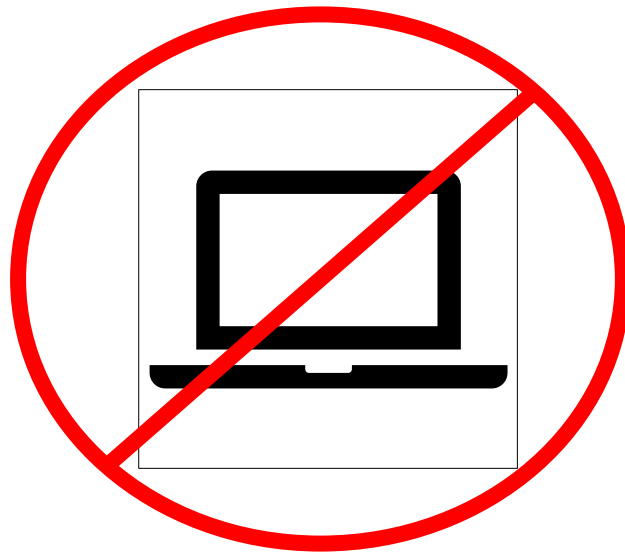




M2 Miage & ASR

Processus de la Sécurité des Systèmes d'information

Damien Ploix



Validation du cours

- Examen écrit : 50 % de la note
- Projet individuel (MIAGE Alternant) ou en groupe (n MIAGE I + m (A)SR) : 25 % de la note
 - Utilisation des IA Interdite
 - Étude d'une activité métier
 - Pour les alternants : leur mission en entreprise
 - Pour les Initiaux / (A)SR : un projet MIAGE en cours ou réalisé
 - Définition d'un périmètre technique
 - Outillage utilisé pour la réalisation de l'activité
 - Site web ou production du projet
 - Réalisation d'une analyse de conformité/préconisations 27002 et identification de risques résiduels et des remédiations
 - Envoi d'un mini mémoire
 - 5 à 10 pages maxi
- Participation aux réponses aux exercices : 25 % de la note

Plan

- Menace(s)
- Organisation de la Sécurité des SI

État de la menace

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2024>



<https://cyber.gouv.fr/le-panorama-de-la-cybermenace> :

Des attaquants qui s'améliorent et profitent des faiblesses techniques

Cas d'usage

La mairie de la ville de La Rochelle (75 000 habitants), met à disposition de ses administrés un portail Internet permettant d'accéder aux services municipaux en ligne (logements, crèches et écoles, stationnement et activités diverses). Le portail est développé, maintenu et administré par le service informatique de la ville.

En période pré-électorale, le système d'information de la ville a fait l'objet d'une double attaque combinée avec demande de rançon :

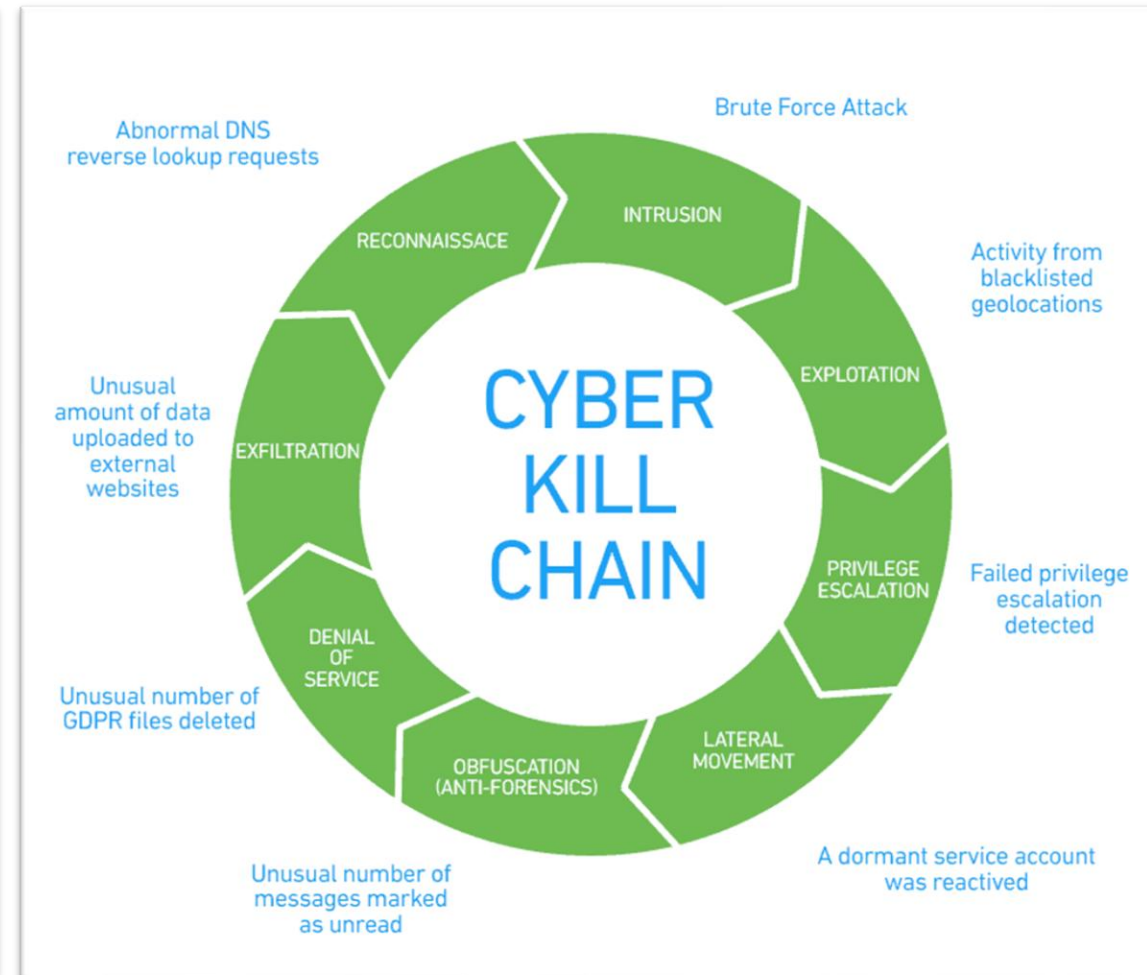
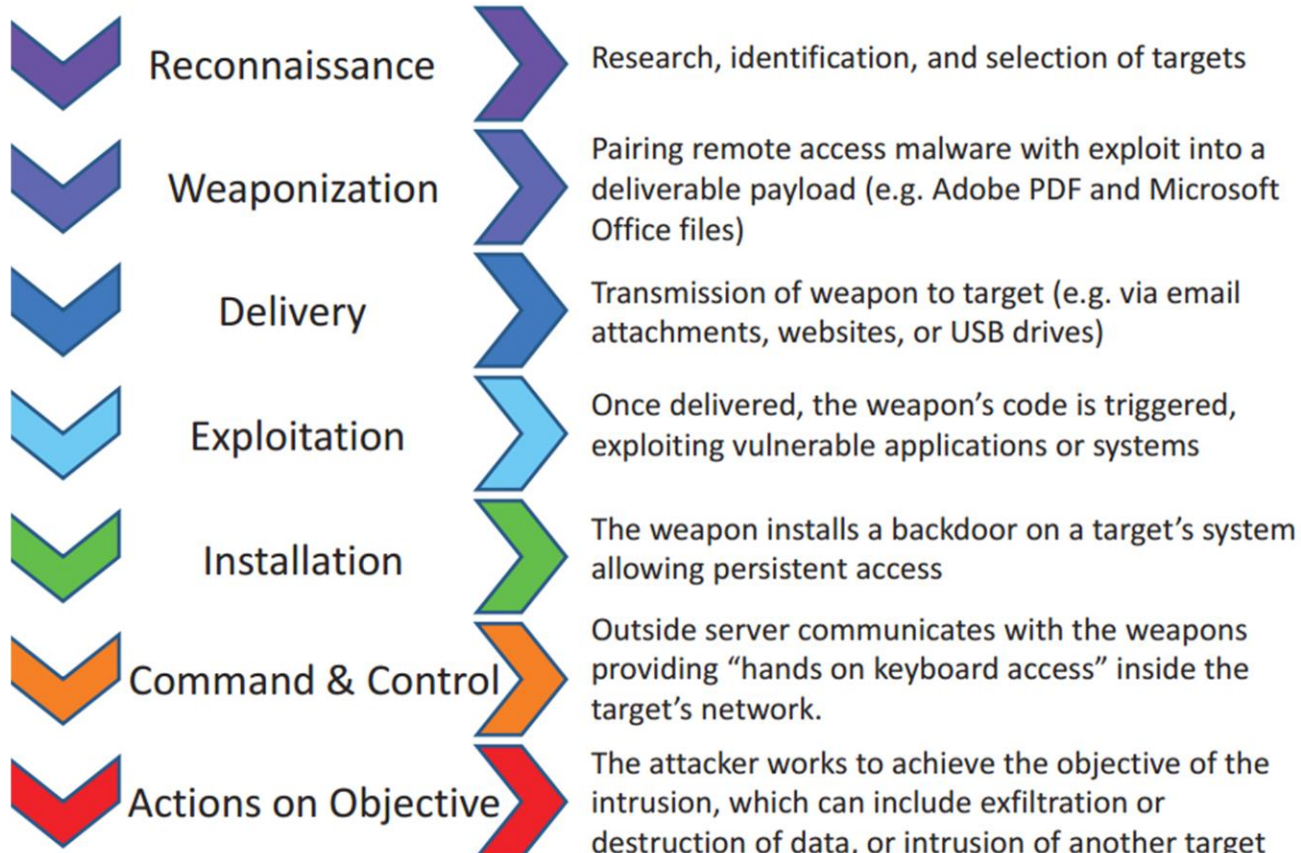
- Le service interne a été corrompu par une attaque de type encryptions des données (<https://attack.mitre.org/techniques/T1486/>),
- Le portail a été rendu hors service via une attaque de type DoS (<https://attack.mitre.org/techniques/T1498/>).

Nous allons identifier :

- Les schémas d'attaques ayant rendu ces attaques possibles,
- Les différentes mesures qui auraient permis de rendre impossible ces attaques, de la détecter ou d'en diminuer l'impact.

Cyber Kill Chain (Lockheed Martin)

Phases of the Intrusion Kill Chain



<https://www.exabeam.com/explainers/information-security/cyber-kill-chain-understanding-and-mitigating-advanced-threats/>

Références de référence

- Base de connaissance MITRE ATT@CK : <https://attack.mitre.org/>
 - <https://www.dragos.com/mitre-attack-for-ics/>
- Framework OSINT (Open Source Intelligence): <https://osintframework.com/>
- CERT (Computer Emergency Response Team) / CSIRT (Computer Security Incident Response Team)
 - ANSSI : www.cert.ssi.gouv.fr
 - EU : <https://cert.europa.eu>
- Publications de l'ANSSI : <https://cyber.gouv.fr/publications>

Plan

- Introduction
- Organisation de la Sécurité des SI

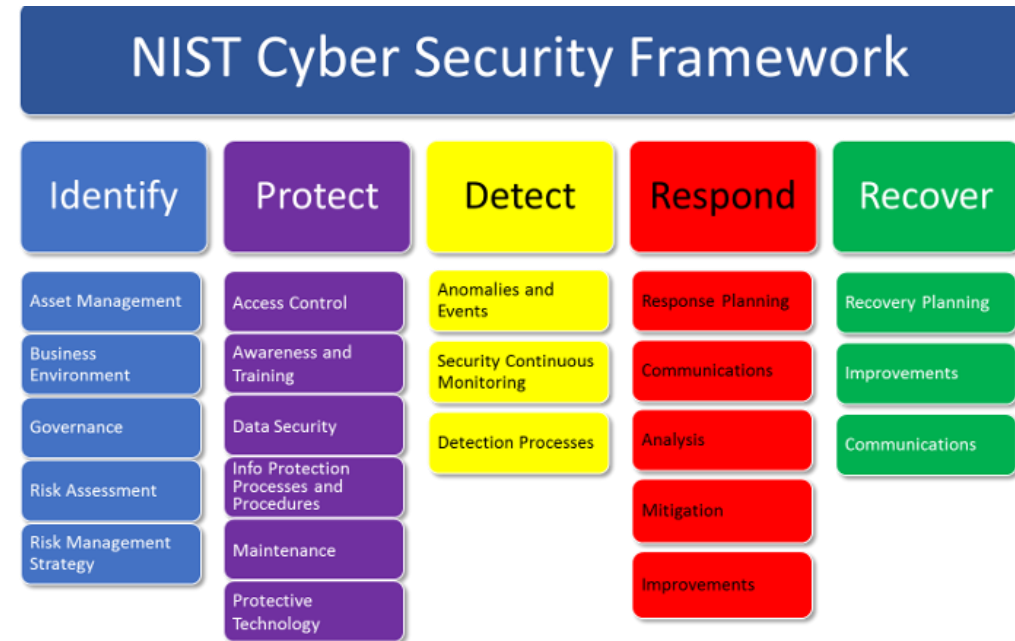
Métiers de la cybersécurité

« La sécurité est un processus, pas un produit » (OSSTMM3)

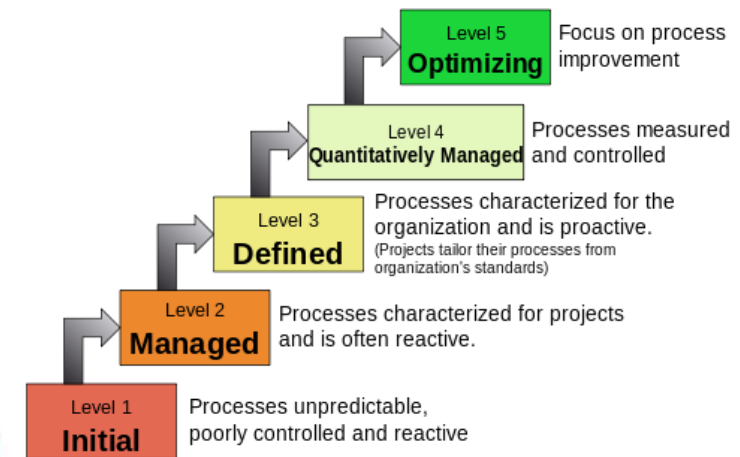
- Trois grandes familles de métiers cyber :
 - **RedTeam** : simuler les attaquants pour identifier les points de faiblesse du SI : 1%,
 - **BlueTeam** : surveiller le SI pour détecter les attaquants et répondre à leur attaque : 4%;
 - (dont **PurpleTeam** et **WhiteTeam**) : identifier les points de faiblesse de la vie du SI et le renforcer : 95% !
- (<https://www.ssi.gouv.fr/guide/panorama-des-metiers-de-la-cybersecurite/>)

Normes : une sémantique partagée

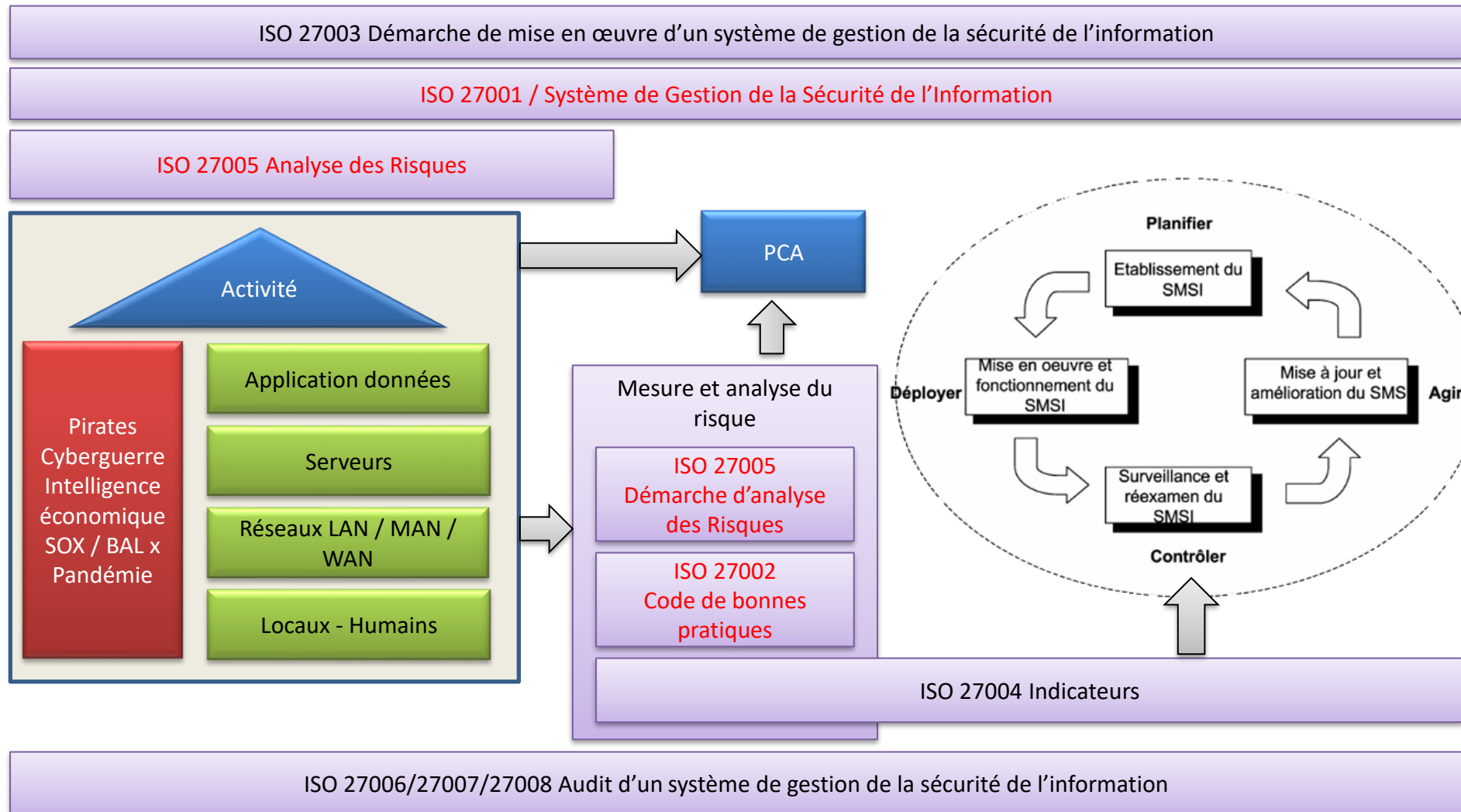
- L'Europe (et la France) :
 - Définition du quoi (ce qu'il faut faire) : ISO 270xx (IT) / IEC 62443 (OT)
 - Le comment est dépendant du contexte technique (guides ANSSI, IEC 62351, ...).
- US : Framework NIST :
<https://doi.org/10.6028/NIST.CSWP.04162018>
 - (correspondance entre les normes : <https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx>)
- Mais aussi :
 - CIS CSC (Center for Internet Security) : <https://www.cisecurity.org/>
 - COBIT 5,
 - ITIL,
 - CMMI,
 - ...



Characteristics of the Maturity levels



Structure globale des normes ISO 270xx



Le cours traitera des parties 27001, 27002 et 27005 de la norme.

Roue de Deming

- Objectif : **amélioration continue et construction des plans d'action**
- Plan : Préparation
 - Comprendre la racine du problème (root cause),
 - Identifier les métriques de mesure de la progression (KPI),
- Do :
 - réaliser, mettre en œuvre
- Check :
 - Mesurer les résultats des changements effectués via les métriques définies en préparation.
- Act (adjust) : agir, ajuster, réagir
 - Est-il possible d'aller plus loin tout en respectant l'ensemble des contraintes ?
 - Est-il temps de passer au pb suivant ?
- Répéter (cycle) :
 - L'amélioration continue nécessite une démarche **récurrente** et ne peut être **unitaire**.



ISO 27001 : SMSI

Système de gestion de la Sécurité SI

1. définir le domaine d'application et les limites du SMSI en termes de caractéristiques de l'activité, de l'organisme, de son emplacement, de ses actifs, de sa technologie, ainsi que des détails et de la justification de toutes exclusions du domaine d'application;
2. définir une politique pour le SMSI en termes de caractéristiques de l'activité, de l'organisme, de son emplacement, de ses actifs, et de sa technologie (27002) ;
3. définir l'approche d'appréciation du risque de l'organisme;
4. identifier les risques / analyser et évaluer les risques / identifier et évaluer les choix de traitement des risques (27005);
5. sélectionner les objectifs de sécurité et les mesures de sécurité (27002) proprement dites pour le traitement des risques;
6. obtenir l'approbation par la direction des risques résiduels présentés;
7. obtenir l'autorisation de la direction pour mettre en œuvre et exploiter le SMSI;
8. préparer une DdA (déclaration d'applicabilité);

ISO 27002/2022 : des mesures qui contribuent à ...

Quoi : Niveau de sécurité de l'information :

- Disponibilité / Intégrité / Confidentialité

Quoi / Objectif : Capacité opérationnelle :

- gouvernance, gestion des assets, application, IAM, réglementaire, ...

Objectif : Type de contrôle :

- Préventif / Détectif / Correctif

Objectif : Concept Cyber (NIST) :

- Identifier / Protéger / Détecter / Répondre / Réparer

Objectif : Domaine de la sécurité :

- Gouvernance / Protection / Défense / Résilience

*sécurisation métier
et technique*

*moyens et stratégie
cyber*

ISO 27002/2022 : des mesures qui contribuent à ...

Sécuriser ***les outils informatiques nécessaires à l'activité métier*** via

- Mesures organisationnelles :
 - Politique / Organisation / gestion RH
- Compréhension / maîtrise des actifs (assets) :
 - Actifs / contrôles d'accès
- Sécurité au quotidien :
 - Cryptographie / locaux / exploitation / communications / mobilité
- Relation externe sécurisées :
 - Acquisition / développement / maintenance / fournisseurs
- Gestion des incidents :
 - Incidents / information dans la continuité de l'activité / conformité

Activités/périmètre de la sécurité du SI

Organisation de la sécurité de l'information

Mesure ISO 27002	Control type	Information Security Properties	Cyber Concept	Operational Capabilities	Security Domains
Fonctions et responsabilités liées à la sécurité de l'information	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_ecosystem #Resilience
Responsabilité du management	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_ecosystem
Séparation des tâches	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Governance #Identity_and_access_management	#Governance_and_ecosystem
Relation avec les autorités	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Respond #Recover	#Gouvernance	#Defense #Resilience
Relation avec des groupes de travail spécialisés	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond #Recover	#Gouvernance	#Defense
Gestion des menaces (Threat Intelligence)	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Respond #Recover	#Threat_and_vulnerability_management	#Defense #Resilience
Rapport des évènements de sécurité	#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_event_management	#Defense

Déclinaison des mesures pour le cas d'usage

- Mesures préventives : ce qu'aurait dû avoir la Mairie de la Rochelle avant l'attaque
 - Fonctions et responsabilités liées à la sécurité de l'information
 - Responsabilité du management
 - Séparation des tâches
- Mesures préventives et correctives : ce qui aurait permis de repartir plus vite
 - Relation avec les autorités
 - Relation avec des groupes de travail spécialisés
- Mesures préventive / Détective et corrective : ce qui aurait prévenu l'attaque et permis une reprise plus rapide
 - Gestion des menaces (Threat Intelligence)
- Mesure détective : ce qui aurait permis de voir l'attaque venir
 - Rapport des événements de sécurité

Activités/périmètre de la sécurité du SI

Relations avec les fournisseurs

- Sécurité de l'information dans les relations avec les fournisseurs
 - Politique de sécurité de l'information dans les relations avec les fournisseurs
 - Sécurité dans les accords conclus avec les fournisseurs
 - Chaîne d'approvisionnement des technologies de l'information et des communications (ICT Supply Chain)
 - Sécurité de l'information dans l'utilisation de service Cloud

Control type	Information Security Properties	Cyber Concept	Operational Capabilities	Security Domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Gouvernance_and_ecosystem #Protection

- Gestion de la prestation de service
 - Surveillance et revue des services des fournisseurs
 - Gestion des changements apportés dans les services des fournisseurs

Control type	Information Security Properties	Cyber Concept	Operational Capabilities	Security Domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security #Information_security_assurance	#Gouvernance_and_ecosystem #Protection #Defense

Déclinaison pour le cas d'usage

- Demande une bonne connaissance de la supply chain (chaîne d'approvisionnement) tant sur les prestations humaines que pour les composants techniques !
- Échange sur le contexte : en quoi ces mesures sont toutes préventives ?
 - Politique de sécurité de l'information dans les relations avec les fournisseurs
 - Sécurité dans les accords conclus avec les fournisseurs
 - Chaîne d'approvisionnement des technologies de l'information et des communications (ICT Supply Chain)
 - Sécurité de l'information dans l'utilisation de service Cloud
 - Surveillance et revue des services des fournisseurs
 - Gestion des changements apportés dans les services des fournisseurs

Activités/périmètre de la sécurité du SI

Conformité

Service ISO 27002	Control type	Information Security Properties	Cyber Concept	Operational Capabilities	Security Domains
Identification de la législation et des exigences contractuelles applicables	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_compliance	#Governance_and_Ecosystem #Protection
Droits de propriété intellectuelle	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_compliance	#Governance_and_Ecosystem
Protection des enregistrements	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_compliance #Asset_management #Information_protection	#Governance_and_Ecosystem
Protection des DCP	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_compliance #Information_protection	#Protection
Revue indépendante de la sécurité de l'information	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_security_assurance	#Governance_and_Ecosystem
Conformité avec les politiques et les normes de sécurité	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_compliance #Asset_management #Information_protection	#Governance_and_Ecosystem

Déclinaison pour le cas d'usage

- Mesures préventives :
 - Identification de la législation et des exigences contractuelles applicables
 - Droits de propriété intellectuelle
 - Protection des enregistrements
 - Protection des DCP
 - Conformité avec les politiques et les normes de sécurité
- Mesure préventive et corrective :
 - Revue indépendante de la sécurité de l'information

Activités/périmètre de la sécurité du SI

Sécurité liée aux ressources humaines

Mesure ISO 27002	Control type	Information Security Properties	Cyber Concept	Operational Capabilities	Security Domains
Vérifications des candidats	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	#Governance_and_ecosystem
Termes et conditions d'embauche	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	
Sensibilisation, apprentissage et formations à la sécurité de l'information	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	
Achèvement ou modification des responsabilités associés au contrat de travail	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security #Asset_management	
Processus disciplinaire	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Human_resource_security	
Accords de confidentialité et de non divulgation (NDA)	#Preventive	#Confidentiality	#Protect	#Human_resource_security #Information_protection #Supplier_relationship	
Télétravail	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection #Physical_security #System_and_network_security	#Protection

Déclinaison pour le cas d'usage

- Mesures préventives :
 - Vérifications des candidats
 - Termes et conditions d'embauche
 - Sensibilisation, apprentissage et formations à la sécurité de l'information
 - Achèvement ou modification des responsabilités associés au contrat de travail
 - Accords de confidentialité et de non divulgation (NDA)
 - Télétravail
- Mesure préventive et corrective :
 - Processus disciplinaire

Activités/périmètre de la sécurité du SI

Gestion des informations et des actifs

- Inventaire et propriété des informations et des actifs
- Classification des informations
- Sécurité de l'Information dans les projets

Control type	Information Security Properties	Cyber Concept	Operational Capabilities	Security Domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Asset_Managment #Information_protection	#Governance_and_ecosystem #Protection

- Marquage et manipulation de l'information
- Utilisation correcte des actifs
- Transfert de l'information
- Restitution des actifs

Control type	Information Security Properties	Cyber Concept	Operational Capabilities	Security Domains
#Preventive	#Confidentiality #Integreity #Availability	#Protect	#Asset_Managment #Information_protection	#Protection #Defense

Déclinaison pour le cas d'usage

- Mesures préventives :
 - Inventaire et propriété des informations et des actifs
 - Classification des informations
 - Sécurité de l'Information dans les projets
 - Marquage et manipulation de l'information
 - Utilisation correcte des actifs
 - Transfert de l'information
 - Restitution des actifs

Activités/périmètre de la sécurité du SI

Mesures techniques : contrôle d'accès

- Expression de besoin du control d'accès
- Authentification sécurisée
- Droits d'accès privilégiés : « moindre privilège »
- Restriction d'accès à l'information : « besoin d'en connaître »

Control type	Information Security Properties	Cyber Concept	Operational Capabilities	Security Domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Déclinaison pour le cas d'usage

- Mesures préventives :
 - Expression de besoin du control d'accès
 - Authentification sécurisée
 - Droits d'accès privilégiés : « moindre privilège »
 - Restriction d'accès à l'information : « besoin d'en connaître »
- Traité plus en détail dans le cadre du cours IAM.

Activités/périmètre de la sécurité du SI

Mesures techniques : Ops

Service ISO 27002	Control type	Information Security Properties	Cyber Concept	Operational Capabilities	Security Domains
Gestion de la capacité	#Preventive #Detective	#Integrity #Availability	#Protect #Identify #Detect	#Continuity	#Governance_and_Ecosystem #Protection
Gestion de la configuration	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration	#Protection
Gestion des changements	#Preventive	#Confidentiality #Integrity	#Protect	#Application_security #System_and_network_security	#Protection
Sauvegarde des informations	#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection
Installation de logiciels sur les systèmes opérationnels	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration #Application_security	#Protection
Procédures d'exploitation documentées	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Recover	#Asset_management #Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability_management #Continuity #Information_security_event_management	#Governance_and_Ecosystem #Protection #Defence

Déclinaison pour le cas d'usage

- Préventives :
 - Gestion de la configuration
 - Gestion des changements
 - Installation de logiciels sur les systèmes opérationnels
- Préventive et détective :
 - Gestion de la capacité
- Préventive et corrective :
 - Procédures d'exploitation documentées
- Corrective :
 - Sauvegarde des informations

Activités/périmètre de la sécurité du SI

Sécurité physique et environnementale

Mesure ISO 27002	Control type	Information Security Properties	Cyber Concept	Operational Capabilities	Security Domains
Périmètre de sécurité physique	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection
Protection des accès	#Preventive		#Protect	#Physical_security #Identity_and_Access_Management	#Protection
Sécurisation des bureaux, salles et locaux techniques	#Preventive		#Protect	#Physical_security #Asset_management	#Protection
Surveillance de la sécurité physique	#Preventive #Detective		#Protect #Detect	#Physical_security	#Protection #Defence
Protection contre les menaces extérieures et environnementales	#Preventive		#Protect	#Physical_security	#Protection
Travail en environnement sécurisé	#Preventive		#Protect	#Physical_security	#Protection
Positionnement et protection des équipements	#Preventive		#Protect	#Physical_security #Asset_management	#Protection
Sécurité des équipements hors site					
Média de stockage					
Maintenance des équipements	#Preventive		#Protect	#Physical_security #Asset_management	#Protection #Resilience
GTB (Gestion technique des bâtiments)	#Detective #Preventive	#Integrity #Availability	#Protect #Detect	#Physical_security	#Protection
Sécurité du câblage	#Preventive	#Confidentiality #Availability	#Protect	#Physical_security	#Protection
Sécurité de la mise au rebut ou de la réutilisation	#Preventive	#Confidentiality	#Protect	#Physical_security #Asset_management	#Protection
Écran et bureau propre	#Preventive	#Confidentiality	#Protect	#Physical_security	#Protection

Déclinaison pour le cas d'usage

- Préventives :
 - Protection des accès
 - Sécurisation des bureaux, salles et locaux techniques
 - Protection contre les menaces extérieures et environnementales
 - Travail en environnement sécurisé
 - Positionnement et protection des équipements
 - Sécurité des équipements hors site
 - Média de stockage
 - Maintenance des équipements
 - Sécurité du câblage
 - Sécurité de la mise au rebus ou de la réutilisation
 - Écran et bureau propre
- Préventives et détectives :
 - Surveillance de la sécurité physique
 - GTB (Gestion technique des bâtiments)

Activités/périmètre de la sécurité du SI

Gestion des incidents liés à la sécurité de l'information

Service ISO 27002	Control type	Information Security Properties	Cyber Concept	Operational Capabilities	Security Domains
Préparation à la gestion d'incident liés à la sécurité de l'information	#Corrective	#Respond #Recover	#Confidentiality #Integrity #Availability	#Governance #Information_security_event_management	#Defense
Appréciation des événements liés à la sécurité de l'information et prise de décision	#Detective	#Detect #Respond	#Confidentiality #Integrity #Availability	#Governance #Information_security_event_management	#Defense
Réponse aux incidents liés à la sécurité de l'information	#Corrective	#Respond #Recover	#Confidentiality #Integrity #Availability	#Governance #Information_security_event_management	#Defense
Tirer des enseignements des incidents liés à la sécurité de l'information	#Preventive	#Identify #Protect	#Confidentiality #Integrity #Availability	#Governance #Information_security_event_management	#Defense
Recueil de preuves	#Corrective	#Detect #Respond	#Confidentiality #Integrity #Availability	#Governance #Information_security_event_management	#Defense
Gestion de la sécurité de l'information en situation d'incident	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Continuity	#Protection #Resilience
Capacité des ICT à assurer la continuité de l'activité métier en situation d'incident	#Corrective	#Availability	#Respond	#Continuity	#Resilience

Déclinaison pour le cas d'usage

- Correctives :
 - Préparation à la gestion d'incident liés à la sécurité de l'information
 - Réponse aux incidents liés à la sécurité de l'information
 - Recueil de preuves
 - Capacité des ICT à assurer la continuité de l'activité métier en situation d'incident
- Détectives :
 - Appréciation des événements liés à la sécurité de l'information et prise de décision
- Préventives :
 - Tirer des enseignements des incidents liés à la sécurité de l'information
- Préventives et correctives :
 - Gestion de la sécurité de l'information en situation d'incident

Activités/périmètre de la sécurité du SI

Mesures techniques : surveillance du SI

Service ISO 27002	Control type	Information Security Properties	Cyber Concept	Operational Capabilities	Security Domains
Logging	#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_event_management	#Protection #Defense
Surveillance des activités	#Detective #Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Asset_management #Information_protection	#Defense

Déclinaison pour le cas d'usage

- Détective :
 - Logging
- Détective et corrective :
 - Surveillance des activités

Activités/périmètre de la sécurité du SI

Mesures techniques : architecture des systèmes (1/2)

Service ISO 27002	Control type	Information Security Properties	Cyber Concept	Operational Capabilities	Security Domains
Utilisation de la cryptographie	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_Configuration	#Protection
Terminaux utilisateurs	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Protection
Protection contre les malwares	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_Network_security #Information_protection	#Protection #Defense
Utilisation de programme privilégiés	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security #Secure_configuration #Application_security	#Protection

Déclinaison pour le cas d'usage

- Préventives :
 - Utilisation de la cryptographie
 - Terminaux utilisateurs
 - Utilisation de programme privilégiés
- Préventive, détective et corrective :
 - Protection contre les malwares

Activités/périmètre de la sécurité du SI

Mesures techniques : architecture des systèmes (2/2)

Service ISO 27002	Control type	Information Security Properties	Cyber Concept	Operational Capabilities	Security Domains
Synchronisation des horloges	#Detective	#Integrity	#Protect #Detect	#Information_security_event_management	#Protection #Defense
Redondance des moyens de traitements	#Preventive	#Availability	#Protect	#Continuity #Asset_management	#Protection #Resilience
Masquage des données	#Preventive	#Confidentiality	#Protect	#Information_protection	#Protection
Protection contre la fuite des données	#Preventive #Detective	#Confidentiality	#Protect #Detect	#Information_protection	#Protection #Defense
Effacement des informations	#Preventive	#Confidentiality	#Protect	#Information_protection #Legal_and_compliance	#Protection

Déclinaison pour le cas d'usage

- Détective :
 - Synchronisation des horloges
- Préventives :
 - Redondance des moyens de traitements
 - Masquage des données
 - Effacement des informations
- Préventive et détective :
 - Protection contre la fuite des données

Activités/périmètre de la sécurité du SI

Mesures techniques : architecture réseau

Service ISO 27002	Control type	Information Security Properties	Cyber Concept	Operational Capabilities	Security Domains
Sécurité du réseau (composants, flux, ...)	#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_Network_security	#Protection
Sécurité des services réseau (SLA, SLO, ...)	#Preventive		#Protect		
Ségrégation des réseaux					
Filtrage des accès aux sites externes (web)					

Déclinaison pour le cas d'usage

- Préventive et détective :
 - Sécurité du réseau (composants, flux, ...)
- Préventives :
 - Sécurité des services réseau (SLA, SLO, ...)
 - Ségrégation des réseaux
 - Filtrage des accès aux sites externes (web)

Activités/périmètre de la sécurité du SI

Mesures techniques : Dev(Sec) (1/2)

Service ISO 27002	Control type	Information Security Properties	Cyber Concept	Operational Capabilities	Security Domains
Codage sécurisé	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
Test de sécurité pendant le développement et la qualification	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Application_security #Information_security_assurance #System_and_network_security	#Protection
Séparation des environnements de développement, du test et de la production	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
Sécurité dans les principes d'architecture et d'ingénierie	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
Exigences de sécurité pour les applications	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection #Defense

Déclinaison pour le cas d'usage

- Préventives :
 - Codage sécurisé
 - Test de sécurité pendant le développement et la qualification
 - Séparation des environnements de développement, du test et de la production
 - Sécurité dans les principes d'architecture et d'ingénierie
 - Exigences de sécurité pour les applications

Activités/périmètre de la sécurité du SI

Mesures techniques : Dev(Sec) (2/2)

Service ISO 27002	Control type	Information Security Properties	Cyber Concept	Operational Capabilities	Security Domains
Accès au code source	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management #Application_security #Secure_configuration	#Protection
Information pour le test	#Preventive	#Confidentiality #Integrity	#Protect	#Information_protection	#Protection
Protection des systèmes d'information pendant les tests d'audits	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security #Information_protection	#Governance_and_Ecosystem #Protection
Gestion des vulnérabilités	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Threat_and_vulnerability_management	#Governance_and_Ecosystem #Protection #Defense
Développement externalisé	#Preventive #Detective	#Confidentiality #Integrity #Availability	#Identify #Protect #Detect	#Application_security #System_and_network_security #Supplier_relationship_security	#Governance_and_Ecosystem #Protection
Cycle de développement intégrant la sécurité (DevSec)	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Application_security #System_and_network_security	#Protection

Déclinaison pour le cas d'usage

- Préventives :
 - Accès au code source
 - Information pour le test
 - Protection des systèmes d'information pendant les tests d'audits
 - Gestion des vulnérabilités
 - Cycle de développement intégrant la sécurité (DevSec)
- Préventive et détective :
 - Développement externalisé

Activités/périmètre de la sécurité du SI

Politique de sécurité de l'information

- « Il convient que le document de politique de sécurité de l'information démontre l'engagement de la direction et définisse l'approche de l'organisme pour gérer la sécurité de l'information. » (ISO 27002)
- Le corpus des politiques de sécurité du SI doit couvrir l'ensemble des thématiques « opérationnelles » et définissant/contextualisant les règles de leur « l'instanciation ».
- Les politiques de sécurité du SI doivent faire l'objet de réexamen à intervalles fixés préalablement ou en cas d'incident majeur.
- Politiques thématiques :
 - Menaces liées à l'utilisateur :
 - Control d'accès, utilisation des actifs, bureau propre et écran vide, appareils mobiles / télétravail, installation de logiciels, classification (et traitement) de l'information
 - Menaces liées à l'outillage du métier SI
 - Sécurité physique et environnementale, sauvegarde, transfert de l'information, communications, ...
 - Menaces liées aux relations avec des tiers
 - Relations avec les fournisseurs, ...

Exemple : organisation des responsabilités autour de la cyber, règles pour l'authentification, la gestion des PC et SmartPhones entreprise, du BYOD, du TAD, de l'hébergement des données ICS et DCP, ...

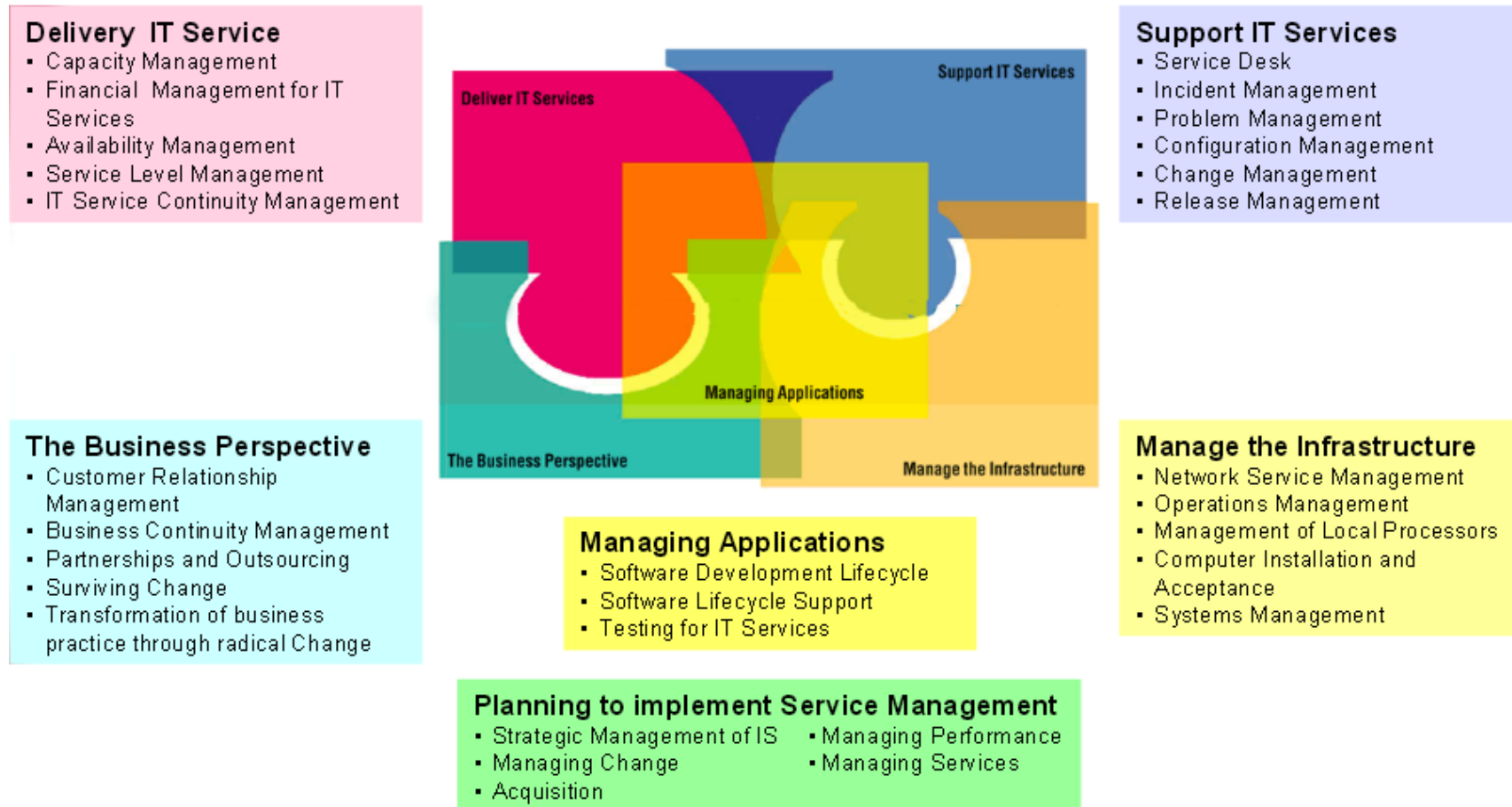
Pros : les règles sont établies

Cons : sans contrôle d'application, les politiques ne servent à rien.

Control type	Information Security Properties	Cyber Concept	Operational Capabilities	Security Domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_ecosystem #Resilience

Sécurité dans ITIL ?

Selon la mise en œuvre, couvre tout ou partie d'ISO 27002



Sécurité dans ITIL ?

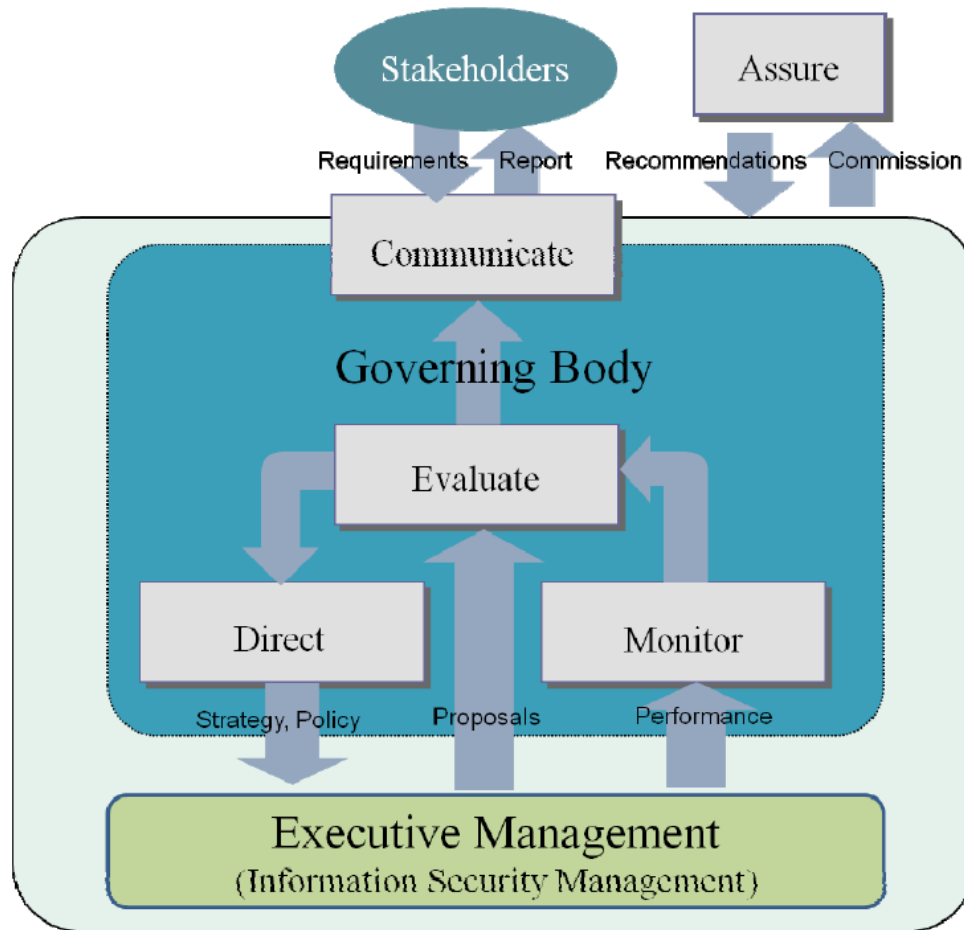
Selon la mise en œuvre, couvre tout ou partie d'ISO 27002

(base Wikipedia)

- **Classification de la sécurité**
 - Disponibilité : l'information doit être disponible et utilisable lorsque nécessaire,
 - Confidentialité : l'information doit être divulguée ou vue uniquement par les utilisateurs qui en ont le droit,
 - Intégrité : l'information doit être complète, précise et on la protège de modifications non autorisées,
 - Authenticité, non répudiation : l'information doit être réputée "de confiance" lorsque des transactions d'affaire ont lieu (et réalisées électroniquement) et lors des échanges entre les organisations ou avec des partenaires de l'organisation.
- **Gestion de la sécurité (Security management) et référentiel de sécurité**
 - la stratégie de sécurité globale (liée aux stratégies d'affaires de l'organisation),
 - la politique de sécurité de l'information (aspects de la stratégie, des contrôles et de la réglementation),
 - le système de gestion de la sécurité de l'information (ou Information Security Management System - ISMS)
 - l'ensemble des contrôles de sécurité pour soutenir la politique
 - la structure organisationnelle de sécurité efficace
 - le processus de surveillance (conformité et remontée de l'information)
 - la stratégie et le plan de communication pour la sécurité
 - la gestion des risques sur la sécurité
 - la stratégie ainsi que le plan de formation et de sensibilisation des utilisateurs

Organisation de la sécurité SI

Gouvernance (recommandation ISO 27014)



Le processus en jeu dans la **gouvernance** de la sécurité du SI identifie les activités :

- Évaluation (Evaluate),
- Pilotage (Direct)
- Mesure (monitor)
- Communication (communicate)

Il est généralement porté par l'organisation de sécurité SI et fait partie des missions du D/RSSI.

En complément, le processus de certification (assure) donne un point de vue indépendant et objectif sur la gouvernance de la sécurité et ses objectifs.

Organisation de la SSI

(Recommandation ISO 27002)

- Définition de l'organisation de la sécurité explicitant :
 - Engagement de la direction vis-à-vis de la sécurité de l'information
 - Coordination de la sécurité de l'information
 - Attribution des responsabilités en matière de sécurité de l'information
 - Système d'autorisation concernant les moyens de traitement de l'information
 - Engagements de confidentialité
 - Relations avec les autorités
 - Relations avec des groupes de spécialistes
 - Revue indépendante de la sécurité de l'information
- Tiers
 - Identification des risques provenant des tiers
 - La sécurité et les clients
 - La sécurité dans les accords conclus avec des tiers

DevSecOps

