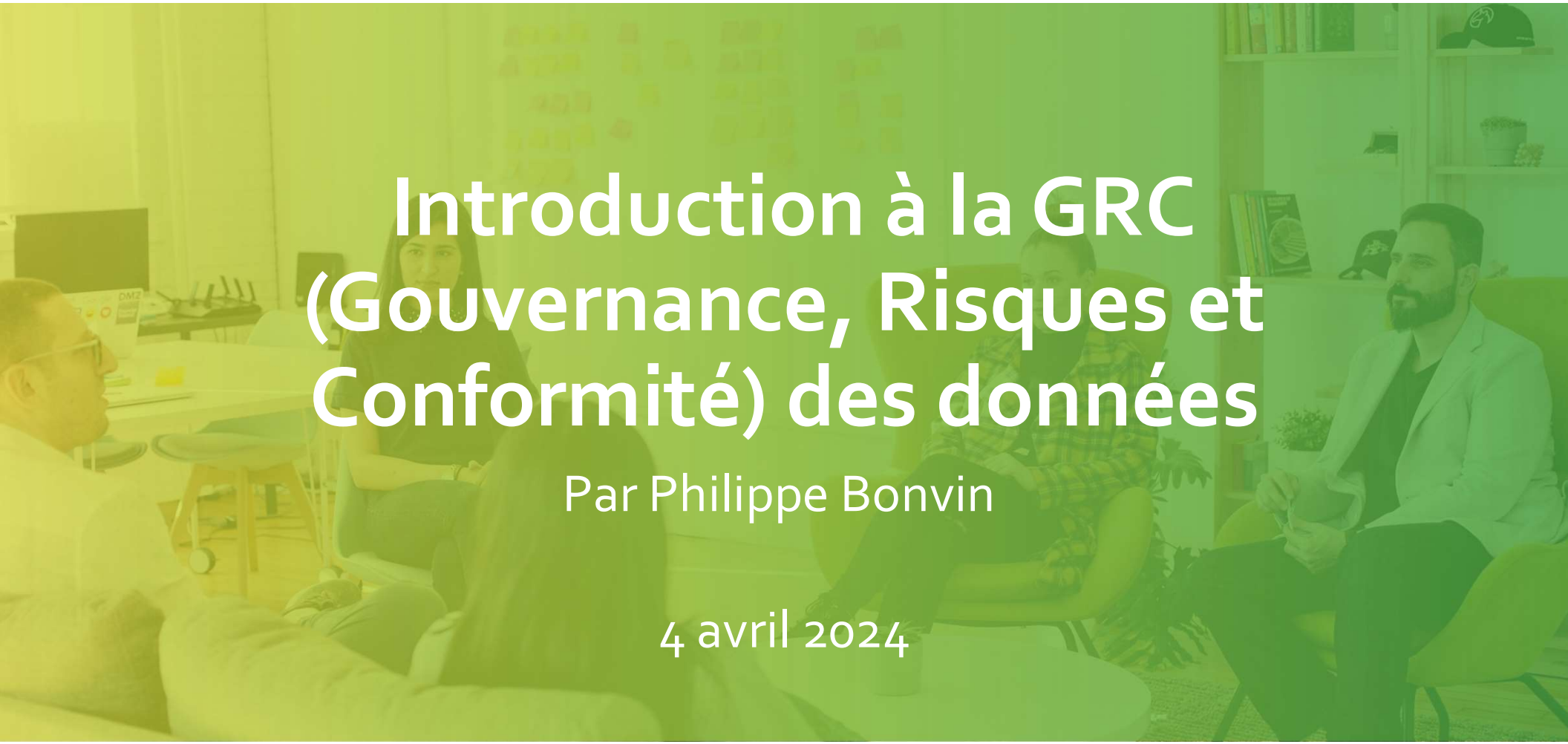


Introduction à la GRC (Gouvernance, Risques et Conformité) des données

Par Philippe Bonvin

4 avril 2024

SMP
SOCIÉTÉ SUISSE DE MANAGEMENT DE PROJET

CONGRÈS DU MANAGEMENT DE PROJET

UNIL | Université de Lausanne
HEC Lausanne

Bienvenue !

- Objectif : être capable d'identifier les éléments essentiels pour encadrer une saine gestion des données en entreprise.

- Pour cela :
  - Savoir identifier et gérer les risques liés aux données
  - Connaître le cadre législatif applicable
  - Connaître les principales normes à appliquer pour une bonne gouvernance

Agenda

1. Introduction à la GRC
2. Parlons gouvernance
3. Pilotage par les risques
4. Quelques notions de droit en protection des données
5. Les cadres stratégiques pour l'entreprise
6. Quelques contrôles techniques
7. Conclusion

Pourquoi parler de la GRC ici ?

La saine gestion des données se repose sur trois éléments fondamentaux :

- La disponibilité
- L'intégrité
- La confidentialité

Introduction à la GRC

Introduction à la GRC

La GRC n’est pas

La GRC est

La GRC en bref

Gouvernance

- Définition de la stratégie afin d'atteindre les objectifs d'entreprise
- Formalisation d'un cadre à l'aide des politiques et procédures d'entreprise
- Mesure de la performance des initiatives
- Standardisation des façons de faire

En bref, optimisation de la création de valeur pour l'entreprise.

La GRC en bref

Gestion des risques

- Identification et classification des actifs à protéger
- Evaluation des menaces par le recensement et l'évaluation de scénarios
- Mise en place de stratégies pour gérer les risques
- Définition des contrôles permettant de faire baisser les risques
- Surveillance du portefolio de risques

En bref, prise de décisions en toute connaissance de cause.

La GRC en bref

Conformité

- Identification des lois et règlement applicables
- Identification des régulations spécifiques à l'industrie
- Application de contrôles assurant le respect du cadre législatif
- Vérification de la bonne application du cadre

En bref, réduction des risques par l'application d'un cadre contraignant.


Parlons gouvernance

Qu’est-ce que la gouvernance ?

La plupart des entreprises existent pour fournir des services afin de créer de la valeur pour leurs parties prenantes. Les processus d'entreprise émanent de la mission, des objectifs et de la stratégie de l'entreprise.

La gouvernance garantit que l'entreprise se conforme aux lois et réglementations applicables et établit des structures organisationnelles matures pour aider à faire appliquer les principes de ***due care*** *and* ***due diligence.***

Gouvernance n’est pas direction !

La gouvernance se concentre toujours sur les aspects suivants :

- L'organisation fait-elle les bonnes choses ?
- Ces choses sont-elles faites immédiatement ?
- L'équipe fait-elle les choses dans les délais et dans les limites du budget ?
- Est-ce que nous optimisons continuellement les risques et obtenons-nous des bénéfices ?

Les 5 objectifs de la gouvernance TI

1. Alignement de la **stratégie TI** avec les **objectifs d'entreprise**
2. Livraison de **valeur** à l'organisation
3. Gestion de la **capacité** et mesure de la **performance**
4. Gestion des **ressources** et des **actifs**
5. Gestion des **risques** et **assurance de la conformité**

Pourquoi faire de la gouvernance ?

De nombreuses organisations comprennent mal l'objectif et la valeur de la gouvernance informatique, car peu de professionnels qualifiés maîtrisent la gouvernance informatique.

Les problèmes courants de gouvernance d'entreprise incluent des seuils de risque obscurs ou mal définis, un faux sentiment de confiance et une mesure inadéquate de la performance.

*Une gouvernance inefficace a un impact substantiel sur l'alignement des activités et la gestion des risques**. Un mauvais alignement peut entraîner une mauvaise identification des données sensibles, des services critiques et des contrôles de sécurité de qualité inférieure**.*

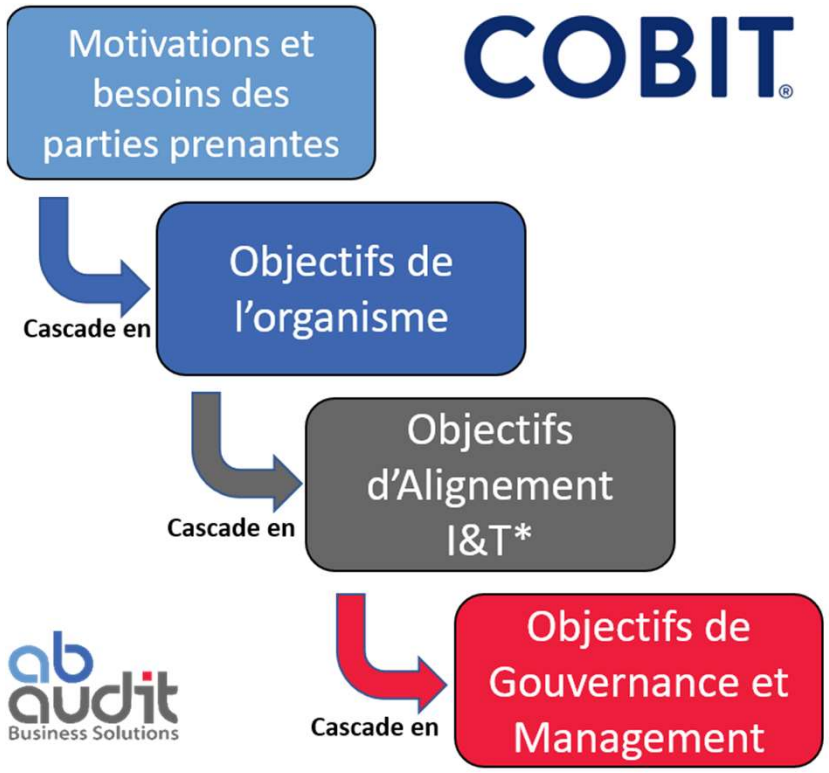
De plus, un mauvais alignement entre l'entreprise et l'informatique affaiblit la communication et les priorités, ce qui entraîne une mauvaise allocation des ressources et un manque de transparence dans la réduction réelle des risques.

Source: https://www.isaca.org/resources/news-and-trends/industry-news/2020/the-value-of-it-governance

La gouvernance en application

- Création d'une stratégie à un horizon de 3 ans
- Préparation d'un programme d'exécution à 1 an aligné avec la stratégie
- Comité de pilotage TI avec des représentants de la direction et des affaires
- Surveillance régulière de la bonne exécution du programme (rapports à la haute direction et établissement des KPI)
- Gestion des projets avec une méthodologie appropriée
- Propriétaires des processus clairement identifiés et responsabilisés

Alignement de la gouvernance



Les 3 lignes de défense

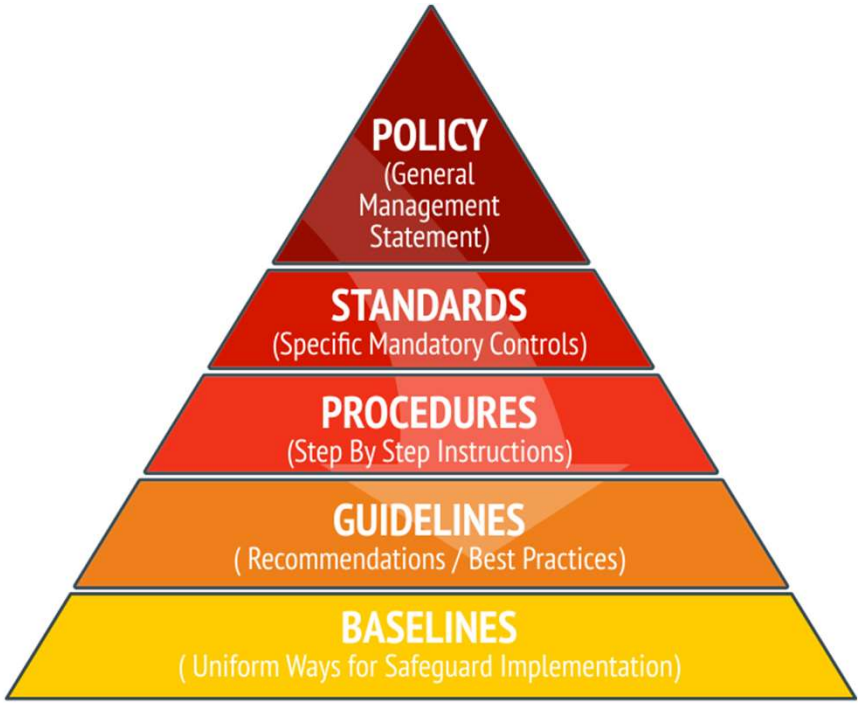
1ère ligne : les opérations / le SOC (Security Operations Center)

2ème ligne : la GRC

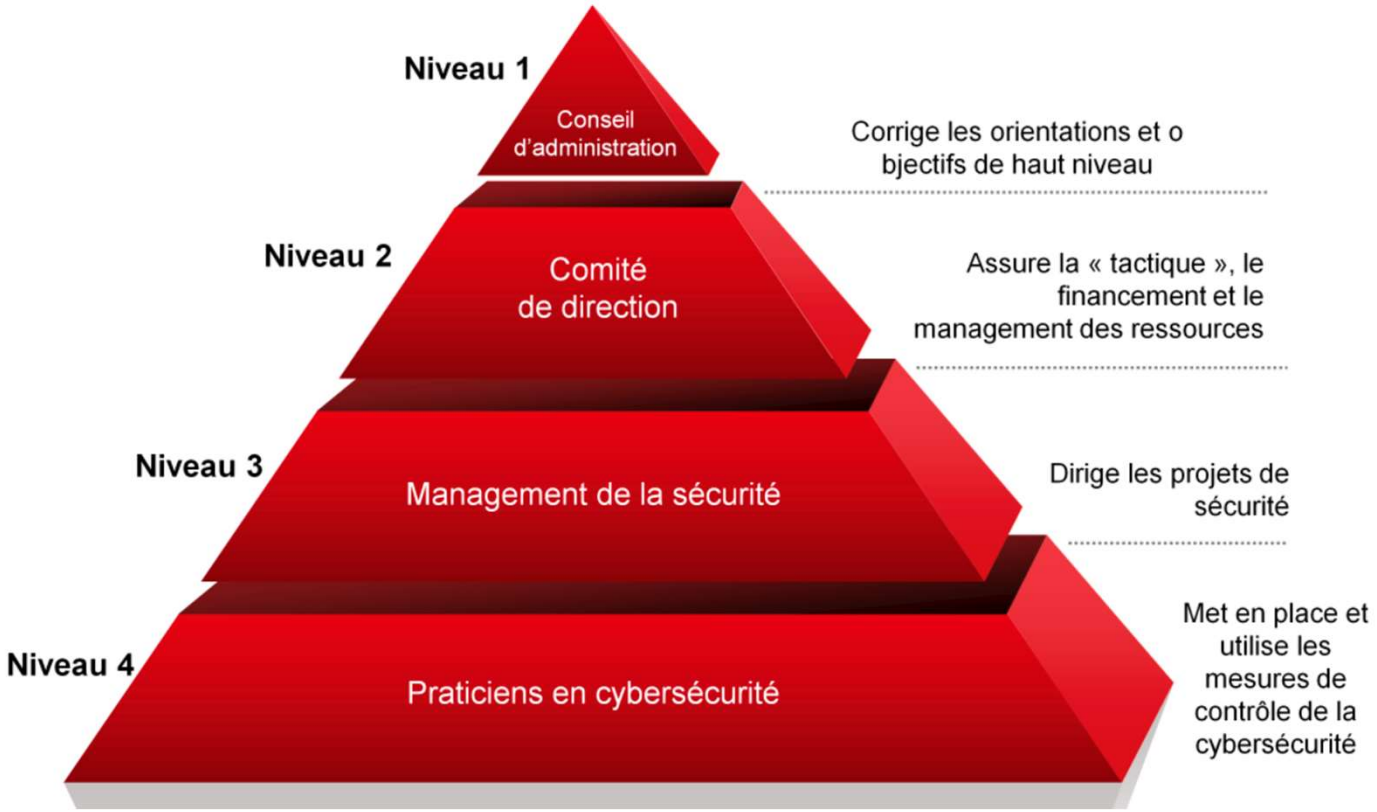
3ème ligne : l'audit interne

Définition d'un cadre

- Policy : Why
- Standard : What
- Procedure : How
- Guideline : Guidance
- Baseline : Uniformization



Rôles dans la gouvernance

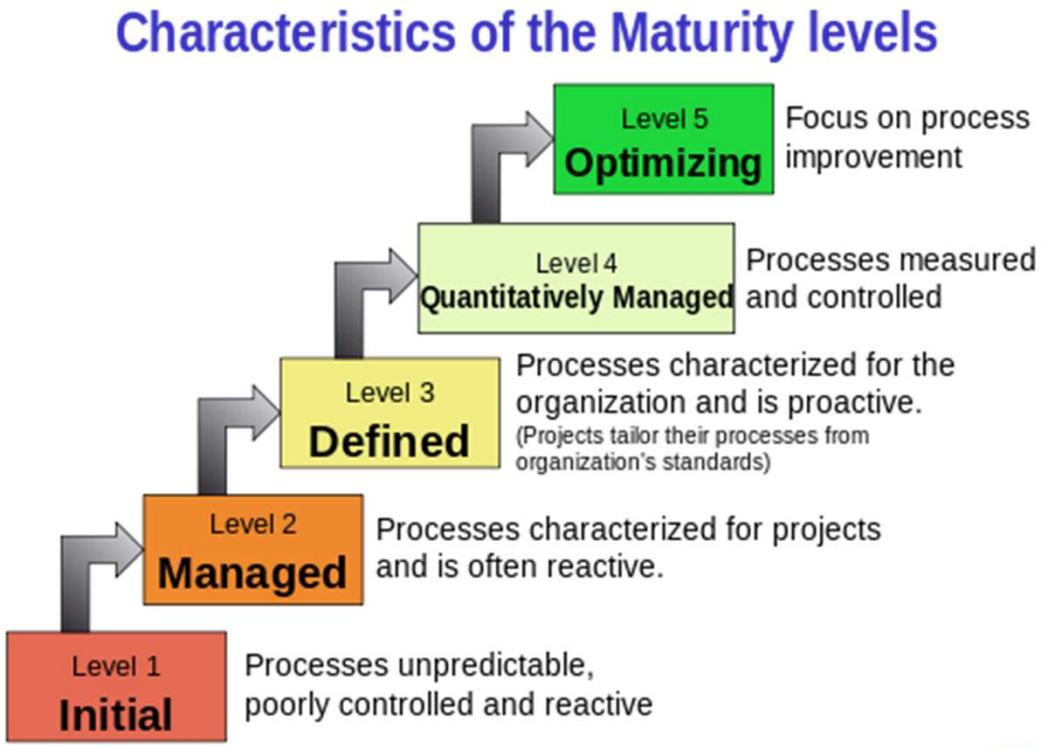


Source: PECB

Evaluation du niveau de maturité

5 niveaux

1. Initial
2. Géré
3. Défini
4. Qualité
5. Optimisation



Sans / Avec la GRC

Sans GRC	Avec GRC
Manque de surveillance efficace	Surveillance efficace dans tous les départements
Se concentrer uniquement sur l'obtention de résultats	Obtenir des résultats avec intégrité et éthique
Silos organisationnels et fonctionnels	Prise de décision intégrée
Manque de visibilité	Technologie, services et vocabulaire partagés
Stratégie décousue	Stratégie intégrée
Duplication des efforts	Créer une fois, utiliser plusieurs
Des coûts élevés	Coûts optimisés
Des efforts inefficaces	Des efforts efficaces
Manque d'intégrité	Culture d'intégrité
Informations gaspillées	Connaissances partagées et communes
Informations fragmentées et éparpillées	Flux d'informations continu et intégré

Gestion de la capacité et mesure de la performance

Objectif : Permettre de s'assurer que les investissements (temps/argent) produisent les effets escomptés.

⇒ Communiquer aux parties prenantes la performance du programme de sécurité.

Généralement, les indicateurs sont développés sous forme pyramidale.

- Dans la base, on va trouver des indicateurs opérationnels.
  - Exemple : Nombre de mises à jour des règles de pare-feu sur un mois, débit du trafic dans le pare-feu, nombre de jours depuis la dernière mise à jour des règles de défense, etc…
- Au niveau de gestion, on va retrouver moins d'indicateurs et ceux-ci vont totaliser les indicateurs opérationnels
  - Exemple : Etat opérationnel du pare-feu, Etat opérationnel de l'anti-virus, Etat opérationnel du DLP.
- Au stratégique, on va également regrouper les indicateurs de gestion
  - Exemple : Gestion de la sécurité : OK/Attention/Problème

Pilotage par les risques

Introduction à la gestion des risques

Il existe plusieurs initiatives de gestion des risques telles que :

- NIST Risk Management Framework
- ISO 27’005 (spécialisé TI) ou ISO 31’000 (général)
- ISACA RiskIT version 2
- OCTAVE, FAIR, etc..

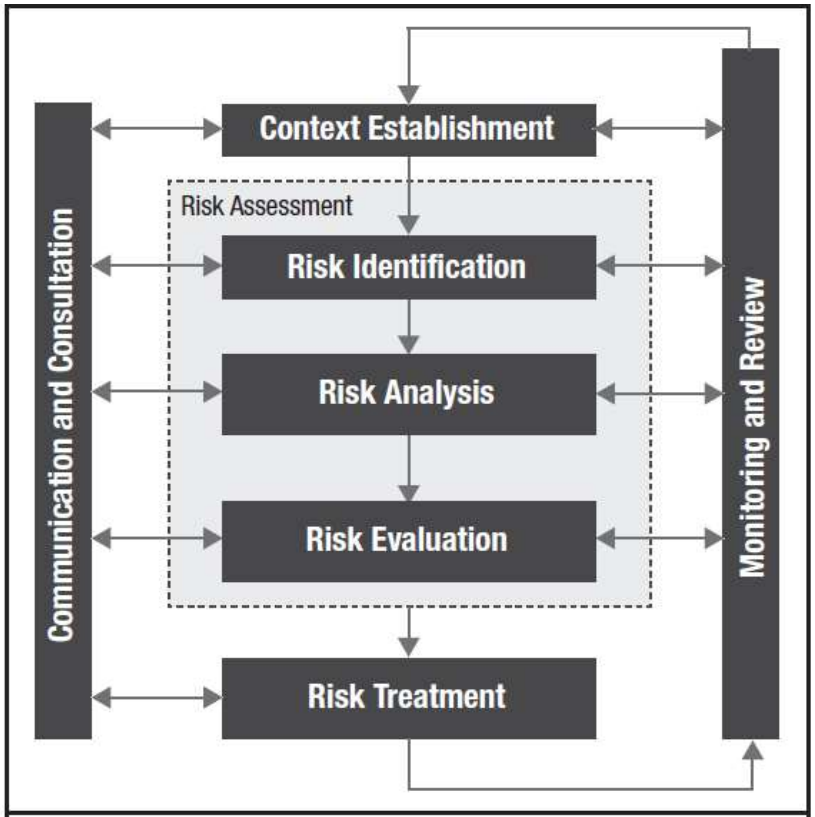
Introduction à la gestion des risques

- La gestion des risques permet de donner une assurance raisonnable. La gestion des risques est traitée par le département GRC: Gouvernance, Risques et Conformité.
- Etapes de l'ERM (Entreprise Risk Management) :
  1. Définition de l'appétit et tolérance au risque de l'organisation
  2. Inventorier tous les risques auxquels l'organisation est exposée
  3. Inventorier tous les actifs à protéger
  4. Evaluation des risques
  5. Sélection des risques pour traitement
  6. Traitement des risques à l'aide de contrôles
  7. Surveillance continuelle du niveau de risque et de l'efficacité des contrôles

Processus de l'ERM

Mise en place d'un programme de gestion des risques en entreprise (ERM) :

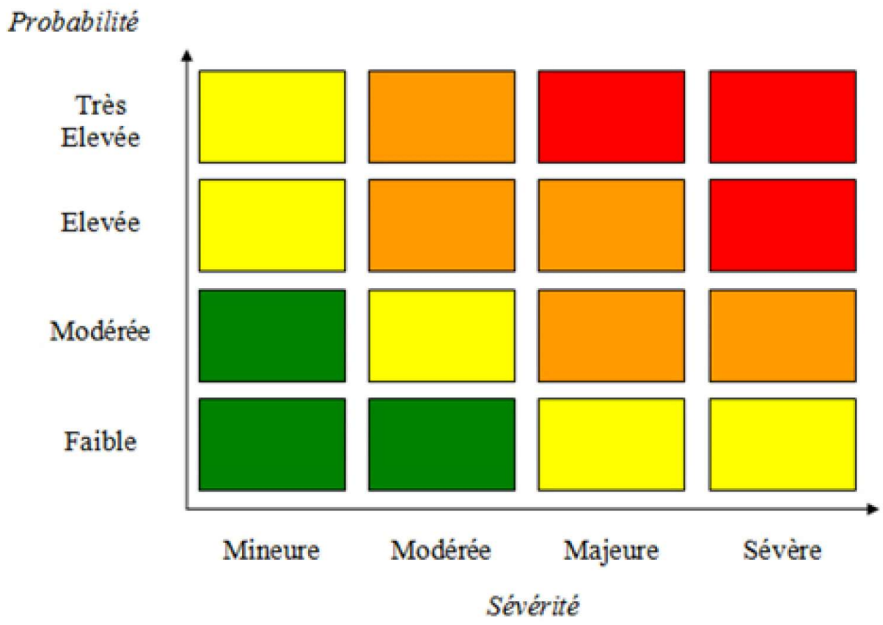
1. Définition de l'appétit et tolérance au risque de l'organisation
2. Inventorier tous les risques auxquels l'organisation est exposée
3. Inventorier tous les actifs à protéger
4. Evaluation des risques
5. Sélection des risques pour traitement
6. Traitement des risques à l'aide de contrôles
7. Surveillance continuelle du niveau de risque et de l'efficacité des contrôles



Source: ISACA, *COBIT 5 for Risk*, USA, 2013, figure 47

Qualification du risque

- *Impact x Menaces x Vulnérabilités = Niveau de risque*
- Calcul du coût du risque :
  - Coût initial (achat de l'actif) +
  - Coût de remplacement de l'actif +
  - Coût d'indisponibilité de l'actif (par ex. perte de productivité)
- .



Méthodes de traitement des risques

- Acceptation du risque
- Transfert du risque
- Réduction du risque
- Évitement du risque

Types de contrôles pour réduire le risque

- Directif (par ex. façons de faire)
- Dissuasif (dissuader un attaquant)
- Retardant (retarder l'effet d'une attaque)
- Préventif (préféré, baisse la probabilité du risque)
- Détectif (permet éventuellement de réduire l'impact)
- Correctif (traite le risque lorsqu'il apparaît)

Coût de gestion des risques

- Les coûts des contrôles des risques doivent toujours être plus petits que le coût de l'actif à protéger !

- Comment calculer le coût de l'actif ?
  - Coût initial (achat) +
  - Coût de remplacement +
  - Coût d'indisponibilité de l'actif (par ex. perte de productivité)

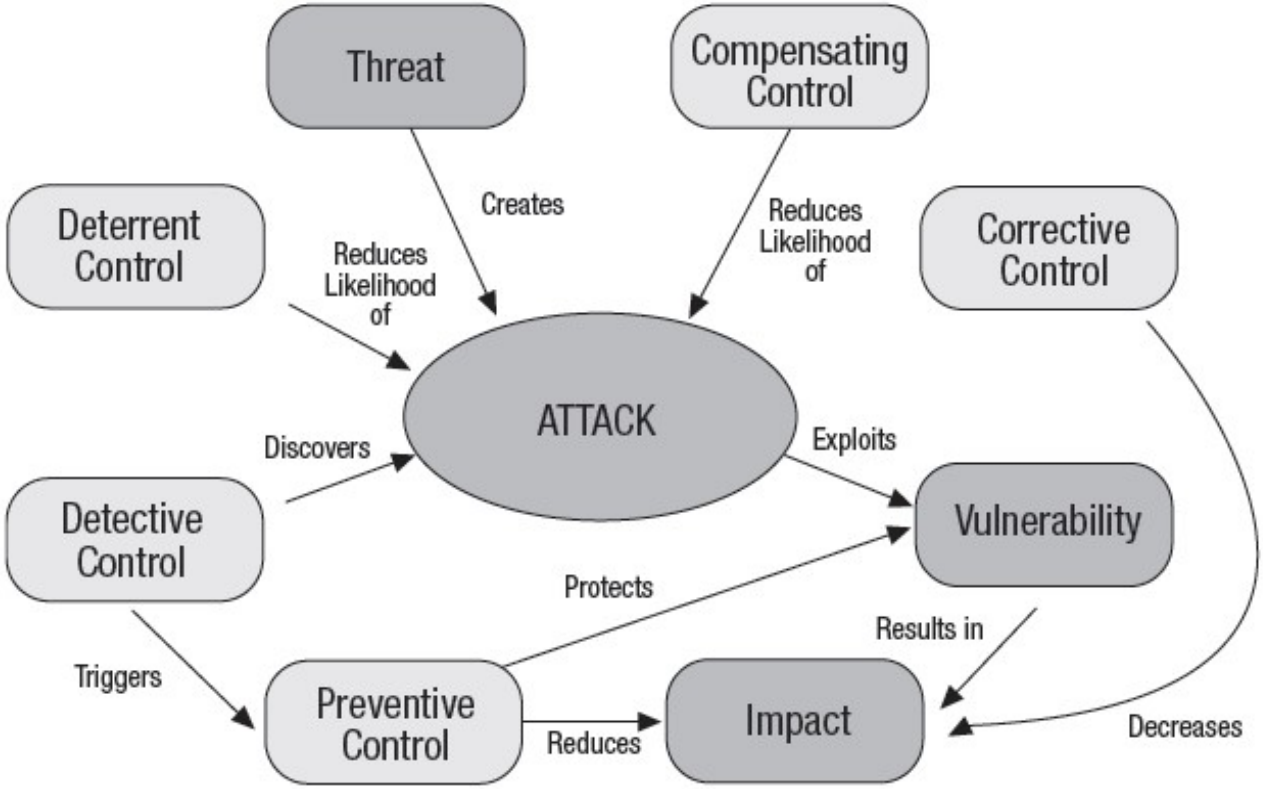
- Evaluation quantitative des risques : lorsque des figures monétaires sont disponibles (risque lié à la perte d'un centre de données par exemple)
- Evaluation qualitative des risques : lorsqu'il est difficile voire impossible d'établir une quantification financière (risque réputationnel par exemple)

Registre des risques

Part I—Summary Data				
Risk statement				
Risk owner				
Date of last risk assessment				
Due date for update of risk assessment				
Risk category	○ STRATEGIC (IT Benefit/Value Enablement)	○ PROJECT DELIVERY (IT Programme and Project Delivery)	○ OPERATIONAL (IT Operations and Service Delivery)	
Risk classification (copied from risk analysis results)	○ LOW	○ MEDIUM	○ HIGH	○ VERY HIGH
Risk response	○ ACCEPT	○ TRANSFER	○ MITIGATE	○ AVOID
Part II—Risk Description				
Title				
High-level scenario (from list of sample high-level scenarios)				
Part III—Risk Response				
Detailed scenario description—Scenario components	Actor			
	Threat Type			
	Event			
	Asset/Resource			
	Timing			
Other scenario information				

Source: COBIT 2019 - ISACA

En résumé



Source: COBIT 2019 - ISACA

Quelques notions de droit en conformité

RGPD

- RGPD – Règlement Général sur la Protection des Données personnelles

- Loi Européenne, applicable à tous les sujets européens
- Règle le transfert des données hors de l'UE
- Défini les manières de traiter les données personnelles
- Défini les rôles de DPO, contrôleur, sous-traitant, etc..

- En Suisse : LPD (Loi sur la Protection des Données personnelles)
- Au Canada: Loi 25
- En Californie : CCPA California Consumer Privacy Act (CCPA)

Le RGPD en 2 minutes

1. Concerne toute opération portant sur des données personnelles
   - Nom, prénom, âge
   - Adresse physique, numéro de téléphone, adresse IP, etc..
   - Données médicales, salaire, affiliations aux partis politiques, religieux, etc.
2. Obligation de tenir un registre des traitements
3. Informer les personnes concernées
4. Respecter le droit des personnes concernées
   - Obtenir le consentement pour le traitement des données
   - Respecter le droit à l'accès, la modification, la suppression et à la portabilité
   - Limitation du traitement aux éléments nécessaires et avec autorisation
5. Sécuriser les données
6. Désigner un délégué à la protection des données personnelles (DPO)
7. Limitation du transfert de données hors de l'UE (liste de pays autorisés, clauses contractuelles standard, …)
8. Sanctions : amende jusqu'à 4% du chiffre d'affaires mondial, sanctions pénales personnelles

Notions élémentaires sur la nLPD

- Mêmes principes que le RGPD.
- Ordonnance sur la protection des données personnelles règle la CIA des données !

- Possibilité de nommer un conseiller à la protection des données personnelles
- Certification possible des systèmes d'information (les systèmes de gestion, les produits, les services et les processus)
- 250 000 CHF d'amende maximum
- Droit à l'accès gratuit dans les 30 jours suivants la demande, sauf exceptions pour des demandes avec des *efforts disproportionnés*, jusqu'à 300 CHF (Art. 19 OPDo)
- Ne s'applique pas aux particuliers faisant un traitement personnel des données
- Utilisation des clauses contractuelles types de l'UE pour les contrats avec les fournisseurs
  - https://rm.coe.int/t-pd-2022-1rev10-en-final/1680abc6b4
- Voir la Loi fédérale sur la protection des données (LPD) et l'ordonnance sur la protection des données (OPDo)

nLPD - Changements

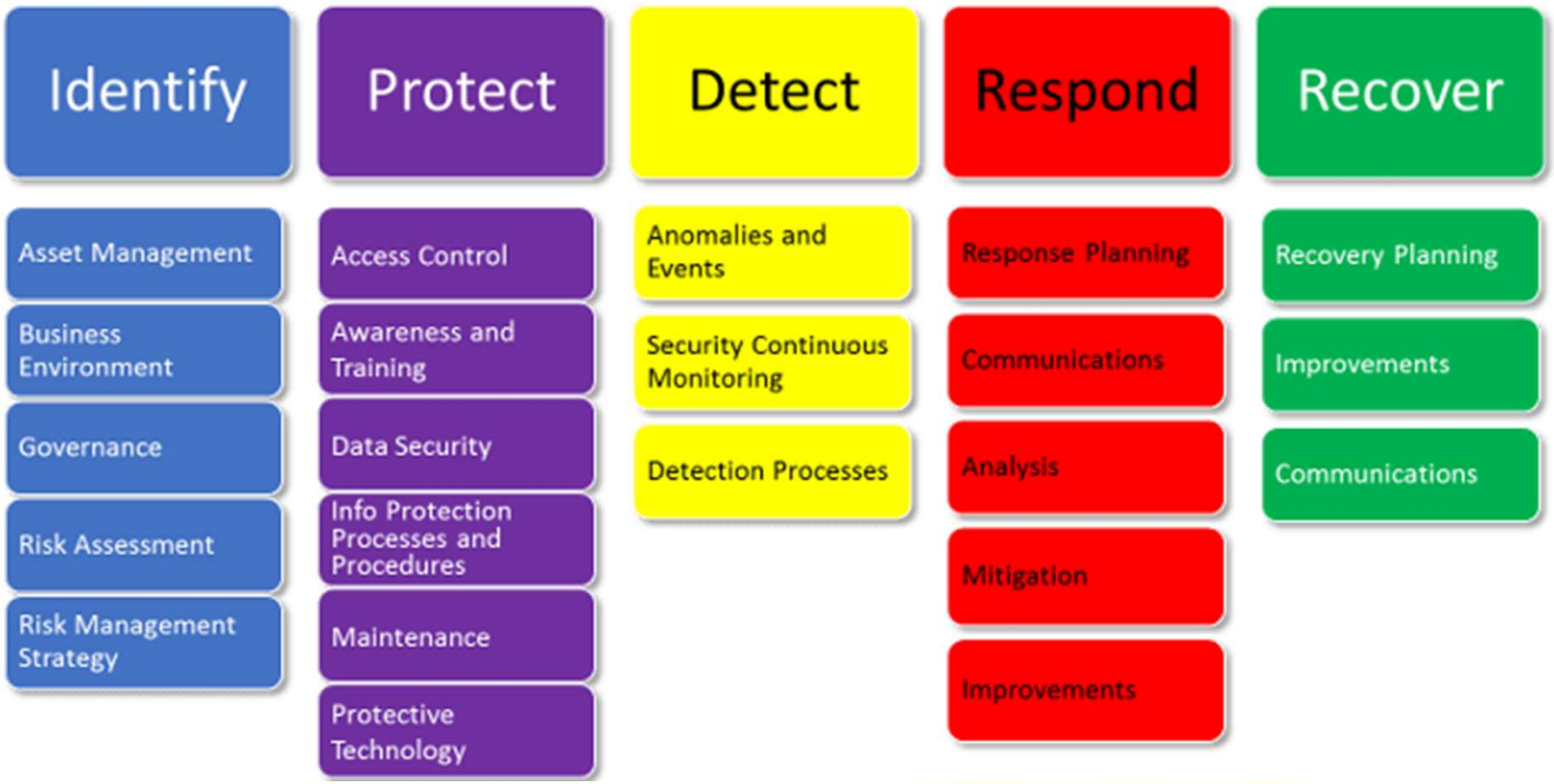
- Seules les données des personnes physiques sont dorénavant couvertes, et non plus celles des personnes morales.
- Les données génétiques et biométriques entrent dans la définition des données sensibles.
- Les principes de "**Privacy by Design**" et de "**Privacy by Default**" sont introduits. Comme son nom l'indique, le principe de "Privacy by Design" (protection des données dès la conception) implique, pour les développeurs, d'intégrer la protection et le respect de la vie privé des utilisateurs dans la structure même du produit ou du service amené à collecter des données personnelles. Le principe de "Privacy by Default" (protection des données par défaut) assure quant à lui le niveau de sécurité le plus élevé dès la mise en circulation du produit ou du service, en activant par défaut, c'est-à-dire sans aucune intervention des utilisateurs, toutes les mesures nécessaires à la protection des données et à la limitation de leur utilisation. Autrement dit, tous les logiciels, le matériel et les services doivent être configurés de manière à protéger les données et à respecter la vie privée des utilisateurs.
- Des analyses d'impacts doivent être menées, en cas de risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées.
- Le devoir d'informer est étendu: la collecte de toutes les données personnelles – et non plus uniquement de données dites sensibles –, doit donner lieu à une information préalable de la personne concernée.
- La tenue d'un **registre des activités de traitement** devient obligatoire. L'ordonnance d'application prévoit toutefois une exemption pour les PME dont le traitement des données présente un risque limité d'atteinte à la personnalité des personnes concernées (moins de 250 personnes)
- Une annonce rapide est requise en cas de violation de la sécurité des données, à adresser au Préposé fédéral à la protection des données et à la transparence (PFPDT).
- La notion de profilage (soit le traitement automatisé de données personnelles) fait son entrée dans la loi.

Loi sur la sécurité de l'information

- Règlemente la sécurité de l'information sur les entreprises de service critique (Art. 74b)
  - Attention à l'étendue qui est large !
- Obligation d'annoncer les incidents dans les 24 heures

Les cadres stratégiques pour l’entreprise

NIST Cyber Security Framework



Norme minimale pour les TIC

- Publié par la Confédération Suisse
- Version actuelle : 2022

- Toutes les industries sont concernées !
- Condensé de ISO 27001, NIST SP800-53, ISA 62443-3, COBIT.

«*La norme minimale est une recommandation, une ligne directrice qui a pour but d'améliorer la résilience informatique. Elle s'adresse en premier lieu aux exploitants d'infrastructures critiques mais elle peut aussi être appliquée par toutes les entreprises qui le souhaitent.*»

Retrouvez-la sur

https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard.html

ISO 27001:2022

- Mettre en place un ISMS (Information Security Management System)
- Permet de définir :
  - La gouvernance liée à la sécurité de l'information et la stratégie.
  - Les processus nécessaires à la maîtrise de la sécurité de l'information.
  - Différentes méthodes pour ainsi analyser les risques et en rendre compte.
  - Les processus de mesure, de suivi et d'amélioration de la sécurité.
  - Les responsabilités liées à la sécurité de l'information.

- Objectifs:
  - Assurer la disponibilité des informations et des services.
  - Sécuriser l'intégrité des données critiques.
  - Garantir la confidentialité des données sensibles ou des données clients.
  - Assurer la disponibilité et la conformité des preuves légales et autres.

ISO 27001:2022 - Annexe A

5. Politiques de sécurité de l'information
6. Organisation de la sécurité de l'information
7. Sécurité du personnel
8. Gestion des actifs
9. Contrôle d'accès
10. Cryptographie
11. Sécurité physique et environnementale
12. Sécurité opérationnelle
13. Sécurité des communications
14. Maîtrise des systèmes d'information
15. Relations avec les fournisseurs
16. Gestion des incidents liés à la sécurité de l'information
17. Gestion de la continuité de l'activité
18. Conformité

COBIT

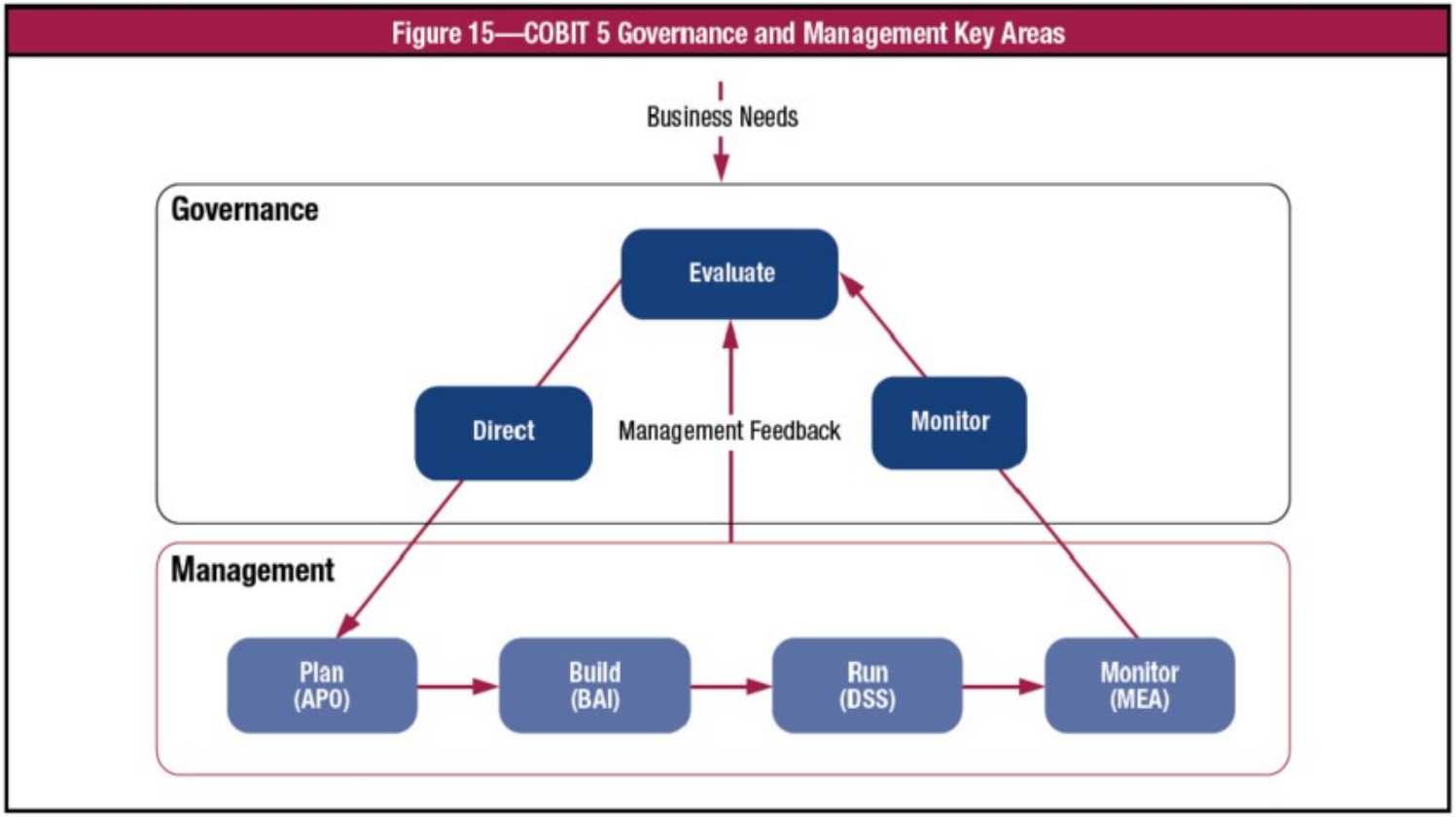
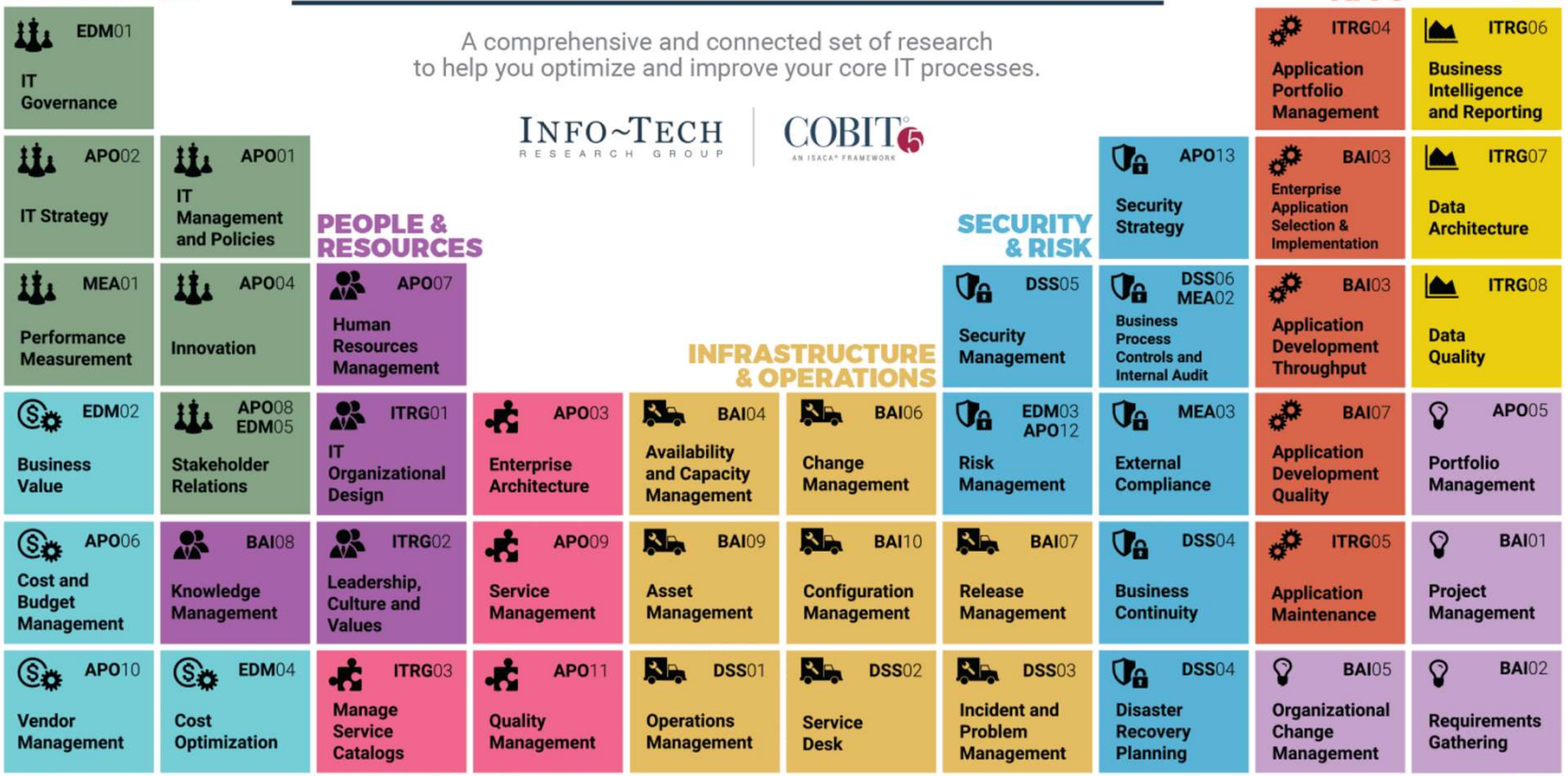


Figure 15—COBIT 5 Governance and Management Key Areas
Business Needs
Governance
Evaluate
Direct
Management Feedback
Monitor
Management
Plan (APO)
Build (BAI)
Run (DSS)
Monitor (MEA)

IT Management & Governance Framework

A comprehensive and connected set of research
to help you optimize and improve your core IT processes.

INFO-TECH RESEARCH GROUP | COBIT 5 AN ISACA® FRAMEWORK



CONGRÈS DU MANAGEMENT DE PROJET

Principes généraux de COBIT 2019

1. **Répondre aux besoins des parties prenantes : C**réer de la valeur en réalisant des avantages informatiques et en utilisant les ressources tout en atténuant les risques.
2. **Couvrir l'entreprise de bout en bout :** cela fait référence à la prise en compte de tous les processus et fonctions métiers liés aux technologies de l'information.
3. **Appliquer un cadre unique et intégré : A**ppliquer des normes unifiées dans toute l'entreprise.
4. **Permettre une approche holistique : P**rendre en compte les sept « facilitateurs » de COBIT, notamment « Personnes, aptitudes et compétences » et « Culture, éthique et comportement ».
5. **Séparer la gouvernance de la gestion : L**es étapes de planification, de construction, d'exécution et de suivi sont séparées des fonctions de gouvernance spécifiques telles que le suivi, l'évaluation et la prise de décision.

ITIL

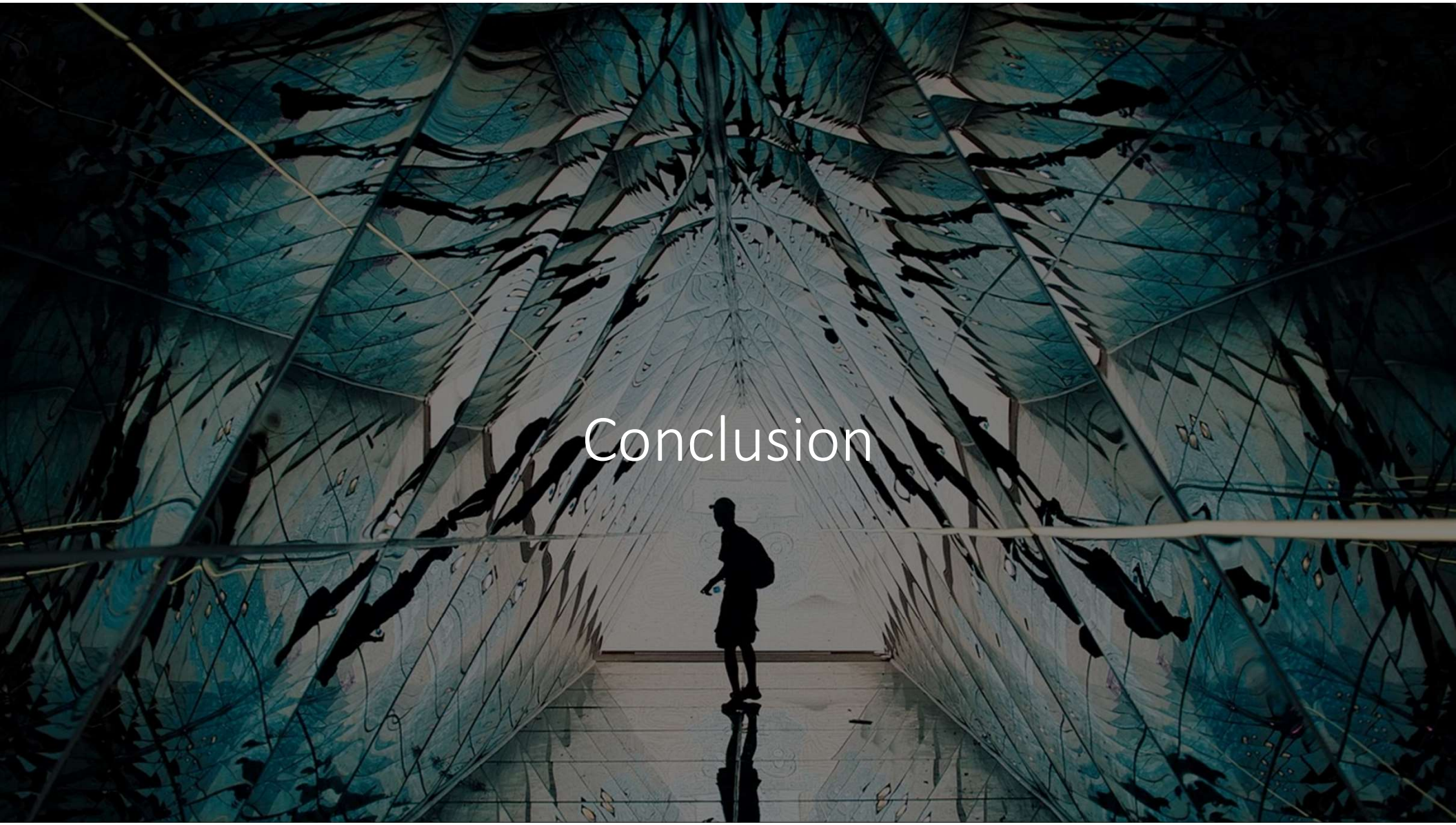
1. **Donner** une orientation client à l'informatique, être au service du business
2. **Améliorer** la qualité des services fournis par l'informatique
3. **Aider** à décrire les processus de la gestion de services informatiques
4. **Améliorer** la productivité et réduire les risques inhérents à l'utilisation de l'informatique
5. **Optimiser** la qualité de service et réduire les coûts à long terme
6. **Améliorer** la communication entre l'informatique et les métiers
7. **Apporter** un vocabulaire commun entre l'informatique et les métiers

Lifecycle Phase	ITIL Processes
Service Strategy	Strategy management for IT services
	Demand management
	Portfolio management
	Business relationship management
	Finance management for IT services
Service Design	Design coordination
	Service level management
	Service catalogue management
	Availability management
	Capacity management
	Information security management
	Supplier management
	IT service continuity management
Service Transition	Transition planning and support
	Change management
	Release and deployment management
	Service asset and configuration management
	Knowledge management
	Service validation and testing
	Change evaluation
Service Operation	Incident management
	Request fulfilment
	Problem management
	Access management
	Event management
Continual Service Improvement	Seven-step service improvement process

Quelques contrôles techniques

ISO 27002

- Dès la 2ème page


Conclusion

En résumé

- La gouvernance détermine la stratégie
- La gestion des risques met en lumière les options possibles
- La conformité assure le respect du cadre règlementaire

- Une approche holistique donne une assurance raisonnable que tous les processus métiers sont adéquatement suivis et documentés.

- Vous connaissez maintenant les principaux cadres en sécurité de l'information et les moyens de les appliquer.

Sources

- CIPM Certified Information Privacy Manager all-in-one exam guide, Gregory, Peter H
- ISACA Certified in Risk and Information Systems Control (CRISC) Exam Guide, Yadav, Vikas
- ITILv4 Reference Guide
- Governance of Enterprise IT based on COBIT 5 - A Management Guide, Geoff Harmer
- ISACA CISM - Certified Information Security Manager Study Guide
- ISACA CRISC - Certified in Risk and Information Systems Control Study Guide
- CISM Certified Information Security Manager All-in-One Exam Guide, by Peter H. Gregory
- CRISC Certified in Risk and Information Systems Control All-in-One Exam Guide, by Peter H. Gregory
- ISC2 Official ISC2 Certified in Cybersecurity (CC) eTextbook
- ISC2 CISSP - Certified Information Systems Security Professional Official Study Guide

Restons en contact !

Philippe Bonvin

Consultant en sécurité de l'information

CISO & Data Protection Officer-as-a-service

- Msc. Eng., Ing., MBA, LLM in Compliance
- CISSP, CCSP, CISM, CRISC, CISA, CIPP/E, CIPM, IPMA-D, CDPO
- Certified Cybersecurity Manager, ISO 27k1 & 22301 Lead Auditor, Certified ISO 27005 Lead Risk Manager, Lead Cloud Security Manager

www.philippe.bonvin.info

philippe@bonvin.info