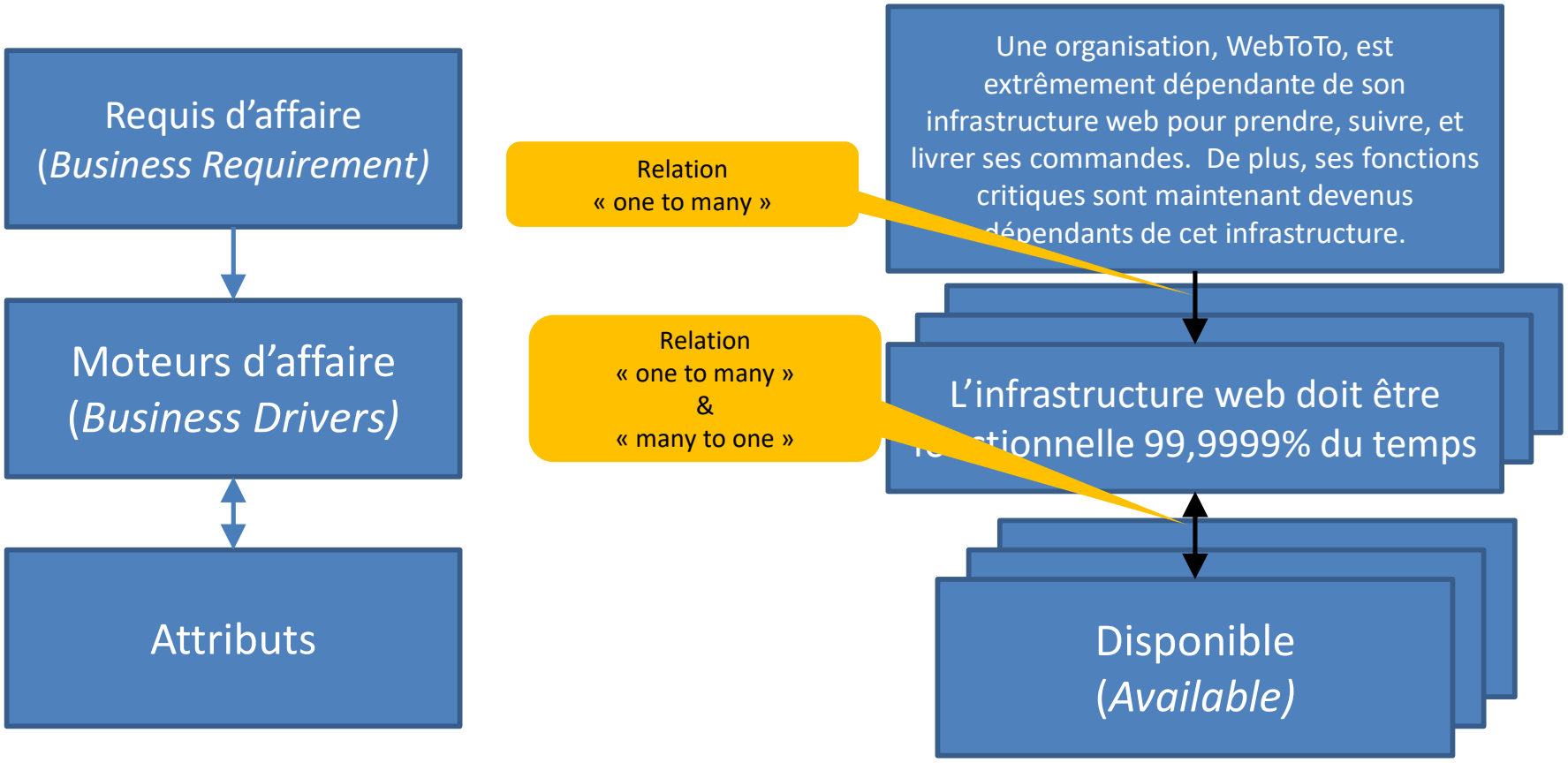
EXEMPLE – COMPLÉTER LA TAXONOMIE SELON LES BDS

3

Construire la taxonomie des attributs (Nom + Définition + Classification)

Échantillon des BD de sécurité		Nom des attributs
BDS1	Protéger la réputation de l'organisation, s'assurer qu'elle est perçue comme compétente dans son domaine	Reputable, Competent
BDS2	Protéger le niveau de confiance des clients envers l'organisation	Confident
BDS6	Besoin d'une politique d'entreprise pour la gestion des données clients, ainsi qu'une surveillance pour assurer la conformité de celle-ci	Controlled, Governable
BDS7	L'architecture de sécurité devrait être indépendante des fournisseurs ou des produits. Elle devrait tracer les lignes directrices pour supporter plusieurs fournisseurs et plusieurs produits.	Architectully open, standards-compliant

MOTEUR DE SÉCURITÉ - EXEMPLE



TRAÇABILITÉ BIDIRECTION ENTRE BDS ET ATTRIBUTS

Moteurs vers Attributs

BDS	Attributs supportant le BDS
BDS1	Reputable, Competent
BDS2	Confident
BDS6	Controlled, Governable
BDS17	Access Controlled, Confident, Confidential, Private

Attributs vers Moteurs

Attribut	BSD
Private	BDS7, BDS9, BDS14
Informed	BDS11
Non-repudiable	BDS23, BDS34
Confident	BDS2, BDS17

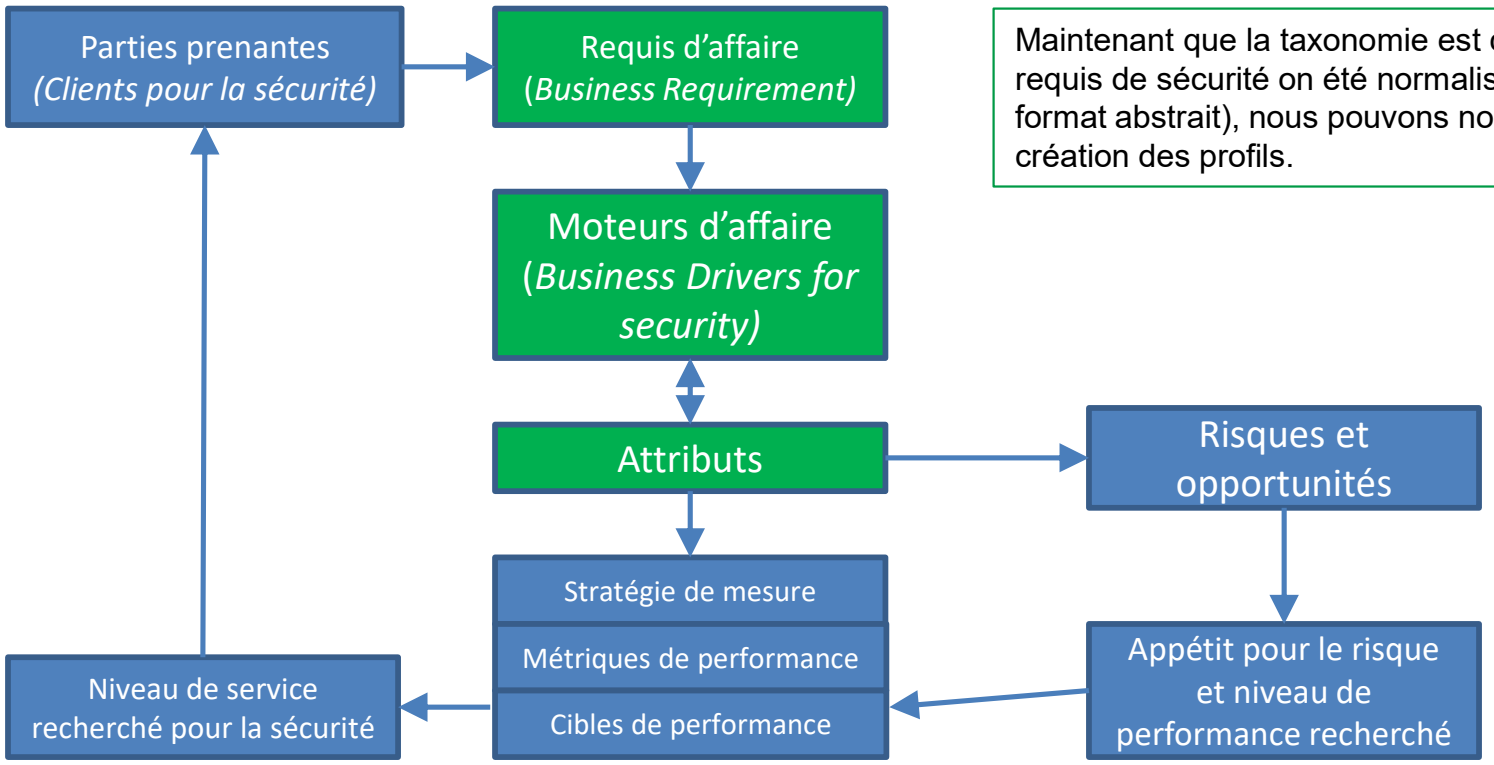
EXEMPLE – CLASSIFICATION ET DÉFINITION DES ATTRIBUTS

3

Construire la taxonomie des attributs (Nom + Définition + Classification)

Classe	Nom	Définition
Business strategy	Reputable	Le système doit se comporter de manière à protéger la réputation de l'organisation
Risk Management	Access-Controlled	L'accès aux informations et aux fonctions du système doit être contrôlé à l'aide d'une gestion de privilèges des sujets demandant d'avoir accès. Les accès non-autorisés ne doivent pas être permis.

LA TAXONOMIE EST COMPLÉTÉ…



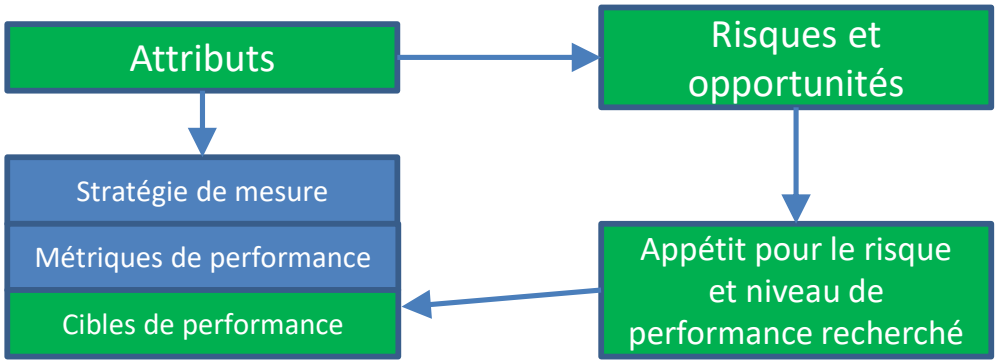
Maintenant que la taxonomie est complété (nos requis de sécurité on été normalisé et mis dans un format abstrait), nous pouvons nous attaquer à la création des profils.

ANALYSE DE RISQUE « IN A NUTSHELL »

4 Évaluer les impacts potentiels des différentes risques (Menaces & Opportunités)

5 Identifier et définir l'appétit et/ou la tolérance au risque de l'organisation ainsi que les niveaux de performances de la sécurité qui sont attendus

6 Établir les cibles de performance



APPROCHE BASÉ SUR LES IMPACTS POTENTIELS (SCÉNARIOS)

4 Évaluer les impacts potentiels des différentes risques (Menaces & Opportunités)

L'impact s'exprime selon les conséquences négatives ou positives d'évènement déterminés sur le BDS ou l'attribut

Un impact négatif s'exprime selon :
- Une réduction de la performance d'un attribut ou d'un BDS
- Un échec à rencontrer la performance attendu
- Une menace

Un impact positif s'exprime selon :
- Une amélioration de la performance d'un attribut ou d'un BDS
- Un succès à rencontrer ou dépasser la performance attendu
- Une opportunité

CIBLES DE PERFORMANCES ET TOLÉRANCE AU RISQUE

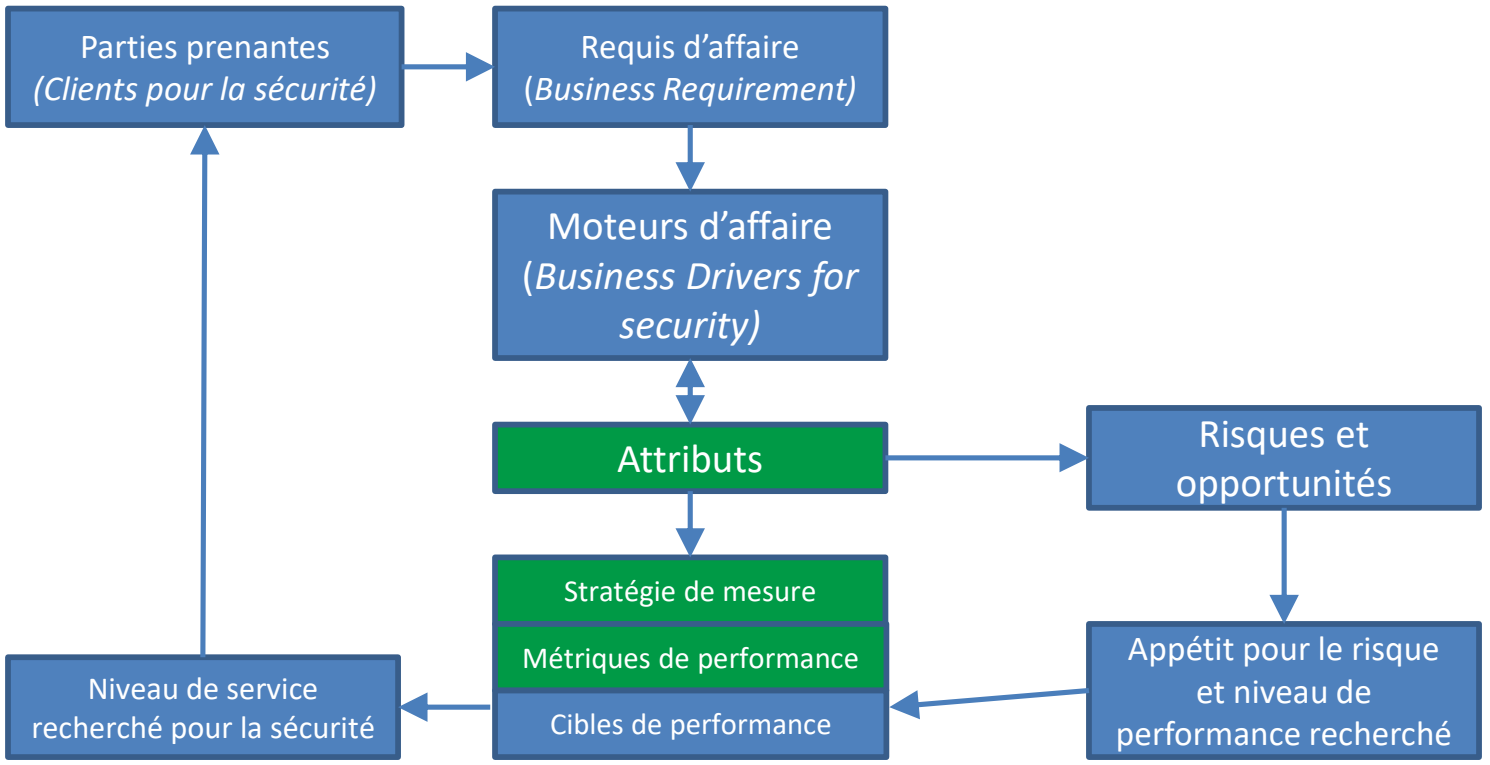
5 Identifier et définir l'appétit et/ou la tolérance au risque de l'organisation ainsi que les niveaux de performances de la sécurité qui sont attendus

6 Établir les cibles de performance

Les cibles performances qu'on établi pour les BDS et les attributs sont, par définition, les limites que l'organisation est prête à accepter pour ce qui est considéré un risque acceptable

- La cible est un objectif d'entreprise, orienté sur la sécurité
- Un échec à atteindre cette cible devrait être considéré comme inacceptable pour une organisation
- Il s'agit d'un paramètre clé pour rendre l'évaluation et l'analyse de risque moins subjective

MESURES ET MÉTRIQUES



CATÉGORIES DE MESURES

Complétude
- Avons-nous l'ensemble des éléments ?
- Est-ce que le système est considéré comme intègre selon une approche reconnue (e.g. S.E.A) ?

Conformité
- Est-ce que la maintenance du système est effectué de manière correct ?
- Avons-nous suivi les feuilles de route d'architecture d'entreprise ?
- Avons-nous suivi les principes directeurs, les politiques et les directives en application pour ce système ?

Est-ce que le système a de la valeur pour l'organisation ?

Assurance
- Est-ce que le système opère de manière simple et efficace ?
- Sommes-nous certains qu'il a été assemblé correctement ?
- Est-ce que le système répond à la demande ?

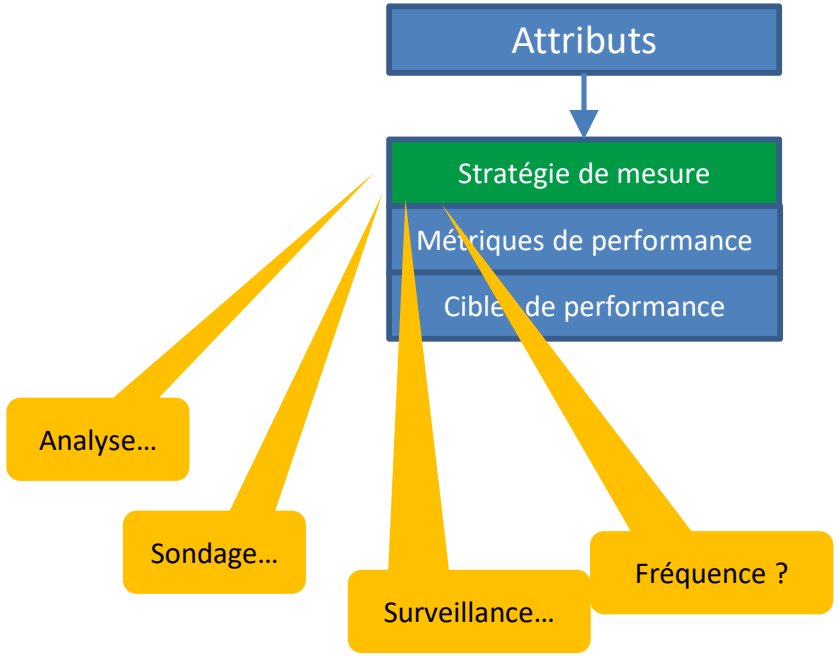
Conformité
- Est-ce que le système est calibré correctement ?
- Est-ce que tous les composantes de l'architecture fonctionnent bien ensemble ?
- Est-ce que nous exploitons le système correctement ?

QUELLE APPROCHE PRENDRE POUR MESURER ?

7 Construire une approche pour mesurer la performance

À très haut niveau, les éléments pour permettre une mesure efficace de la performance sont :

- Aligner avec les besoins de l'organisation
- Dans un langage approprié à l'auditoire cible
- Spécifique à la culture organisationnelle

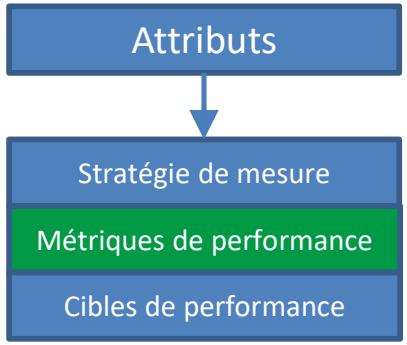


DÉFINITION DES MÉTRIQUES DE PERFORMANCE

8 Définir les cibles de performance attendues face au BDS ou l'attribut

Lignes directrices à suivre :

- Les données utilisées pour calculer les métriques devraient être déjà disponibles
- Les métriques devraient être calculés et construites de manière indépendante des groupes ayant un partit pris
- Le type de métrique utilisé peut changer selon l'évolution de la maturité de la sécurité ou du système, e.g. Lorsqu'un système devient conforme au attente, il ne sert plus à rien de mesurer le niveau de conformité de celui-ci. Un changement vers un autre type de métrique devient pertinent… performance ?
- Les métriques doivent être testées avant le « go live »
- Gérer les attentes des parties prenantes



TYPES DE MÉTRIQUES

8 Définir les types de métriques

Soft metrics :

- Qualitative
- Subjective
- Ouverte à l'interprétation et à l'opinion du lecteur (e.g. l'autorité qui défini la cible ou un auditeur)

Hard metrics :

- Quantitative ou binaire
- Objective
- Fixe, aucune interprétation possible

Descriptive :

- Description de l'état actuel de l'objet

Comparative :

- Description de l'état actuel de l'objet qu'on veut mesurer en comparaison d'un autre objet similaire dans un endroit différent ou à un moment différent

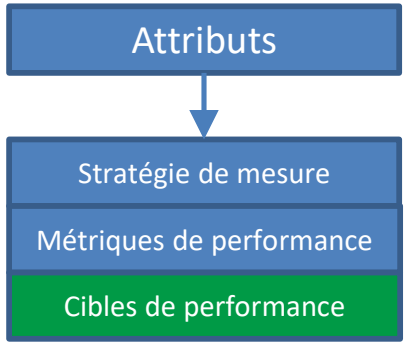
Prédictive :

- Description de l'état actuel de l'objet qu'on veut mesurer en relation avec son évolution dans le temps afin de prédire un état futur potentiel

CADRE CONCEPTUEL

8 Définir les cibles de performance attendues face au BDS ou l'attribut

Business Requirement				
Business Driver for Security				
Attribute (with risk-proportional Performance Target)	Measurement Category	Measurement Approach	Metric Type	Metric Format *-value - percentage - volume - etc.*
Cost-Effective	*Justification*	*Monitor*	*Predictive*	*Value*

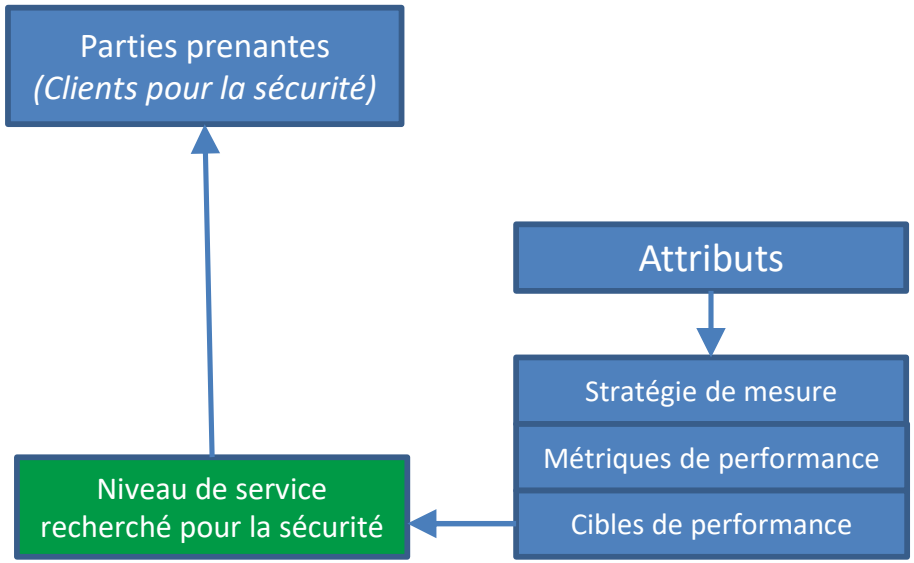


DÉFINIR LES NIVEAUX DE SERVICE DE SÉCURITÉ

9 Définir les niveaux de service de sécurité attendu par l'organisation face au BDS

Considérations :

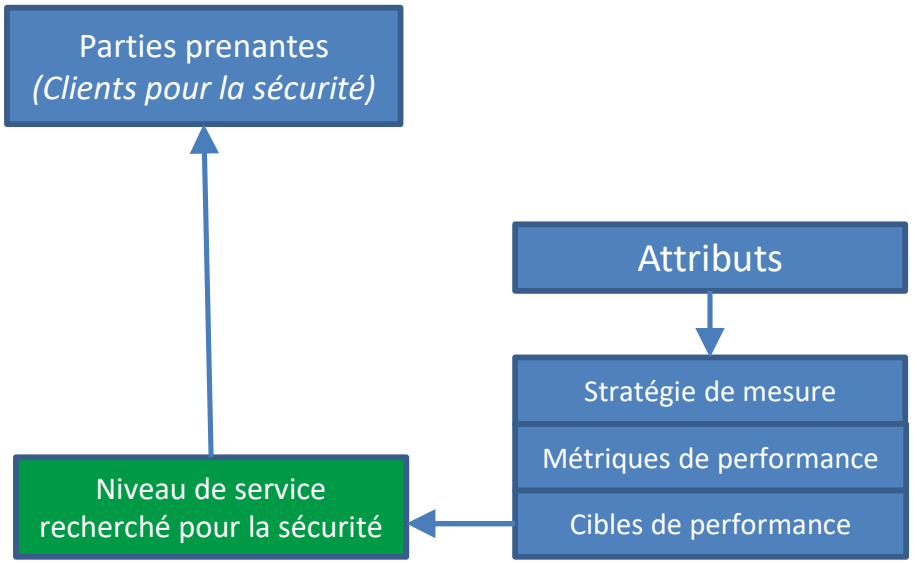
- Quels sont les attentes du responsable de domaine (e.g. VP E-business) de la part de l'AS par rapport au BDS qu'ils nous a exprimé ? En tant que responsable, est-il confortable ?
- Qu'est-il attendu de la part du responsable de domaine pour pouvoir offrir le service à l'entreprise ?



DÉFINIR LES NIVEAUX DE SERVICE DE SÉCURITÉ

9 Définir les niveaux de service de sécurité attendu par l'organisation face au BDS

PDG : *« Je ne veux pas savoir combien de virus ont été bloqués ce matin ! Ce que je veux savoir, c'est comme l'AS qui me coûte si cher m'aide à atteindre mes requis d'affaire. »*



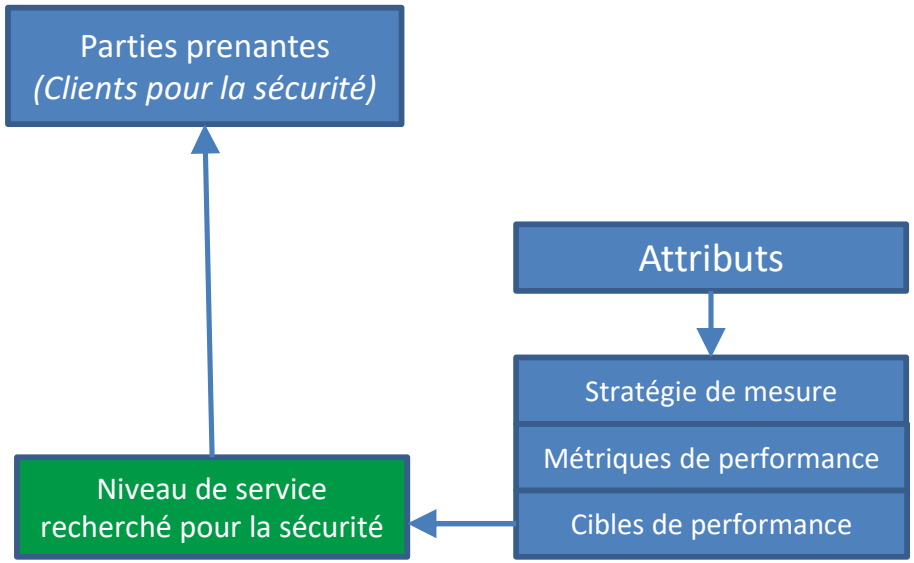
Rappel :

Être orienté sur l'organisation signifie de na jamais perdre de vue les buts, les objectifs et les facteurs clé de succès de l'organisation… tout en assurant que la stratégie de sécurité supporte, améliore et protège ces buts, objectifs et facteurs de succès, de manière démontrable.

DÉFINIR LES NIVEAUX DE SERVICE DE SÉCURITÉ

10 Feedback

Le feedback est effectué grâce aux différents rapports de performance en fonction des SLA entendus, dans le langage approprié pour l'auditeur et en lien avec les requis d'affaire, les BDS et les attributs qui le concerne



STRUCTURE POTENTIELLE POUR UN PROFIL D'ATTRIBUT

Attribute	Attribute Classification	Attribute Definition	Owner (Accountable Authority)	Performance Target	Recommended Measurement Category	Recommended Measurement Approach	Recommended Metric Type
"Error-free"	Operational Attribute	*"The system should operate without producing errors."*	System Owner	99.9% of all system output is correct	Performance	Random sample of system output conducted on a daily basis	Percentage

EXEMPLE COMPLET (ESA P.97)

BSD	Maintenir la nature privée des informations personnelles des clients
Sélection de(s) l'attribut(s)	Private
Définition	La nature privée des informations des clients être protégé en fonction des lois actuellement en vigueur sur la protection des renseignements personnels dans chaque pays qui héberges l'entreprise.
Type de métrique	Hard : Selon le nombre d'incidents rapportés, incluant les tentatives infructueuses
Comment on mesure ?	On mesure le nombre d'incident par période et on les classes selon le type et la sévérité. On mesure l'efficacité à détecter et rapporter les incidents
Cible de performance	1 : Nombre maximum de fuite acceptable : 0 2: La durée maximum pour une tentative avant d'être rapporté : < 60 sec
Collecte & Évaluation	Nombre de fuite; Max, min et moyenne du délais avant qu'un incident soit rapporté;

EXERCICE – PROFIL D'ATTRIBUT (30 MINS)

1 Entretien au sujet des requis d'affaire avec un exécutif

Définir les BDS, attributs et profils

Entretien avec le CFO de Banque Toto :

«J'ai bien peur d'être plutôt sceptique à propos de la sécurité. Cela nous a coûté beaucoup d'argent par le passé sans démontrer aucun avantage tangible. Tous les plans que nous développons dans le cadre de cette initiative d'architecture doivent faire l'objet d'une analyse claire des coûts et des avantages. Je veux voir une démonstration claire d'un retour sur notre investissement. Je ne suis pas convaincu que la plupart de ce que nous appelons la «sécurité» présente un réel avantage commercial et, dans certains cas, il me semble que cela nuit réellement aux l'activités commerciales. »

EXERCICE – PROFIL D'ATTRIBUT

2 Identifier les moteurs d'affaire (*Business drivers for security*) des parties prenantes

Entretien avec le CFO de Banque Toto :

«J'ai bien peur d'être plutôt sceptique à propos de la sécurité. Cela nous a coûté beaucoup d'argent par le passé sans démontrer aucun avantage tangible. Tous les plans que nous développons dans le cadre de cette initiative d'architecture doivent faire l'objet d'une analyse claire des coûts et des avantages. Je veux voir une démonstration claire d'un retour sur notre investissement [BDS1]. Je ne suis pas convaincu que la plupart de ce que nous appelons la «sécurité» présente un réel avantage commercial [BDS2]et, dans certains cas, il me semble que cela nuit réellement aux l'activités commerciales.[BDS3]»

Échantillon des BD de sécurité	
BDS1	S'assurer que la sécurité a un coût avantageux et procure une bonne valeur.
BDS2	S'assurer que la sécurité mise en place est appropriée au système et à l'organisation
BDS3	Préserver la productivité des ressources
BDS4	Maintenir la confiance dans la protection
BDS5	Fournir un environnement de confiance

Cost-Effective, *efficiente, mesured*

Productive, *Business Enable*

Accurate, informed, supported, *Efficient*

Trusted, protected

EXERCICE – PROFIL D'ATTRIBUT (30 MINS)

1 Entretien au sujet des requis d'affaire avec un exécutif

Définir les BDS, attributs et profils

Entretien avec le VP-Marketing de Banque Toto :

«Un élément important de notre stratégie commerciale au cours des dernières années a été de développer des partenariats de coentreprises… [notre société] et le partenaire concerné doivent se donner mutuellement accès aux systèmes d'information d'entreprise, tout en maintenant leur indépendance et leur propre niveau de contrôle. Nous partageons certaines choses, mais pas tout. Notre architecture de sécurité doit prendre en charge cette situation. »

EXERCICE – PROFIL D'ATTRIBUT

2 Identifier les moteurs d'affaire (*Business drivers for security*) des parties prenantes

Entretien avec le VP-Marketing de Banque Toto :

«Un élément important de notre stratégie commerciale au cours des dernières années a été de développer des partenariats de coentreprises… [notre société] et le partenaire concerné doivent se donner mutuellement accès aux systèmes d'information d'entreprise, tout en maintenant leur indépendance et leur propre niveau de contrôle[BDS1]. Nous partageons certaines choses, mais pas tout[BDS2]. Notre architecture de sécurité doit prendre en charge cette situation. »

	Échantillon
BDS1	Protéger les partenaires avec lesquels l'organisation fait des affaires d'abus, de pertes de revenus ou de PII
BDS2	S'assurer que les employés qui utilisent le système on le bon niveau d'accès tout en préservant le principe du « need to know ».

Protected, *Auditable, private, confidentiel*

Access-controlled, Private, Authorized, Protected,*enforceble*

MATRICE SABSA

Business Drivers for Security

Attributs

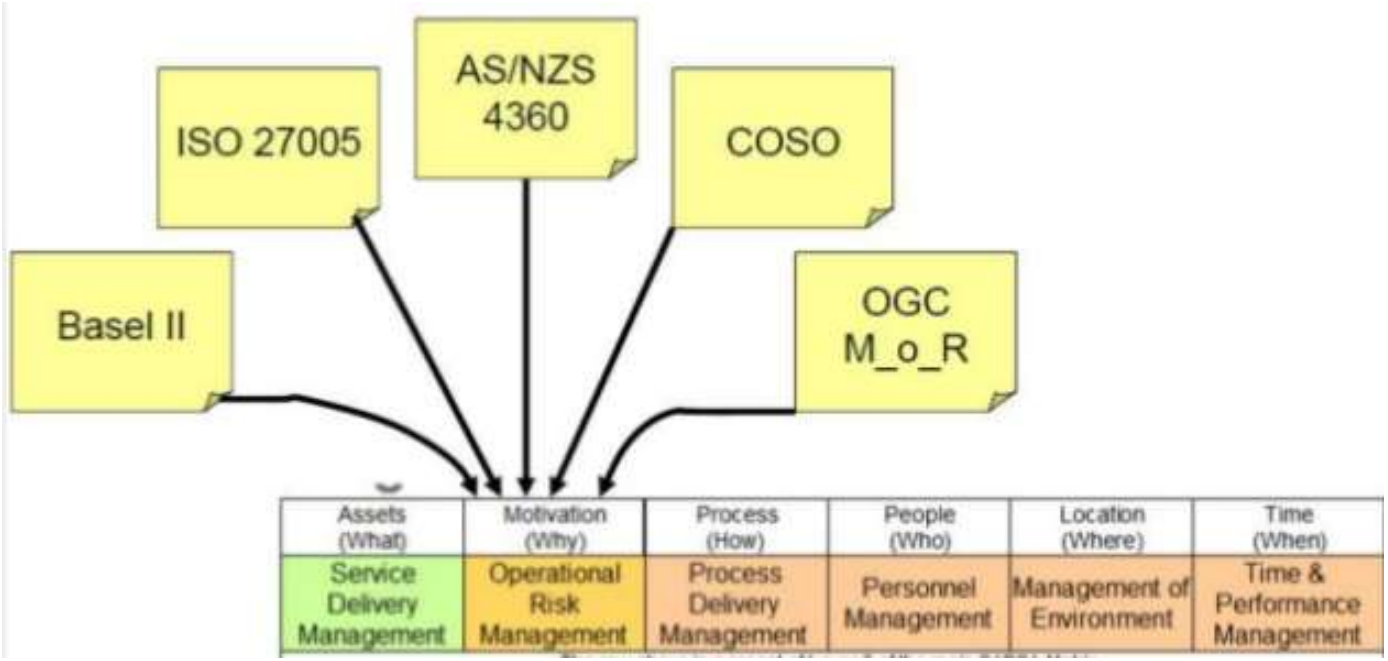
Risques et opportunités

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Management Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

Évaluation des risques opérationnels

UNIVERSITÉ DE SHERBROOKE

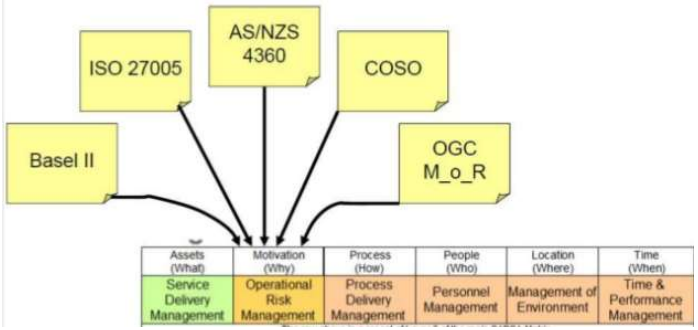
ALIGNEMENT SUR LES CADRES STANDARDS



DÉFINITION DE CE QU'EST LE RISQUE OPÉRATIONNEL

Basel II

« Le risque de perte provenant d'une défaillance ou d'une implémentation inadéquate de processus internes, de systèmes, d'évènements ou d'une mauvaise compréhension de ceux-ci par les individus… donc une mauvaise utilisation de ceux-ci »



MODÉLISATION DES RISQUES

Variables de bases à évaluer :

- *Actifs : Ce qui a de la valeur pour l'organisation*
- *Menaces : Évènement dommageable pour les actifs de l'organisation*
- *Impacts : Le résultat d'une menace qui se réalise et qui cause un tord aux actifs ciblés*
- *Vulnérabilités : Faiblesse au niveau des processus d'opération ou des systèmes qui pourra permettre à une menace de se réaliser en exploitant un actif et causant un impact*

Chance d'occurrence (Likelihood)

- Niveau de la menace, il s'agit de la chance que l'évènement se matérialise durant un période donnée de temps
- Niveau de vulnérabilité, il s'agit qu'une menace exploite avec succès un actif et créé un impact

ÉTAPES D'ÉVALUATION DES RISQUES

1. Les actifs de valeurs pour l'organisation
2. Quels sont les menaces qui mettent à risque les actifs de l'organisation
3. Pour chaque menace, si elle se réalise, quel serait l'impact sur l'actif touché
4. Si c'est un important, quelles sont ses vulnérabilité et ses faiblesses ?
5. Est-ce qu'on peut réduire cette faiblesse ?
    1. Nouveaux contrôles
    2. Coûts
6. Quel est l'analyse coût/bénéfice de la réduction de la chance d'occurrence ?

ÉTAPES D'ÉVALUATION DES RISQUES

0. Pour quelles raisons ?

Impact d'affaire:

- Sécurité
- Opérations
- Règlementaire

1. Quoi et où?

Quels sont les actifs les plus critiques ?

À quels endroits sont-ils?

- Systèmes, Locations

2. Comment ?

Comment l'entreprise peut-elle être impactée **(3)** ?

- Vulnérabilité **(4)**
- Scénario de tests

5. Plans de mitigation (projets)

6. Quand et combien ?
Mesure de l'impact sur le risque dans le temps et coûts associés

Progrès des priorités

Stratégie de cybersécurité

UNIVERSITÉ DE SHERBROOKE

MODÉLISATION DES MENACES

Domaines des menaces

Domaine	Description	Agents de menaces
Individus	Pertes causées par : • Violation volontaire ou involontaire (négligence) des politiques internes • Erreurs humaines	• Employés actuels ou passés • Candidats potentiels
Processus	Pertes causées par : • Déficiences dans une procédure • Absence de procédure adéquate • Faute dans le suivi d'une procédure	• Employés • Clients • Fournisseurs • Fournisseurs de services • Agents, partenaires ou public
Systèmes	Pertes causées par : • Bris imprévu • Résilience insuffisante	• Faute technique
Externe	Pertes causées par : • Désastre naturel • Désastre causé par l'homme • Actions malicieuses ou négligence des tierces parties • Actions autorisées des tierces parties	• Évènement naturel • Accidents • Agents malicieux • Agents négligents

MODÉLISATION DES MENACES

Catégorie des menaces

- Base de donnée compréhensive des différentes catégories de menaces, cartographiées par domaine (ESA p.192)

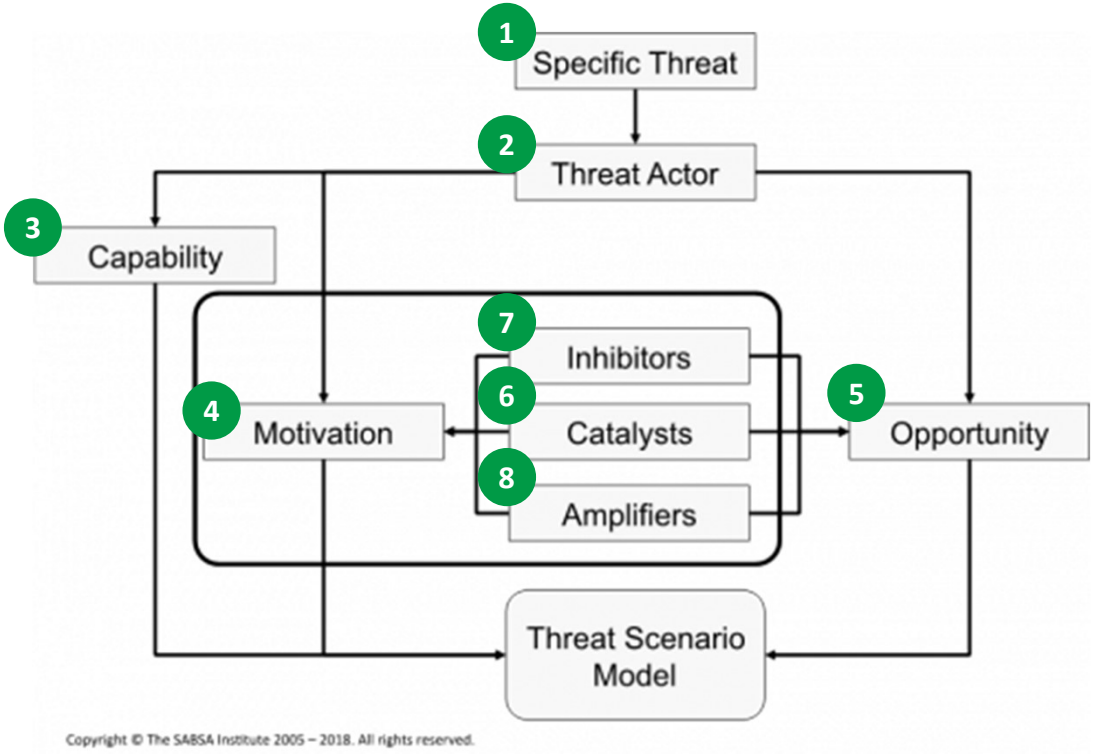
MODÉLISATION DES AGENTS MENACES

Threat Actors	Intent	Access	Trust	Skills	Resources	Common Tactics/Actions	Description	Scope
Employee Reckless	Non-Hostile	Internal	None	Adept	Limited	Benign shortcuts and misuse of authorizations, “pushed wrong button”	Current employee who knowingly and deliberately circumvents safeguards for expediency, but intends no harm or serious consequences	n
Employee Untrained	Non-Hostile	Internal	Administrator	Moderate	Limited	Poor process, unforeseen mistakes, “pushed wrong button”	Current employee with harmless intent but unknowingly misuses system or safeguards	y
	Non-Hostile	Internal	Employee	None	Limited	Poor process, unforeseen mistakes, “pushed wrong button”	Current employee with harmless intent but unknowingly misuses system or safeguards	y
Information Partner / Technology Supplier Untrained	Non-Hostile	Internal	Limited	Operational	Moderate	Poor internal protection of company proprietary materials, Remote access to operational technology	Someone with whom the company has voluntarily shared sensitive data / provided access to the operational technology	y
Activist	Hostile	External	None	Adept	Moderate	Electronic or physical business disruption; theft of business data	Highly motivated but non-violent supporter of cause	y
	Hostile	External	None	Adept	Moderate	Public announcements for PR crises, theft of business data. Smear campaigns and dissemination of misinformation.	Attention-grabber who may employ any method for notoriety; looking for “15 minutes of fame”	y
	Hostile	External	None	Adept	Moderate	Brand Dilution and Devaluation	Unauthorized use of CN's brands and logos on sites containing objectionable content, such as pornography, or claiming partnership, affiliation or other endorsements.	y

Modélisation détaillée des agents de type individus

SCÉNARIO DE MENACE

1. Une menace sélectionné de la base de donnée ou d'une autre source documentée
2. Un acteur recommandé dans une des matrices d'acteurs de menaces
3. Niveau de ressources auxquels l'acteur peut avoir accès
4. Les motivations de l'acteur
5. Description de l'opportunité offerte à l'acteur (niveau d'accès, faiblesse, etc)
6. Changement à l'état actuel qui pourrait causé le déclanchement des hostilités
7. Ce qui pourrait retenir/empêcher l'acteur de passer aux actes
8. Ce qui pourrait encourager l'acteur à passer aux actes



TABLES DES MENACES (ESA P.203-205)

Menaces

Évènement naturels, Accidents, Défaillances technologiques, Individus, Organisations Externes

Capacités des menaces

Financière, Technique, Logiciel, Expertise, Littéraire, Expérience, Habiletés, etc

Motivation

Gain personnel ou de groupe

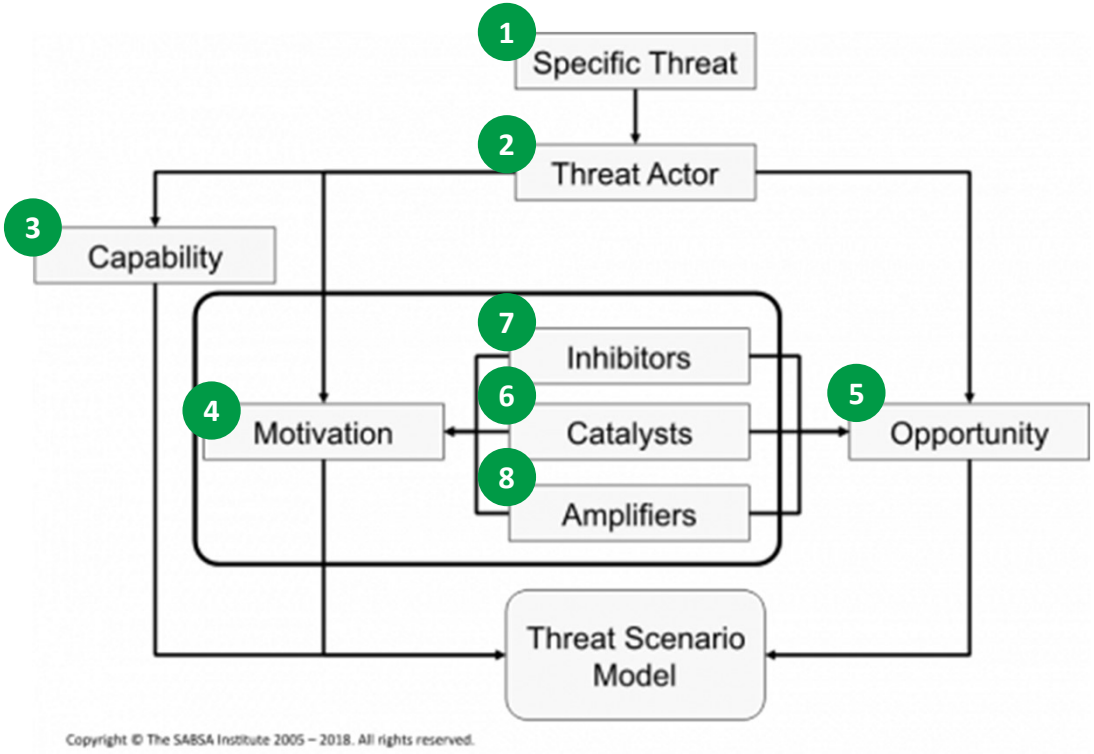
Catalyseur, inhibiteur ou amplificateur

Peur de se faire prendre ou d'échouer, accès limitant l'opportunité, Coût élevé, Opinion du public

SCÉNARIO DE MENACE – EXEMPLE (P.202)

1. Injection de code malicieux dans une application dans le but de saboter l'organisation
2. Un ancien employé du groupe de développement
3. Possède tous les outils requis
4. Revenge
5. Accès complet à l'environnement de développement
6. Congédiement
7. La peur de se faire prendre
8. Perception que le code peut être bien camouflé

Scénario de menace



SCÉNARIO DE MENACE - SIMPLIFIÉ

Scenario #	Threat agent	Threat action	Type of impact
Generic scenarios (used to think about system specific ones)			
GS1	Threat	is abusing access rights, leading to	(C I A) loss of
GS2	Employees	are generating errors in OT system creating a	(I A) Loss of
GS3	Employees	are inputting information incorrectly in OT system creating a	(I) Loss of Integrity
GS4	Employees	damaged OT system creating a	(A) Loss of Availability

Scenario #	Threat agent	Threat action	Type of impact	Business Impact
GS30	Cyber Vandal	Create a service interruption using DOS techniques in BOS, ITCM or TMDS , leading to inability of operate	(A) Loss of Availability	Inability to operate
GS29	Cyber Vandal	Break in a critical PTC/OT systems[1] leading to unauthorized changes on systems and/or information provoking safety mishaps and/or delays on operations	(I A) Loss of	Safety mishaps, Delays on operations
GS12	Cyber Vandal	Using obsolete technologies not able to meet cyber security requirements, leading to exploit vulnerabilities to break critical PTC/OT systems[1] to provoke safety mishaps and/or delays on operations	(I A) loss of	Safety mishaps, Delays on operations

CARTOGRAPHIE DES ACTIFS – SANS INSTITUTE

Table 1 - Asset Attributes

Attribute		Description
Unique ID		A unique ID for each asset should be assigned. Examples of a unique numbering scheme include information assets - CA.IN.01, network assets - CA.NT.01, and subsystem assets - CA.SS.01.
Description		A description of the asset that is meaningful to a business owner.
Ownership		Identification of the individual or organization who owns the asset.
Location		Physical and/or logical location information of the asset.
Security Categorization		Impact or injury assessment of confidentiality, integrity and availability is performed during a security categorization process to create a statement of sensitivity for the critical assets in the organization.
C	**Confidentiality**	Confidentiality impact assessment of High, Medium, or Low
I	**Integrity**	Integrity impact assessment of High, Medium, or Low
A	**Availability**	Availability impact assessment of High, Medium, or Low
Value		Monetary value of the assets.

PROFILE DES MENACES – SANS INSTITUTE

Table 3 - Cyber Criminal Threat Actor Profile

Name:	**Cyber Criminal**
ID: TA.E.01	
Description: Cyber criminals hack computer systems for financial gain.	
Relationship: External	**Region of Operation:** Eastern Europe, North America
Motive: Financial gain	**Intent:** Deliberate, Competitive
Capability: High technical capability, well-funded, large number, stealthy, patient and persistent, and high intensity.	
Target Victim: Financial, Retail, Food Industry.	
Action: Cyber criminals and state-sponsored threat actors often use the same tools but will usually leave a different attack footprint. Financially motivated criminals will not be as persistent as espionage motivated state-sponsored threat actors who wish to maintain control within a target for a long period of time. These threat actors will use tampering (physical), brute force (hacking), spyware (malware), capture stored data (malware), adminware (malware), RAM scrapers (malware).	
Targeted Asset: Automatic Teller Machines (ATM), Point of Sale (POS) controller, POS terminal, Database, Desktop.	
Objective: Steal credit card numbers, bank information, and social media and email account information and sell them on the black market.	

MODÈLE DE RISQUE (P.206)

ID	BDS	Attribut	Security Requirement	Menace	Impact	V-Impact	Vulnerabilité	V-Vuln	Cat-Risk	Obj. Control	Cible Vuln	Cat-Mitigated Risk
BD1	Les affaires sont de plus en plus orientées sur le client	Trusworthy Private Confidential	Les clients qui nous confient leurs informations personnelles doivent se sentir en confiance et savoir qu'il n'y aura pas de fuite	PII exposé à des sujets non autorisés	Perte de confiance	H	Control inadéquat au niveau de la protection de l'information	H	A (Red)			

1 2 3 4 5

Objectifs de contrôles

1. **BDS et attributs selon le profilage d'attribut**
2. **Évaluation des menaces** : Selon les scénarios de menaces développés. Un BDS peut avoir plusieurs scénarios de menace reliés
3. **Évaluation de l'impact** : Une fois que nous avons les moteurs et les attributs, nous pouvons décrire et évaluer l'impact potentiel
4. **Évaluation de la vulnérabilité** : Faire une évaluation des forces et faiblesses du système, des individus, des processus reliés au BSD. Il faut s'assurer de conduire cette évaluation en abstraction de toute mesure déjà en place. Ceci permet une meilleure vision des Objectifs de contrôle à mettre en place
5. **Catégorisation du risque** : Calculé selon V-Impact et V-Vuln

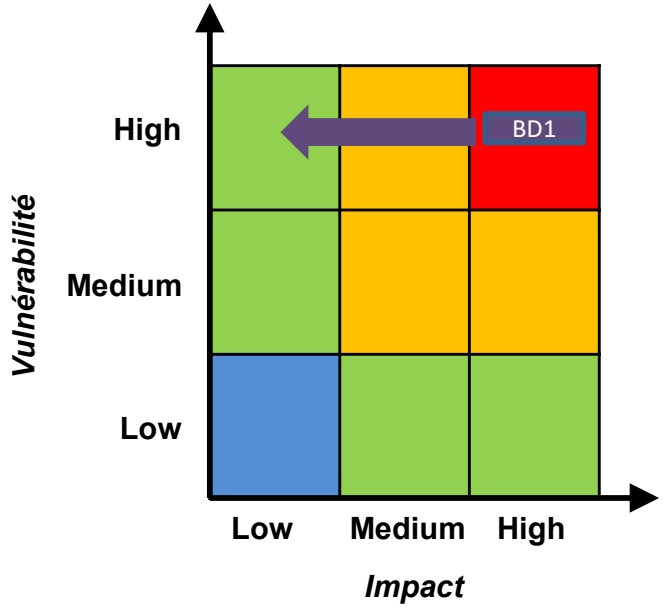
MODÈLE DE RISQUE (P.206)

ID	BDS	Attribut	Security Requirement	Menace	Impact	V-Impact	Vulnerabilité	V-Vuln	Cat-Risk	Obj. Control	Cible Vuln	Cat-Mitigated Risk
BD1	Les affaires sont de plus en plus orientées sur le client	Trusworthy Private Confidential	Les clients qui nous confient leurs informations personnelles doivent se sentir en confiance et savoir qu'il n'y aura pas de fuite	PII exposé à des sujets non autorisés	Perte de confiance	H	Control inadéquat au niveau de la protection de l'information	H	A (Red)			

1 2 3 4 5

Objectifs de contrôles

5. **Catégorisation du risque** : Calculé selon V-Impact et V-Vuln



Risque sévère	Actions immédiates requises
Risque significatif	Les actions devraient être planifiées rapidement
Risque acceptable	Sous surveillance
Risque négligeable	Aucune action requise

UNIVERSITÉ DE SHERBROOKE

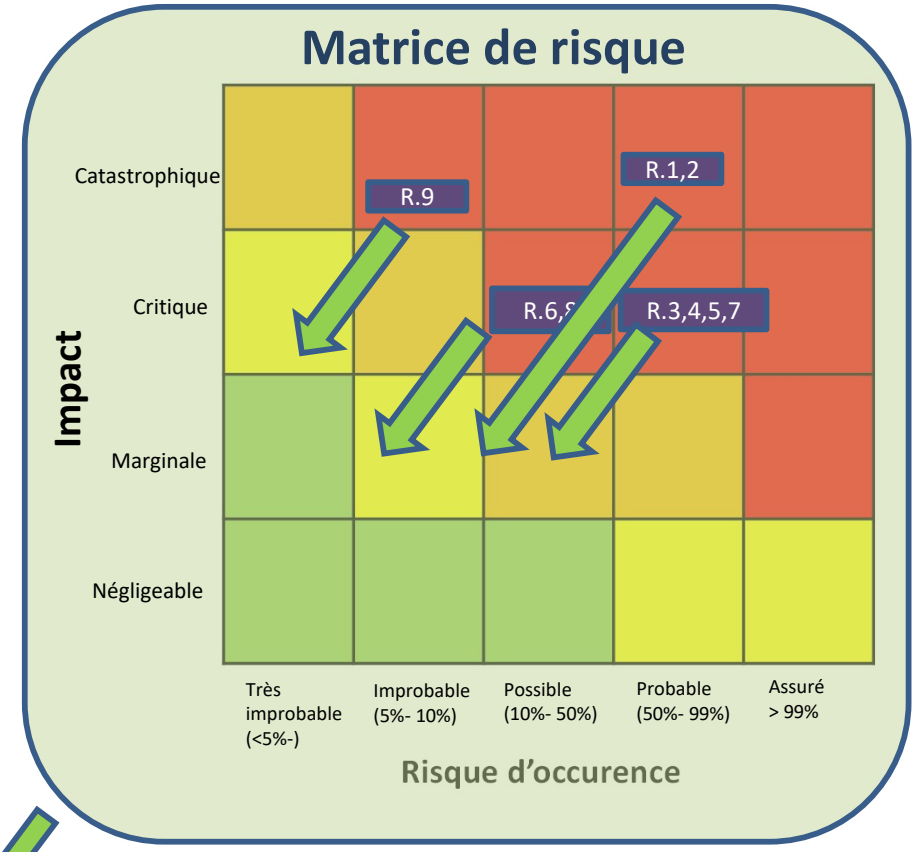
MODÈLE DE RISQUE (P.206) – UN PEU PLUS COMPLEXE

Menace	Description	Niveau
Cyber Vandal et Mobster	Création d'une interruption de service en utilisant une technique de DOS/DDOS ayant pour cible un actif critique de l'entreprise, menant celle-ci à une incapacité complète ou partielle d'opérer de manière normale. Autres risques reliés couvert par le plan de mitigation: • Attaque à distance des systèmes TI à partir du réseau interne ou externe; • Propagation de l'attaque • Abus de vulnérabilité connu • Comptes à hauts privilèges compromise • Attaque sur l'AD	

Plan de mitigation	Projets
- **Mettre en place une isolation et une segmentation sécuritaire du réseau**	**Infra - Isolation du réseau**
- S'assurer que les contrôle d'accès régissant les interconnexions entre les systèmes sont alignés avec les principes de "need to know and least privilege".	ICAM
- Assurer une saine gestion des accès distants aux systèmes de la SAQ	**Infra – Isolation du réseau** ICAM – Gestion des accès distants
- Assurer une révision périodique des accès aux systèmes critiques	ICAM
- Assurer que les normes de durcissement sont suffisante et appliqué aux systèmes critiques	Sécurité des systèmes et applications
- Implanter un processus de « Secure SDLC » afin de s'assurer que les nouveaux systèmes et nouvelles application n'introduisent pas de nouvelles surfaces d'attaque.	**Évolution du cadre de sécurité**
- Valider que les nouveaux systèmes supportent nativement les concepts de hautes disponibilités	Sécurité des systèmes et applications
- Assurer que les processus de surveillances réseau et de détection des fautes sont en place	**SOC and SIEM**
- Définir et implanter les processus de gestions des incidents	**SOC and SIEM**
- Définir les plans de réponse et de retour à la normale pour les DOS (R&R)	**SOC and SIEM + link with ops + DR**
- Définir les guides et les procédures supportant les contrôles mentionnés ci-haut	**Évolution du cadre de sécurité**

MODÈLE DE RISQUE (P.206) – UN PEU PLUS COMPLEXE

#	Scénarios de risques	E-com	BO corpo	X	Entrep
R.1	Attaque par Déni de service	√	√	√	?
R.2.a	Cyber intrusion à distance	√	√	√	√
R.3	Installation de logiciels malveillants à distance	√	√	√	√
R.4	Exploitation à distance de vulnérabilité causé par une obsolescence de nos logiciels	√	√	√	*
R.5.a	Abus d'accès logiques	√	√	√	√
R.5.b	Abus d'accès physique		√	√	
R.6	Saisie d'information incohérente		√		
R.7	Changements non authorisés aux systèmes	√	√	√	√
R.8	Changements non authorises aux données critiques de la SAQ	√	√		
R.9	Les clés d'encryption ont été compromise	√	√	√	√

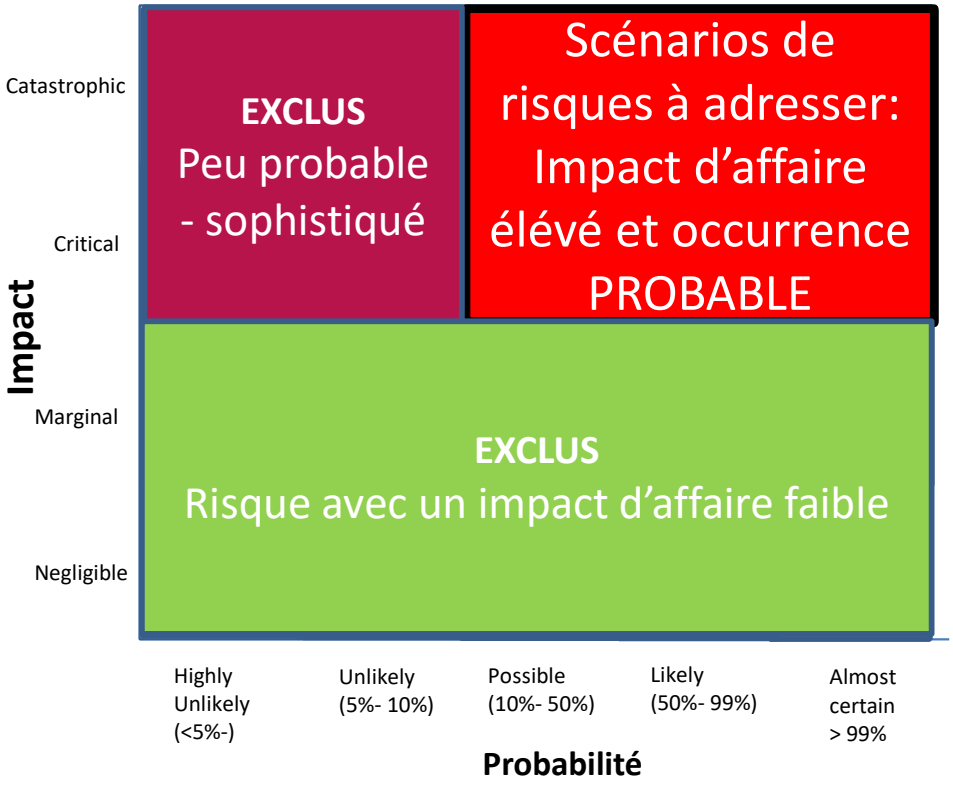


Réduction des risques à un niveau acceptable par l'entreprise suite à la mise en place des plans de mitigation.

UNIVERSITÉ DE SHERBROOKE

PRIORISATION DES RISQUES

Matrice de risques



Les scenarios de risque sélectionnés sont ceux qui présente un risque d'occurrence réel et qui pourraient avoir un impact significatif sur la capacité de la SAQ à conduire à bien sa mission d'affaire.

- En fonction de la tolérance au risque établis avec les différentes parties prenantes
- Définir la zone d'impact qui n'est pas acceptable
- Définir la zone de probabilité ou de vulnérabilité qui n'est pas acceptable
- Les scenarios de risque sélectionnés (zone rouge) sont ceux qui présente un risque d'occurrence réel et qui pourraient avoir un impact significatif sur la capacité de l'organisation à conduire à bien sa mission d'affaire.

EXERCICE – MODÈLE DE RISQUE (30 MINS)

1 Entretien au sujet des requis d'affaire avec un exécutif

À l'aide des BDS, attributs et profils, construire les scénarios de menace et le modèle de risque.

Entretien avec le VP-Marketing de Banque Toto :

«Un élément important de notre stratégie commerciale au cours des dernières années a été de développer des partenariats de coentreprises… [notre société] et les partenaires concernés doivent se donner mutuellement accès aux systèmes d'information d'entreprise, tout en maintenant leur indépendance et leur propre niveau de contrôle. Nous partageons certaines choses, mais pas tout. Notre architecture de sécurité doit prendre en charge cette situation. »

Processus d’affaire et les besoins en sécurité

UNIVERSITÉ DE SHERBROOKE

INTERACTIONS ENTRE ENTITÉS D'AFFAIRE

Les différentes interactions entre les entités ont tous besoins de :

- Identification des entités : Afin de s'assurer du caractère unique de chacune d'elle
- Authentification : Une démonstration que l'entité est bien celle qu'elle prétend être
- Autorisation : Gestion de ce que l'entité peut faire

Ces entités peuvent être des individus, des entités corporative ou des entités logiques (e.g. applications)

PROCESSUS DE TRANSACTIONS ÉLECTRONIQUES

Les processus portant sur les transactions en ligne doivent revue avec diligence :

- Besoins de conformité interne
- Besoins de conformité externe
- Large portefeuille de menaces
- Impact sur l'organisation souvent important
- Besoins en sécurité en constante évolution

Les individus

LES INDIVIDUS

Les parties prenantes à maitriser afin de pouvoir déterminer les requis et moteurs de sécurité :

- Chaine hiérarchique : afin de comprendre son impact sur les autorisations, la gouvernance et le contrôle de l'organisation
- Chaine d'approvisionnement : Les relations de confiance en place avec les fournisseurs, les modèles de confiance implicite et les risques que ça induit
- Externalisation TI : Gestion des politiques de sécurité ainsi que les risques qui viennent avec cette décision
- Partenaires stratégiques : Le partage d'information et de responsabilité
- Fusions, aquisitions, etc : Comment l'architecture de sécurité réagit à des changement organisationnel de cette ampleur.

Localisation

UNIVERSITÉ DE SHERBROOKE

LE MODÈLE GÉOGRAPHIQUE

Le modèle géographique doit considérer les aspects reliés à la géographie organisationnelle et aspect reliés aux localisations physique de l'organisation.

Considération possible pour l'architecture d'entreprise :

- Langues
- Fuseaux horaires
- Lois et règlements
  - Protection des renseignements personnels
  - RGPD/GDPR

De plus, l'architecture de sécurité doit prendre en compte les aspects reliés à la sécurité d'être multi-site :

- Travail à distance
- Accès à distance des fournisseurs
- Employés multi-site
- Contexte Awareness Security

RGPD

Lois européenne touchant les données personnelles…

- prénom, nom
- date de naissance
- Genre
- Lois européenne touchant les données personnelles
- Photo
- posts sur réseaux sociaux

et les données sensibles et biométriques

- Données de santé
- Origines ethniques
- Sexualité
- Opinions politiques
- Croyances religieuses
- ADN
- Empreintes digitales
- Reconnaissance faciale

RGPD

Personally Identifiable Information (PII)

Une information qui peut servir à reconnaitre un individu ou à l'identifier dans un certain contexte

(ex : vos données de localisation sur GoogleMaps)

Le consentement est primordial

La RGPD vise à redonner le pouvoir et la libre utilisation des données aux individus.

Et le choix

Avoir le choix de ne pas communiquer ses données, sans subir de préjudices (toutefois l'utilisateur peut ne plus avoir accès au service ou à l'intégralité du service).

RGPD

Le but doit être explicite

Le but de la récolte des données doit être mentionné explicitement à l'utilisateur (ex : "vos données seront utilisées pour l'envoi de newsletter").

Le consentement doit être explicite

Son consentement doit être intelligible par une "action déclarative" de sa part, sans ambiguïté (ex : Je suis d'accord pour que mes données soient réutilisées pour…)

Transparence

L'utilisateur peut accéder à tout moment à ses données

Réversibilité du consentement

L'utilisateur peut retirer son consentement à tout moment et réclamer la suppression de ses données s'il le souhaite.

RGPD

La RGPD a de spéciale qu'elle est de portée extraterritoriale.

Sont concernés, toutes les entreprises qui :

- ❏ commercialisent des produits et services au sein de l'UE
- ❏ possèdent des bureaux en zone UE
- ❏ développent des sites internet et apps mobiles disponibles dans des langues de la zone UE
- ❏ affichent des prix de vente en devises de l'UE
- ❏ possèdent des noms de domaine provenant de l'UE

RGPD

La réglementation est obligatoire si l'entreprise :

❑ récolte et gère régulièrement des données clients

❑ a plus de 250 salariés

❑ manipule des données clients pour le compte de clients B2B (de plus de 250 personnes)

❑ récolte et gère des données sensibles et biométriques

❑ récolte des données qui pourraient mettre en danger les droits et libertés des individus

Time Dependency

TIME DEPENDENCY MODEL

L'architecture contextuelle doit considérer les aspects temporels de la sécurité pour l'organisation :

- *Horomarquage (timestamp) des transactions*
- *Appliquer les notions de confidentialité et d'intégrité sans toucher la disponibilité*
- *Limites de temps organisationnelles*
  - *Système boursier*
  - *Système de loterie*

Semaine prochaine

À VENIR LA SEMAINE PROCHAINE

Semaine 5 – 07 février 2023

Lecture : ESA chapitre 10 – Architecture Conceptuelle (p.217-268) + notes supplémentaires

Bonne lecture !

Question ?