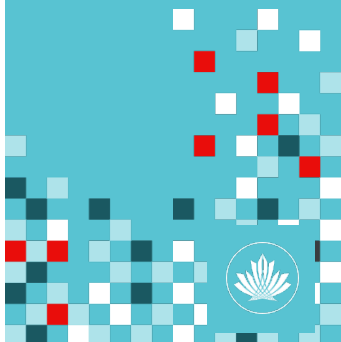
Ma blonde pense que je ne respecte pas assez sa vie privée…

… en tout cas, c’est ce qu’elle écrit dans son journal intime.



Ce qu'il faut savoir sur le cadre d'application en cybersécurité du NIST

Jeff Gardiner, pMBA, B.Sc., B.A., CISSP, CD | Calcul Canada

Le 29 avril 2021

De la compote de pomme!
Non, attendez une minute…

Identifier le problème

Est-ce…

- …un problème technique?
- … un problème de processus?
- … un problème de protection de renseignements personnels?
- … un problème de méconnaissance des menaces?
- … un problème de contrôle de la sécurité?
- … un problème de sécurité de l’information?

Quel problème la cybersécurité règle-t-elle?


Orchidée
PARIS
SHOES
S.P.A

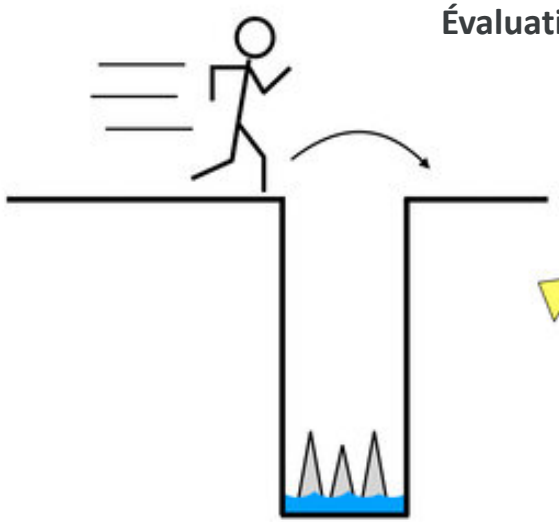
RISQUE = PROBABILITÉ x RÉPERCUSSIONS

Assessment of Risk Exposure = Risk Probability x Impact

(Severity = Likelihood x Consequence)

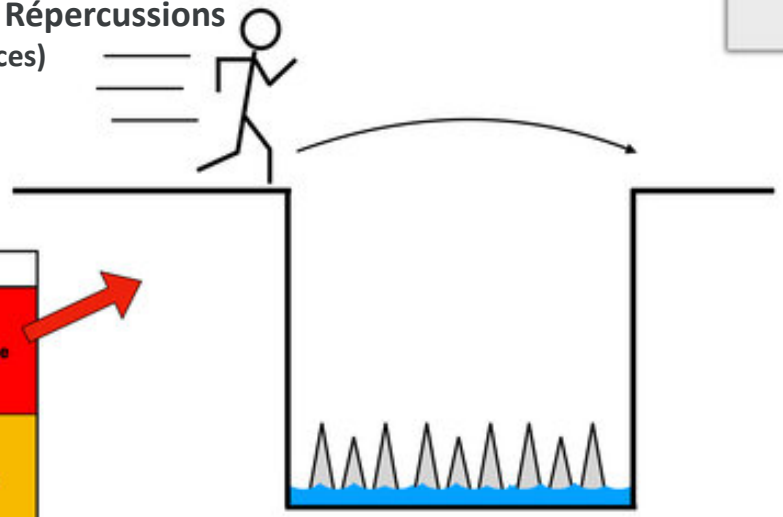
Évaluation du degré de risque = Probabilité x Répercussions

(Gravité = Vraisemblance x Conséquences)



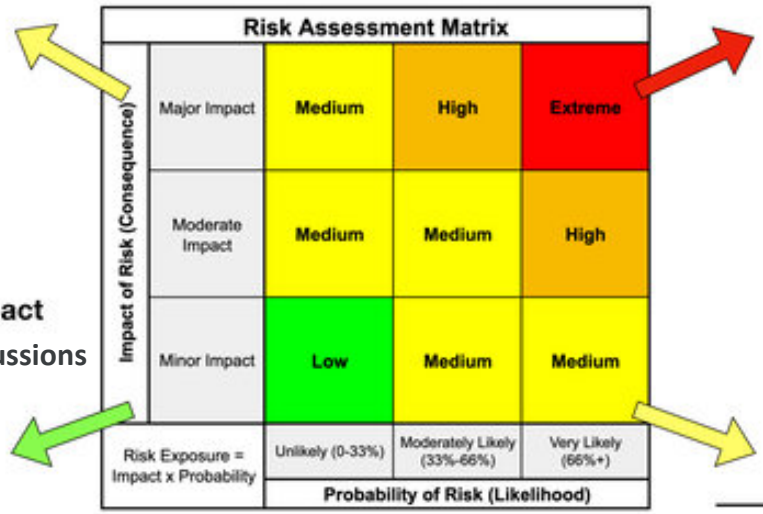
Low Probability & High Impact

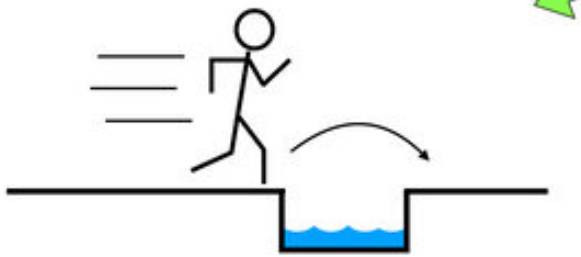
Faible probabilité et sérieuses répercussions



High Probability & High Impact

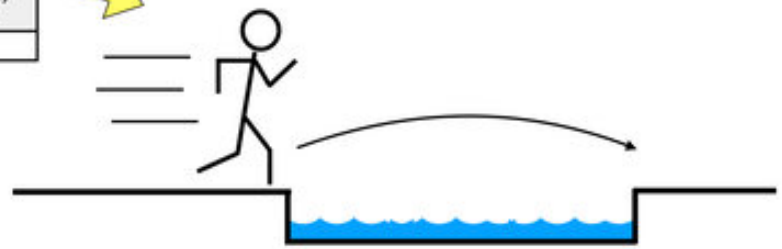
Probabilité élevée et sérieuses répercussions





Low Probability & Low Impact

Faible probabilité et faibles répercussions



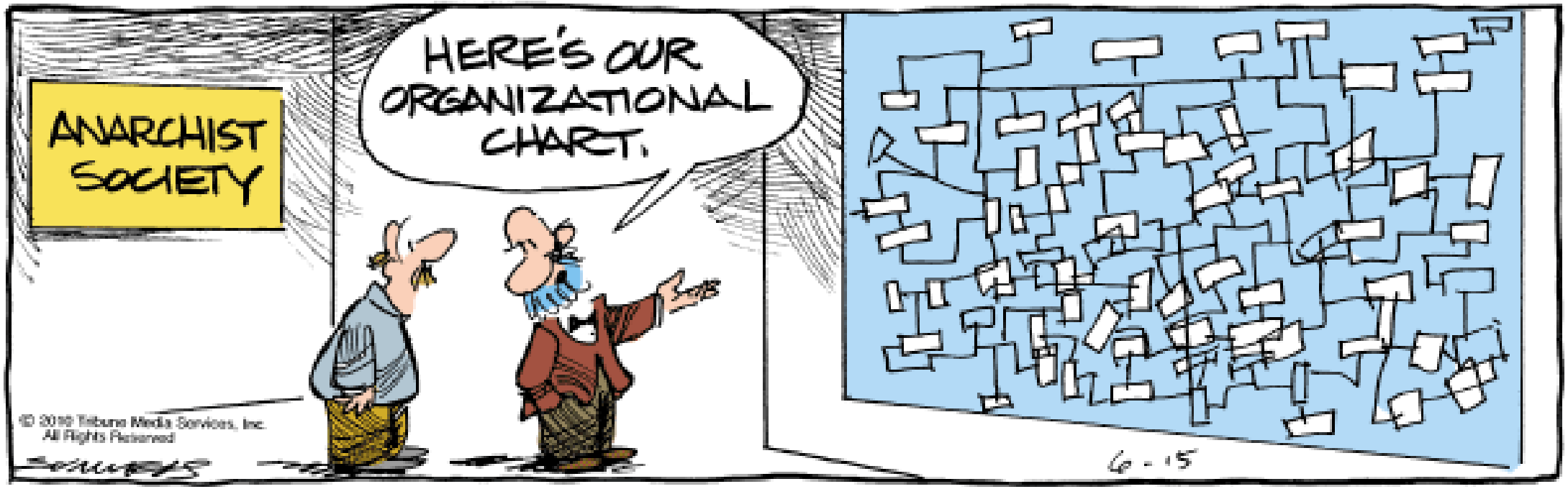
High Probability & Low Impact

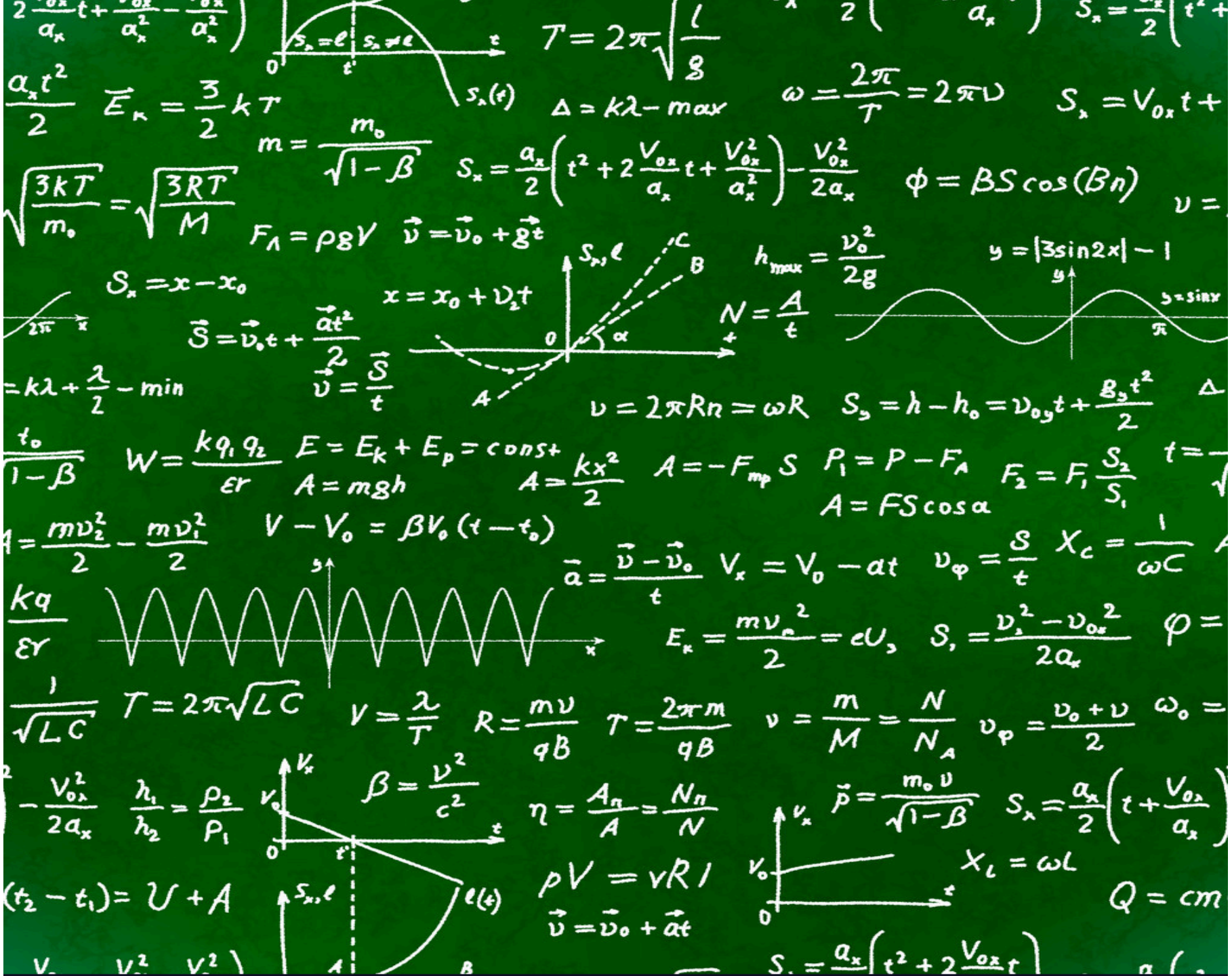
Probabilité élevée et faibles répercussions

Pourquoi la cybersécurité est-elle nécessaire?

Société des anarchistes

Et voici notre organigramme




$T = 2\pi\sqrt{\frac{l}{g}}$
$\frac{a_x t^2}{2}$
$\vec{E}_к = \frac{3}{2}kT$
$m = \frac{m_0}{\sqrt{1-\beta}}$
$\Delta = k\lambda - max$
$\omega = \frac{2\pi}{T} = 2\pi\upsilon$
$S_x = V_{0x}t +$
$\sqrt{\frac{3kT}{m_0}} = \sqrt{\frac{3RT}{M}}$
$S_x = \frac{a_x}{2}\left(t^2 + 2\frac{V_{0x}}{a_x}t + \frac{V_{0x}^2}{a_x^2}\right) - \frac{V_{0x}^2}{2a_x}$
$\phi = BS\cos(Bn)$
$F_A = \rho g V$
$\vec{\upsilon} = \vec{\upsilon}_0 + \vec{g}t$
$h_{max} = \frac{\upsilon_0^2}{2g}$
$y = |3\sin 2x| - 1$
$S_x = x - x_0$
$x = x_0 + \upsilon_x t$
$N = \frac{A}{t}$
$\vec{S} = \vec{\upsilon}_0 t + \frac{\vec{a}t^2}{2}$
$\vec{\upsilon} = \frac{\vec{S}}{t}$
$= k\lambda + \frac{\lambda}{2} - min$
$\upsilon = 2\pi Rn = \omega R$
$S_y = h - h_0 = \upsilon_{0y}t + \frac{g_y t^2}{2}$
$\frac{t_0}{\sqrt{1-\beta}}$
$W = \frac{kq_1q_2}{\varepsilon r}$
$E = E_k + E_p = const$
$A = mgh$
$A = \frac{kx^2}{2}$
$A = -F_{mp}S$
$P_1 = P - F_A$
$F_2 = F_1\frac{S_2}{S_1}$
$A = FS\cos\alpha$
$= \frac{m\upsilon_2^2}{2} - \frac{m\upsilon_1^2}{2}$
$V - V_0 = \beta V_0(t - t_0)$
$\vec{a} = \frac{\vec{\upsilon} - \vec{\upsilon}_0}{t}$
$V_x = V_0 - at$
$\upsilon_\varphi = \frac{S}{t}$
$X_C = \frac{1}{\omega C}$
$\frac{kq}{\varepsilon r}$
$E_к = \frac{m\upsilon_e^2}{2} = eU_з$
$S_1 = \frac{\upsilon_x^2 - \upsilon_{0x}^2}{2a_x}$
$\varphi =$
$\frac{1}{\sqrt{LC}}$
$T = 2\pi\sqrt{LC}$
$V = \frac{\lambda}{T}$
$R = \frac{m\upsilon}{qB}$
$T = \frac{2\pi m}{qB}$
$\upsilon = \frac{m}{M} = \frac{N}{N_A}$
$\upsilon_p = \frac{\upsilon_0 + \upsilon}{2}$
$\omega_0 =$
$\frac{V_{0x}^2}{2a_x}$
$\frac{h_1}{h_2} = \frac{\rho_2}{\rho_1}$
$\beta = \frac{\upsilon^2}{c^2}$
$\eta = \frac{A_n}{A} = \frac{N_n}{N}$
$\vec{p} = \frac{m_0\upsilon}{\sqrt{1-\beta}}$
$S_x = \frac{a_x}{2}\left(t + \frac{V_{0x}}{a_x}\right)$
$X_L = \omega L$
$(t_2 - t_1) = U + A$
$pV = \nu RT$
$\vec{\upsilon} = \vec{\upsilon}_0 + \vec{a}t$
$Q = cm$
$S_x = \frac{a_x}{2}\left(t^2 + 2\frac{V_{0x}}{a_x}t\right)$

Qu’est-ce que le NIST?

- Le **National Institute of Standards and Technology** (**NIST**) est un organisme américain qui ne règlemente pas.

- Sa fondation remonte à en 1901 (anciennement, *National Bureau of Standards*).

- Commission consultative sur la sécurité et la protection des renseignements personnels

- Publie des normes et des cadres d'application

Qui utilise les cadres d'application du NIST?

- Le gouvernement des É.-U.
- La moitié des entreprises américaines
- Le gouvernement canadien - ITSG-33 : gestion des risques (repose sur la norme 800-53 Rev 4 du NIST)
- Recommandé au secteur public par le gouvernement du Canada https://cyber.gc.ca/fr/en-route-vers-la-securite-dentreprise
- Canarie et beaucoup d'universités canadiennes

Le « Framework for Improving Critical Infrastructure Cybersecurity »

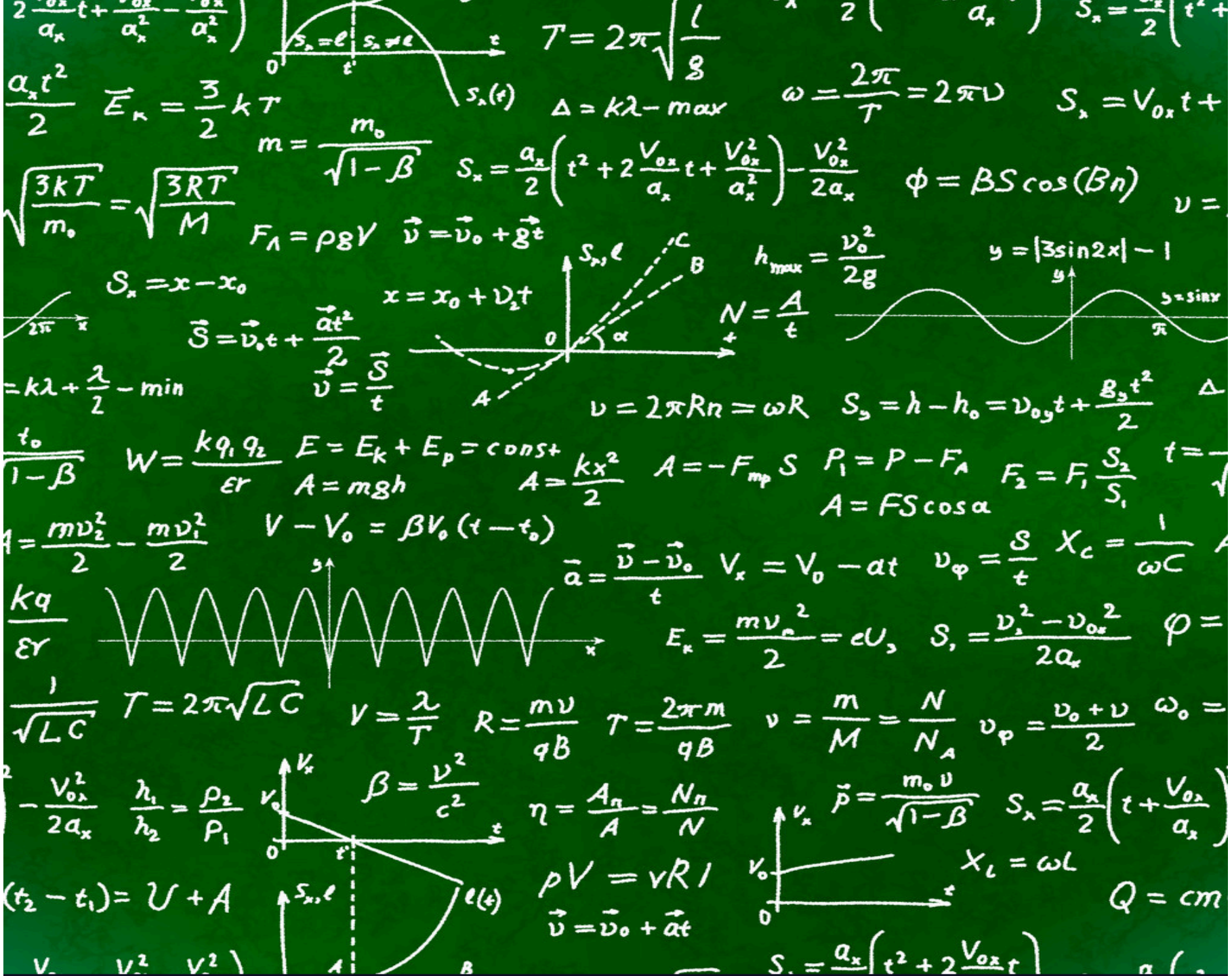
ou cadre d'application pour améliorer les infrastructures cruciales en cybersécurité

Ver 1.1

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

cyberframework@nist.gov


$T = 2\pi\sqrt{\frac{l}{g}}$
$\frac{a_x t^2}{2}$
$\vec{E}_к = \frac{3}{2}kT$
$m = \frac{m_0}{\sqrt{1-\beta}}$
$\Delta = k\lambda - max$
$\omega = \frac{2\pi}{T} = 2\pi\upsilon$
$S_x = V_{0x}t +$
$\sqrt{\frac{3kT}{m_0}} = \sqrt{\frac{3RT}{M}}$
$S_x = \frac{a_x}{2}\left(t^2 + 2\frac{V_{0x}}{a_x}t + \frac{V_{0x}^2}{a_x^2}\right) - \frac{V_{0x}^2}{2a_x}$
$\phi = BS\cos(Bn)$
$F_A = \rho g V$
$\vec{\upsilon} = \vec{\upsilon}_0 + \vec{g}t$
$h_{max} = \frac{\upsilon_0^2}{2g}$
$y = |3\sin 2x| - 1$
$S_x = x - x_0$
$x = x_0 + \upsilon_x t$
$N = \frac{A}{t}$
$\vec{S} = \vec{\upsilon}_0 t + \frac{\vec{a}t^2}{2}$
$\vec{\upsilon} = \frac{\vec{S}}{t}$
$= k\lambda + \frac{\lambda}{2} - min$
$\upsilon = 2\pi Rn = \omega R$
$S_y = h - h_0 = \upsilon_{0y}t + \frac{g_y t^2}{2}$
$\frac{t_0}{\sqrt{1-\beta}}$
$W = \frac{kq_1q_2}{\varepsilon r}$
$E = E_k + E_p = const$
$A = mgh$
$A = \frac{kx^2}{2}$
$A = -F_{mp}S$
$P_1 = P - F_A$
$F_2 = F_1\frac{S_2}{S_1}$
$A = FS\cos\alpha$
$= \frac{m\upsilon_2^2}{2} - \frac{m\upsilon_1^2}{2}$
$V - V_0 = \beta V_0(t - t_0)$
$\vec{a} = \frac{\vec{\upsilon} - \vec{\upsilon}_0}{t}$
$V_x = V_0 - at$
$\upsilon_\varphi = \frac{S}{t}$
$X_C = \frac{1}{\omega C}$
$\frac{kq}{\varepsilon r}$
$E_к = \frac{m\upsilon_e^2}{2} = eU_з$
$S_1 = \frac{\upsilon_x^2 - \upsilon_{0x}^2}{2a_x}$
$\varphi =$
$\frac{1}{\sqrt{LC}}$
$T = 2\pi\sqrt{LC}$
$V = \frac{\lambda}{T}$
$R = \frac{m\upsilon}{qB}$
$T = \frac{2\pi m}{qB}$
$\upsilon = \frac{m}{M} = \frac{N}{N_A}$
$\upsilon_p = \frac{\upsilon_0 + \upsilon}{2}$
$\omega_0 =$
$\frac{V_{0x}^2}{2a_x}$
$\frac{h_1}{h_2} = \frac{\rho_2}{\rho_1}$
$\beta = \frac{\upsilon^2}{c^2}$
$\eta = \frac{A_n}{A} = \frac{N_n}{N}$
$\vec{p} = \frac{m_0\upsilon}{\sqrt{1-\beta}}$
$S_x = \frac{a_x}{2}\left(t + \frac{V_{0x}}{a_x}\right)$
$X_L = \omega L$
$(t_2 - t_1) = U + A$
$pV = \nu RT$
$\vec{\upsilon} = \vec{\upsilon}_0 + \vec{a}t$
$Q = cm$
$S_x = \frac{a_x}{2}\left(t^2 + 2\frac{V_{0x}}{a_x}t\right)$

Principales caractéristiques

Fondements des versions actuelles et futures du cadre d'application

Utilise un langage courant et peu compliqué

- Compréhensible pour de nombreux professionnels

S'adapte à beaucoup de **technologies**[1.1], **phases de cycle de vie**[1.1], secteurs et usages

- Conçu pour être *individualisé*

Repose sur les risques

- Répertoire des issues en cybersécurité
- N'indique pas *en quoi* ni *dans quelle mesure* la cybersécurité convient ou pas

Conçu pour être combiné

- Tirer parti de ce qui existe déjà et fonctionne bien

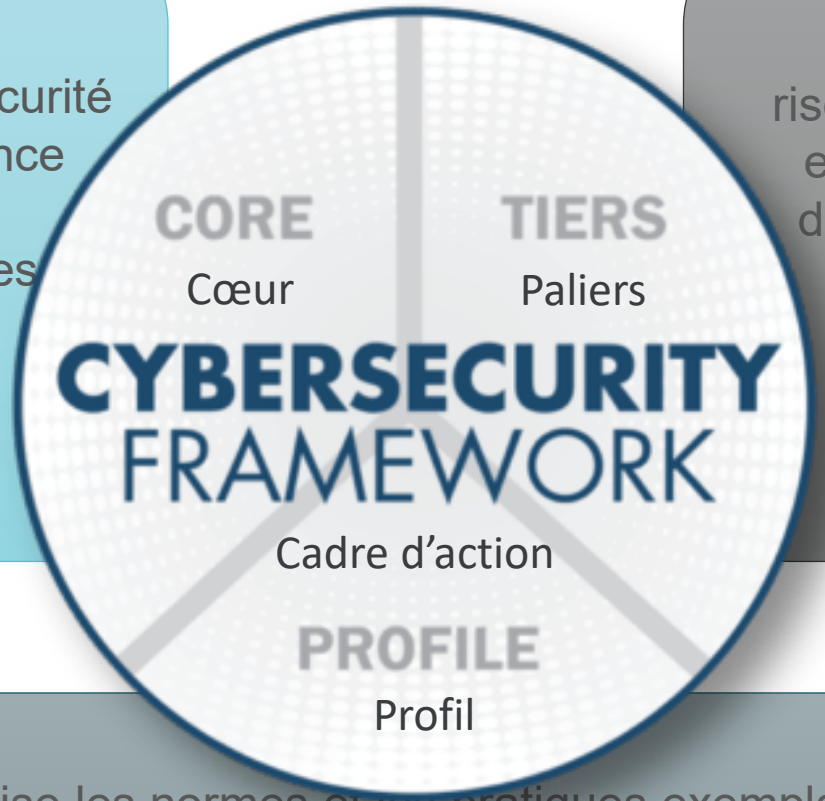
Document en évolution

- Permet aux pratiques exemplaires de devenir une *norme pour chacun*
- Peut être mis à jour d'après la manière dont les *technologies et les menaces* évoluent
- Progresse *plus rapidement* que la réglementation et la législation
- Peut être actualisé en fonction de ce que les intervenants *découvrent lors de la mise en œuvre*

Éléments du cadre d'application en cybersécurité

Issues de la cybersécurité et sources de référence

Permet de signaler les cyber-risques dans l'organisation

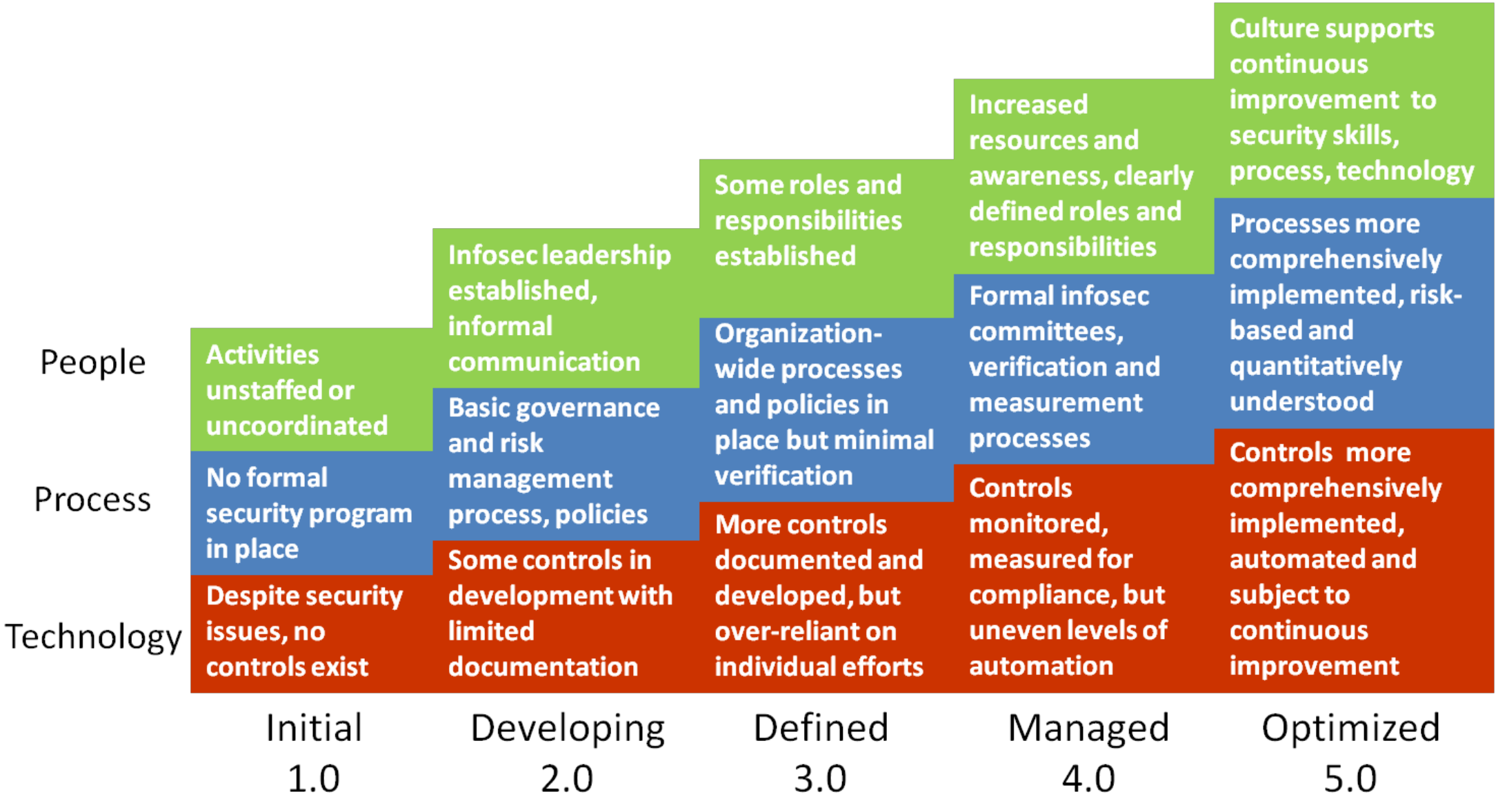


Décrit comment l'organisation gère les risques en cybersécurité et gradue les pratiques de gestion des risques; en présente les principales caractéristiques

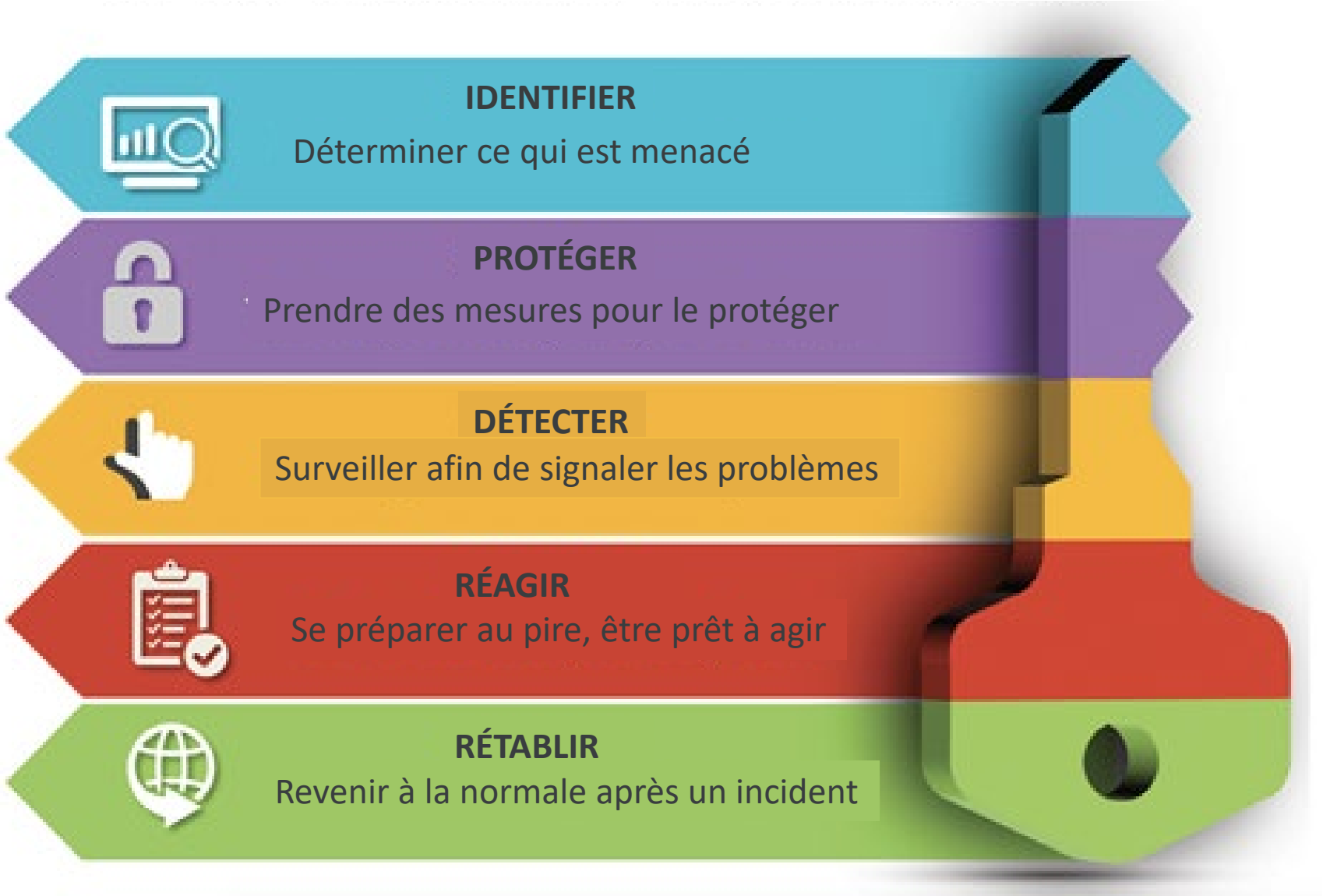
Harmonise les normes et les pratiques exemplaires de l'industrie avec les principes du cadre d'application dans un cas pratique
Facilite la priorisation et la quantification sans perdre de vue les impératifs de l'entreprise

PALIERS DE MISE EN ŒUVRE

Vers la maturité en cybersécurité

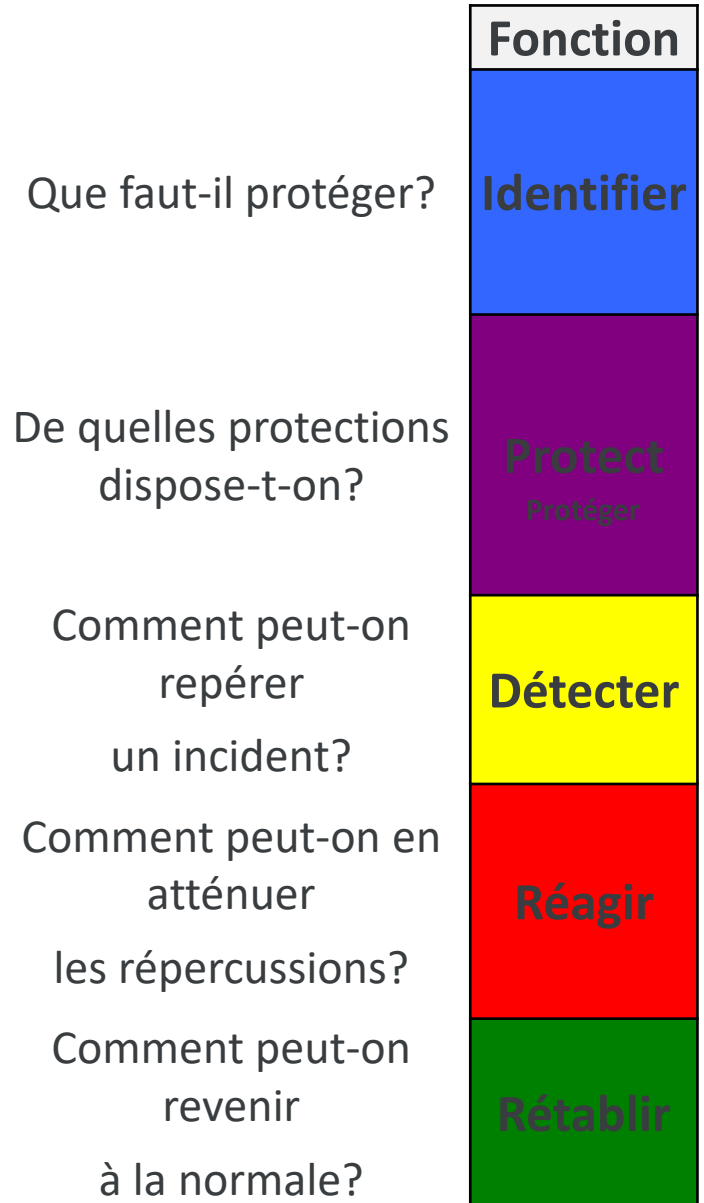


Les cinq fonctions du cadre d'action en cybersécurité du NIST



Cœur

Répertoire des issues en cybersécurité



- Se comprend facilement
- S’applique à n’importe quelle méthode de gestion des risques
- Définit la portée réelle de la cybersécurité
- Englobe prévention et réaction

Cœur

Répertoire des issues en cybersécurité

What processes and assets need protection?

What safeguards are available?

What techniques can identify incidents?

What techniques can contain impacts of incidents?

What techniques can restore capabilities?

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management[1.1]
Protect	**Identity Management, Authentication and Access Control**[1.1]
	Awareness and Training
	Data Security
	Information Protection Processes & Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

Cœur – Exemple[1.1]

Élément du cadre d'application en cybersécurité

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	**CIS CSC** 4 **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9

Cœur – Exemple[1.1]

Élément du cadre d'application en cybersécurité

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

Cœur – Exemple

Élément du cadre d'application en cybersécurité

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Analysis (RS.AN):** Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Forensics are performed	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	**CIS CSC** 19 **COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev. 4** SI-5, PM-15

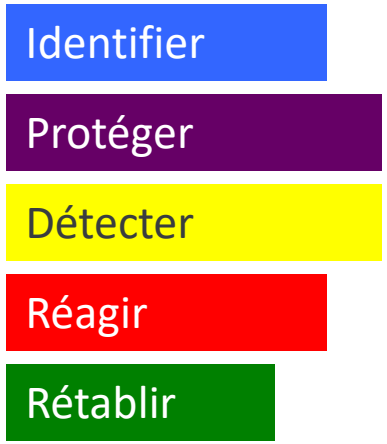
Élément	Version 1.1	Remarques
Fonctions	5	
Catégories	23	• Ajout d'une catégorie dans ID.SC – chaîne d'approvisionnement
Sous-catégories	108	• Ajout de 5 sous-catégories dans ID.SC • Ajout de 2 sous-catégories dans PR.AC • Ajout de 1 sous-catégorie chacune dans PR.DS, PR.PT et RS.AN • Énoncé plus clair dans 7 autres
Sources de référence	5	

Profil

Individualiser le cadre d'application en cybersécurité

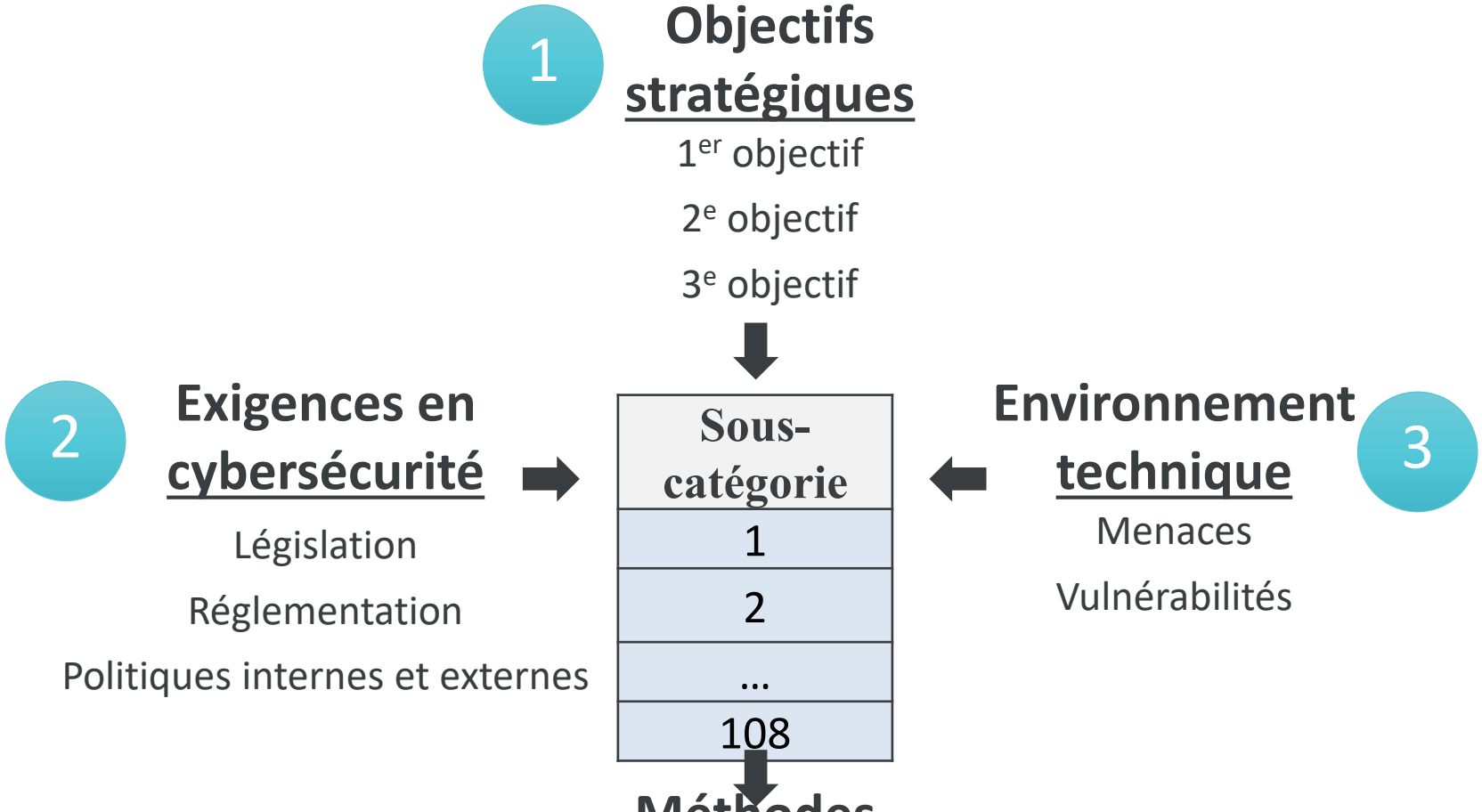
Façons d'envisager un profil :

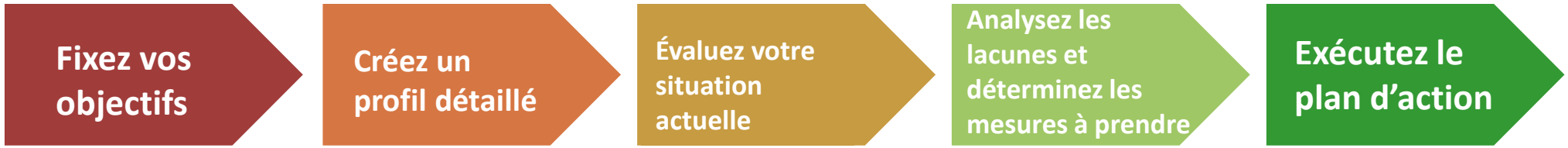
- Personnaliser le Cœur pour un secteur, un sous-secteur ou un organisme donnés
- Combiner la logique de la mission et les issues en cybersécurité
- Harmoniser les besoins de cybersécurité avec les méthodes d'exploitation
- Évaluer et exprimer l'état final recherché
- Faciliter la prise de décisions pour gérer les risques en cybersécurité

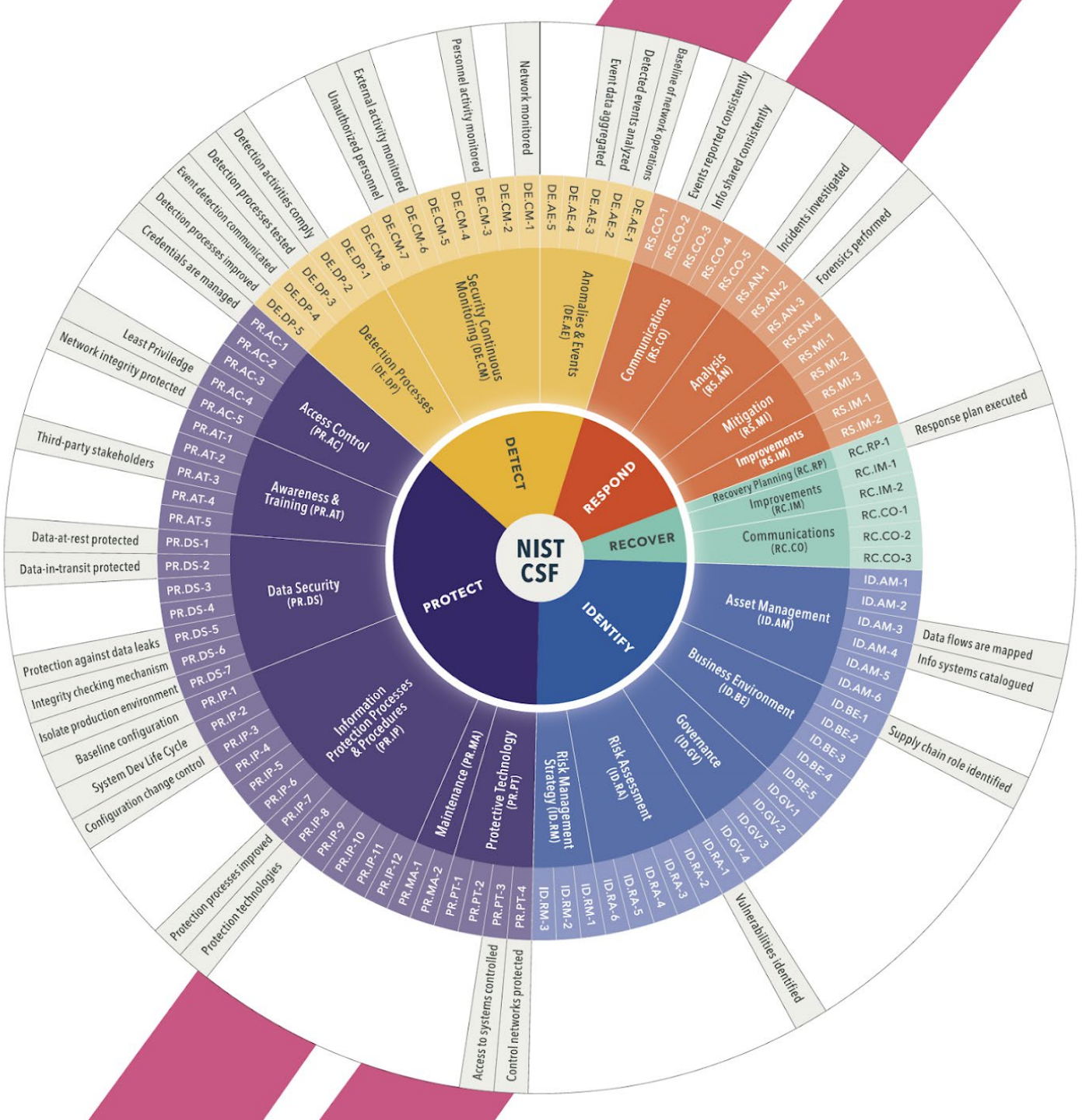


Renseignements de base sur le profil

Le profil peut être créé à partir de trois sortes d'informations.



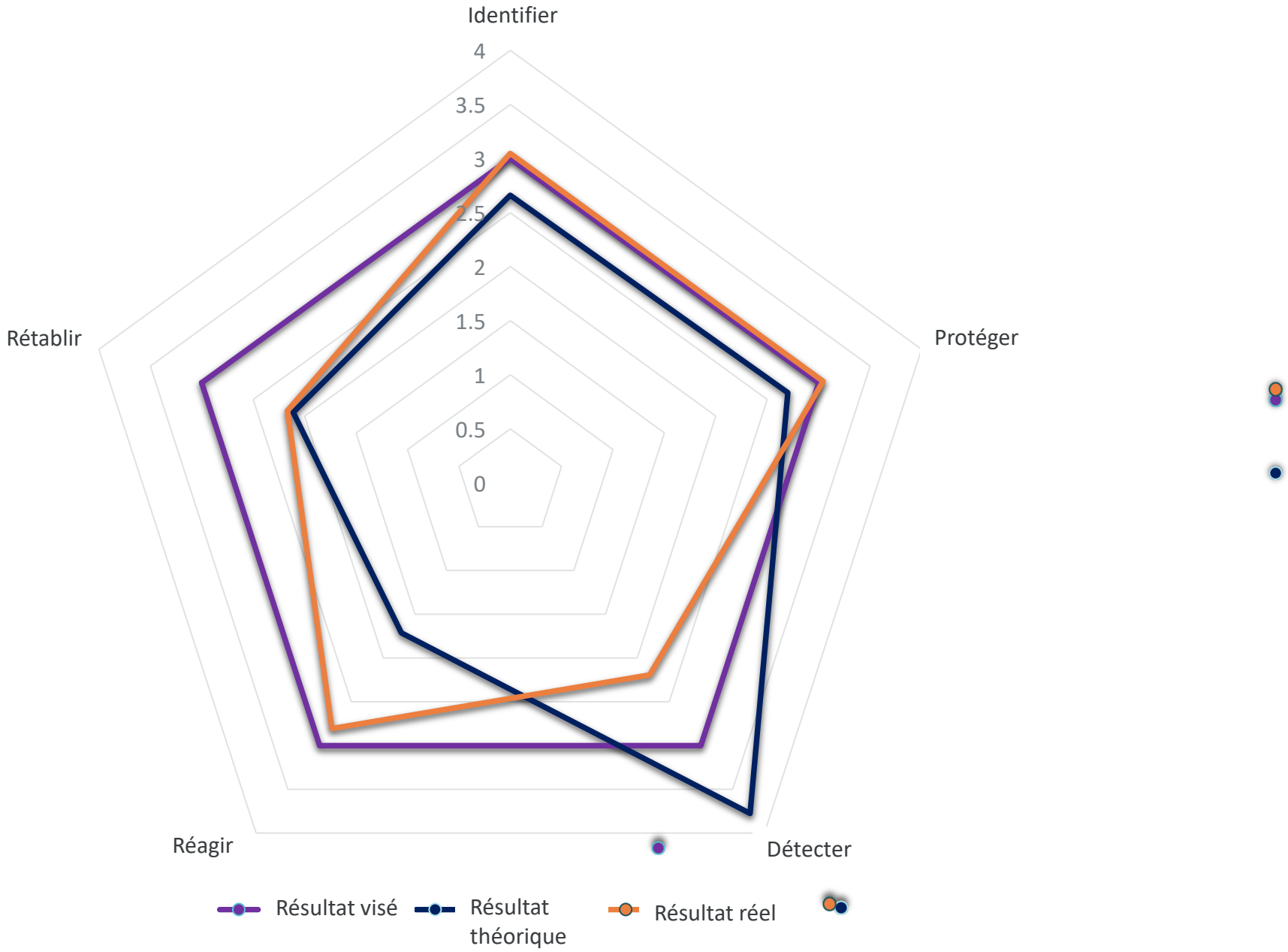

Fixez vos objectifs
Créez un profil détaillé
Évaluez votre situation actuelle
Analysez les lacunes et déterminez les mesures à prendre
Exécutez le plan d'action


NIST CSF
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
Asset Management (ID.AM)
Business Environment (ID.BE)
Governance (ID.GV)
Risk Assessment (ID.RA)
Risk Management Strategy (ID.RM)
Access Control (PR.AC)
Awareness & Training (PR.AT)
Data Security (PR.DS)
Information Protection Processes & Procedures (PR.IP)
Maintenance (PR.MA)
Protective Technology (PR.PT)
Anomalies & Events (DE.AE)
Security Continuous Monitoring (DE.CM)
Detection Processes (DE.DP)
Communications (RS.CO)
Analysis (RS.AN)
Mitigation (RS.MI)
Improvements (RS.IM)
Recovery Planning (RC.RP)
Improvements (RC.IM)
Communications (RC.CO)
ID.AM-1
ID.AM-2
ID.AM-3
ID.AM-4
ID.AM-5
ID.AM-6
ID.BE-1
ID.BE-2
ID.BE-3
ID.BE-4
ID.BE-5
ID.GV-1
ID.GV-2
ID.GV-3
ID.GV-4
ID.RA-1
ID.RA-2
ID.RA-3
ID.RA-4
ID.RA-5
ID.RA-6
ID.RM-1
ID.RM-2
ID.RM-3
PR.AC-1
PR.AC-2
PR.AC-3
PR.AC-4
PR.AC-5
PR.AT-1
PR.AT-2
PR.AT-3
PR.AT-4
PR.AT-5
PR.DS-1
PR.DS-2
PR.DS-3
PR.DS-4
PR.DS-5
PR.DS-6
PR.DS-7
PR.IP-1
PR.IP-2
PR.IP-3
PR.IP-4
PR.IP-5
PR.IP-6
PR.IP-7
PR.IP-8
PR.IP-9
PR.IP-10
PR.IP-11
PR.IP-12
PR.MA-1
PR.MA-2
PR.PT-1
PR.PT-2
PR.PT-3
PR.PT-4
DE.AE-1
DE.AE-2
DE.AE-3
DE.AE-4
DE.AE-5
DE.CM-1
DE.CM-2
DE.CM-3
DE.CM-4
DE.CM-5
DE.CM-6
DE.CM-7
DE.CM-8
DE.DP-1
DE.DP-2
DE.DP-3
DE.DP-4
DE.DP-5
RS.CO-1
RS.CO-2
RS.CO-3
RS.CO-4
RS.CO-5
RS.AN-1
RS.AN-2
RS.AN-3
RS.AN-4
RS.MI-1
RS.MI-2
RS.MI-3
RS.IM-1
RS.IM-2
RC.RP-1
RC.IM-1
RC.IM-2
RC.CO-1
RC.CO-2
RC.CO-3
Data flows are mapped
Info systems catalogued
Supply chain role identified
Vulnerabilities identified
Access to systems controlled
Control networks protected
Protection processes improved
Protection technologies
Configuration change control
System Dev Life Cycle
Baseline configuration
Isolate production environment
Integrity checking mechanism
Protection against data leaks
Data-in-transit protected
Data-at-rest protected
Third-party stakeholders
Network integrity protected
Least Priviledge
Credentials are managed
Detection processes improved
Event detection communicated
Detection processes tested
Detection activities comply
Unauthorized personnel
External activity monitored
Personnel activity monitored
Network monitored
Event data aggregated
Detected events analyzed
Baseline of network operations
Events reported consistently
Info shared consistently
Incidents investigated
Forensics performed
Response plan executed

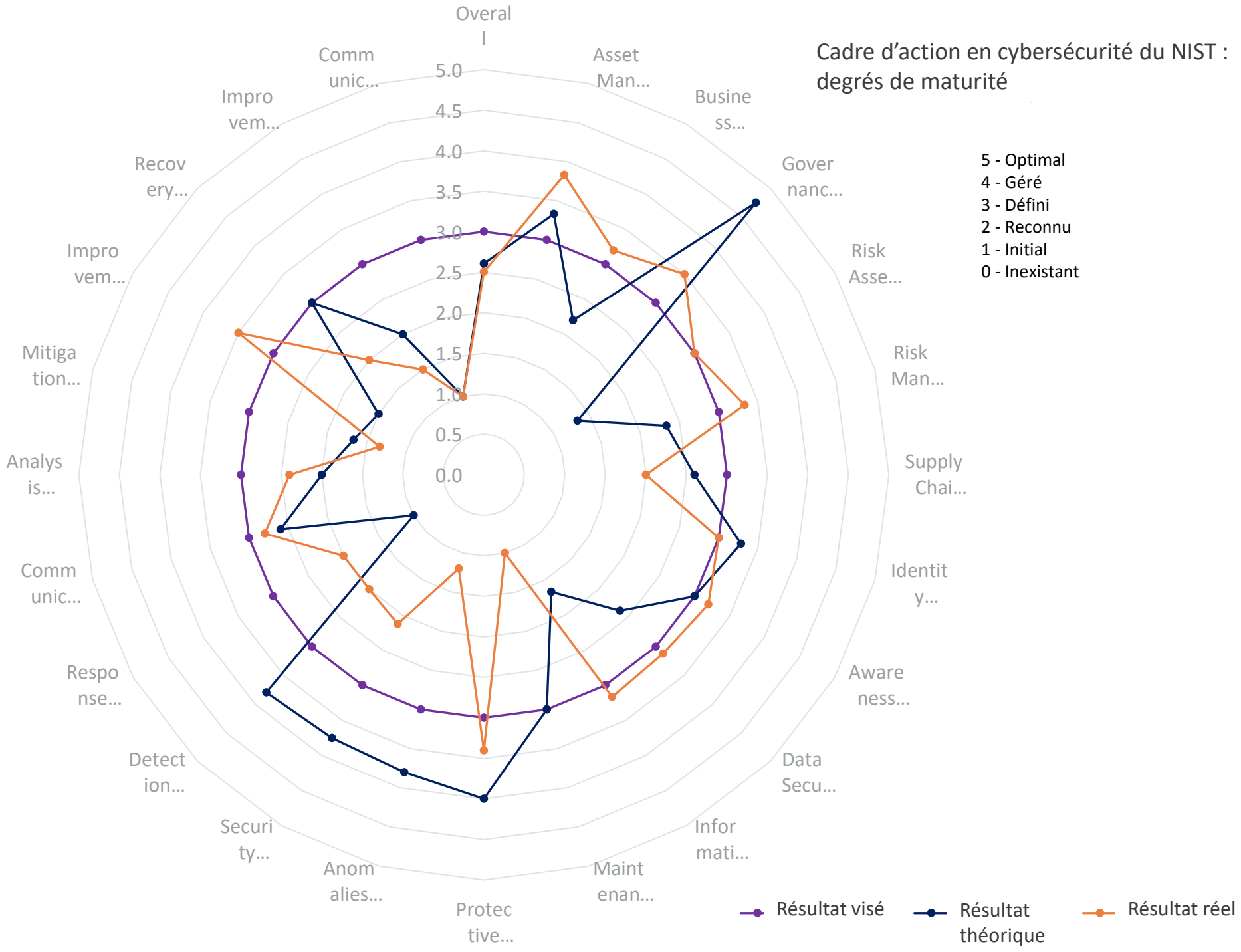
Un exemple : le NIST en action

Ce qu'on ne peut quantifier ne peut être géré. – Peter Drucker

Cadre d’action en cybersécurité du NIST : objectifs stratégiques ou généraux



Cadre d’action en cybersécurité du NIST : degrés de maturité



Une norme? – Un cadre d'application?

Ce qu'on ne peut quantifier ne peut être géré. – Peter Drucker

Normes

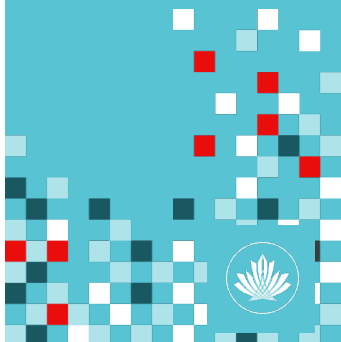
CIS CSC – **Norme de contrôle (sans les 20 critiques)**
COBIT 5 – **Objectifs de contrôle pour les technologies de l'information et les technologies connexes (ISACA)**
ISA 62443-2-1:2009 – **Sécurité des systèmes d'automatisation et de commande**
ISO/IEC 27001:2013 – **Management de la sécurité de l'information (norme de l'ISO)**
NIST 800-53 Rev 4 – **Sécurité et mesures pour la protection des renseignements personnels**

Norme

La conformité à une norme permet d’évaluer ou de valider le plan de l’organisation en cybersécurité.

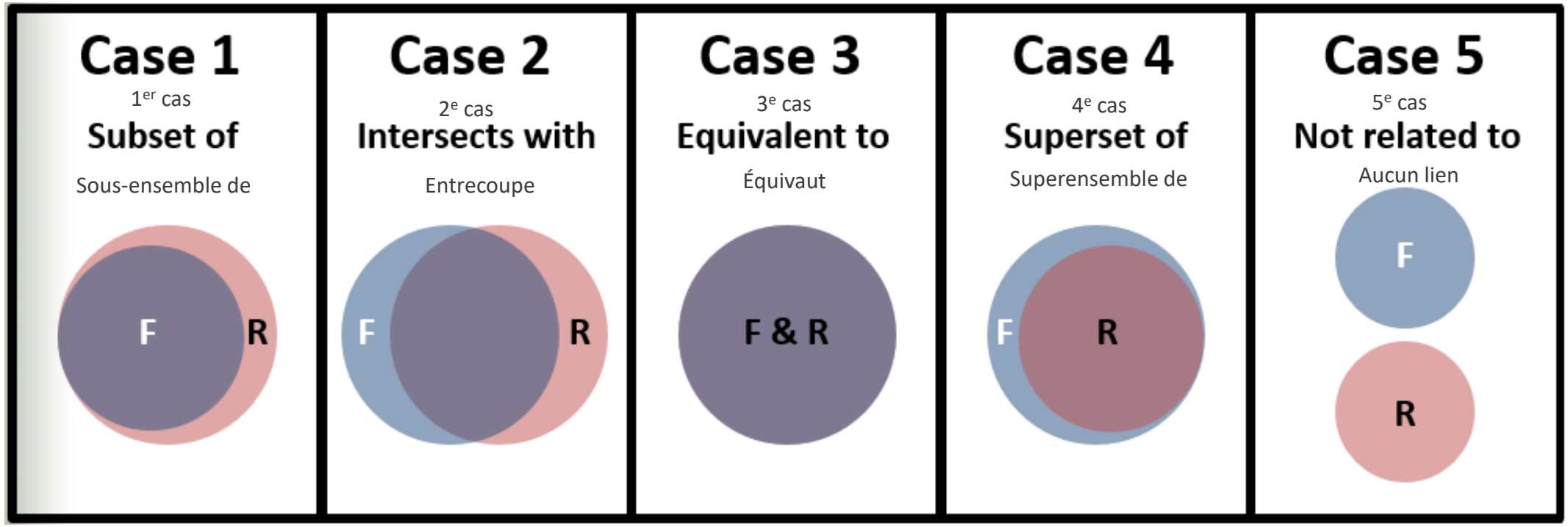
Cadre d’application

Le cadre d’application aide l’organisation à se concentrer sur les résultats.



Types de liens

Sources de référence en ligne



Clé

Cadre d'application – bleu

Document de référence - rouge

*Le **cadre d'application en cybersécurité du NIST** est un instrument élaboré par le Département du commerce des É.-U. en collaboration avec les secteurs public et privé ainsi que les universités pour rehausser la gestion des risques en cybersécurité. Son usage est facultatif.*


R
Q

canarie

canarie.ca | @canarie_inc

jeff.gardiner@computecanada.ca

Webinar Recording Policy

This webinar will be recorded and archived, including all audio. The video will be archived on the CANARIE YouTube channel and may be promoted through CANARIE communication channels.

Any text questions or comments, if responded to, will remain anonymous and not be part of the recording.

The recorded video will include your voice, if audio participation is enabled.

Politique concernant l'enregistrement des webinaires

Ce webinaire sera enregistré et archivé, y compris tout le matériel audio. La vidéo sera conservée sur le canal YouTube de CANARIE et pourra être promue au moyen des filières de communication de CANARIE.

Si on y répond, les questions écrites et orales demeureront anonymes et ne feront pas partie de l'enregistrement.

Toutefois, si la fonction « participation audio » a été activée, le fichier vidéo inclura votre voix.