Modélisation d'infrastructures informatiques pour l'identification et la prévention des risques

Présentation forcée préparée sous la pression insupportable de mes encadrants

Benjamin Somers

Sommaire

Sommaire

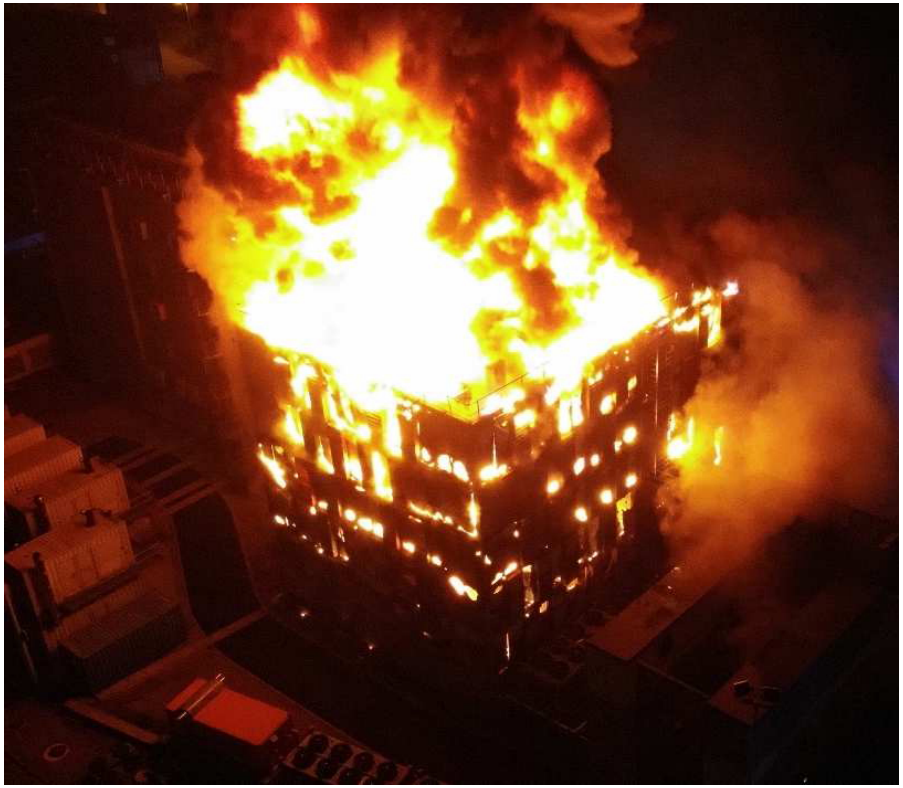
L’analyse de risque « comme à la maison »

Elles sont belles mes batteries, hein ? C’est français!

Mais dis-donc Roger, c’est pas un peu dangereux de ne pas avoir de système d’extinction d’incendie ?

T’inquiète!

L’analyse de risque « comme à la maison »



L’analyse de risque « comme à la maison »

Et donc cette zone réseau ne peut pas accéder à celle-là, c’est ça ?

Euuuuh. Ouais, on va dire ça, t’inquiète!

Très bien, voilà votre certification ISO 27000!

Sûreté et sécurité

Risque de sûreté

BLEEPINGCOMPUTER

Home > News > Security > CircleCI's hack caused by malware stealing engineer's 2FA-backed session

CircleCI's hack caused by malware stealing engineer's 2FA-backed session

By **Lawrence Abrams** January 14, 2023 05:28 PM 0

Hackers breached CircleCi in December after an engineer became infected with information-stealing malware that their 2FA-backed SSO session cookie, allowing access to the company's internal systems.

Earlier this month, CircleCi disclosed that they suffered a security incident and warned customers to rotate their tokens and secrets.

In a new security incident report on the attack, CircleCi says they first learned of the unauthorized access to their systems after a customer reported that their GitHub OAuth token had been compromised.

This compromise led to CircleCi automatically rotating the GitHub OAuth tokens for its customers.

On January 4th, an internal investigation concluded that an engineer had become infected on December 16th with information-stealing malware that the company's antivirus software did not detect.

This malware was able to steal a corporate session cookie that had already been authenticated via 2FA, allowing the threat actor to log in as the user without having to authenticate via 2FA again.

"Our investigation indicates that the malware was able to execute session cookie theft, enabling them to impersonate the targeted employee in a remote location and then escalate access to a subset of our production systems," explains CircleCi's new incident report.

Quarkslab's blog

Vulnerabilities in the TPM 2.0 reference implementation code

Date Tue 14 March 2023 By Francisco Falcon Category Vulnerability . Tags TPM Trusted Platform Module CVE-2023-1017 CVE-2023-1018

In this blog post we discuss the details of two vulnerabilities we discovered in the Trusted Platform Module (TPM) 2.0 reference implementation code. These two vulnerabilities, an out-of-bounds write (CVE-2023-1017) and an out-of-bounds read (CVE-2023-1018), affected several TPM 2.0 software implementations (such as the ones used by virtualization software) as well as a number of hardware TPMs.

Introduction

In October 2021, Microsoft released Windows 11. One of the installation requirements that stood out was the need for a Trusted Platform Module (TPM) 2.0. An implication of this requirement is that, in order to be able to run Windows 11 within a virtual machine, virtualization software must provide a TPM to VMs, either by doing passthrough to the hardware TPM on the host machine, or by supplying a virtual TPM to them.

We found this to be an interesting topic for vulnerability research, since the addition of virtual TPMs means extended attack surface on virtualization software that can be reached from within a guest, and so it could potentially be used for a virtual machine escape. As a result of the research effort, we discovered two security issues: an out-of-bounds write identified as CVE-2023-1017, and an out-of-bounds read identified as CVE-2023-1018. They can be triggered from user-mode applications by sending malicious TPM 2.0 commands with encrypted parameters. Interestingly, these two vulnerabilities turned out to have a way longer reach than we initially thought: given that they originate in the reference implementation code published by the Trusted Computing Group (TCG for short, the nonprofit organization that publishes and maintains the TPM specification), these security bugs affected not only every virtualization software we tested, but hardware implementations as well.

Risque de sécurité

Sûreté et sécurité

Risque de sûreté

- Entrave au fonctionnement des systèmes
- Cause non malveillante

Exemples :

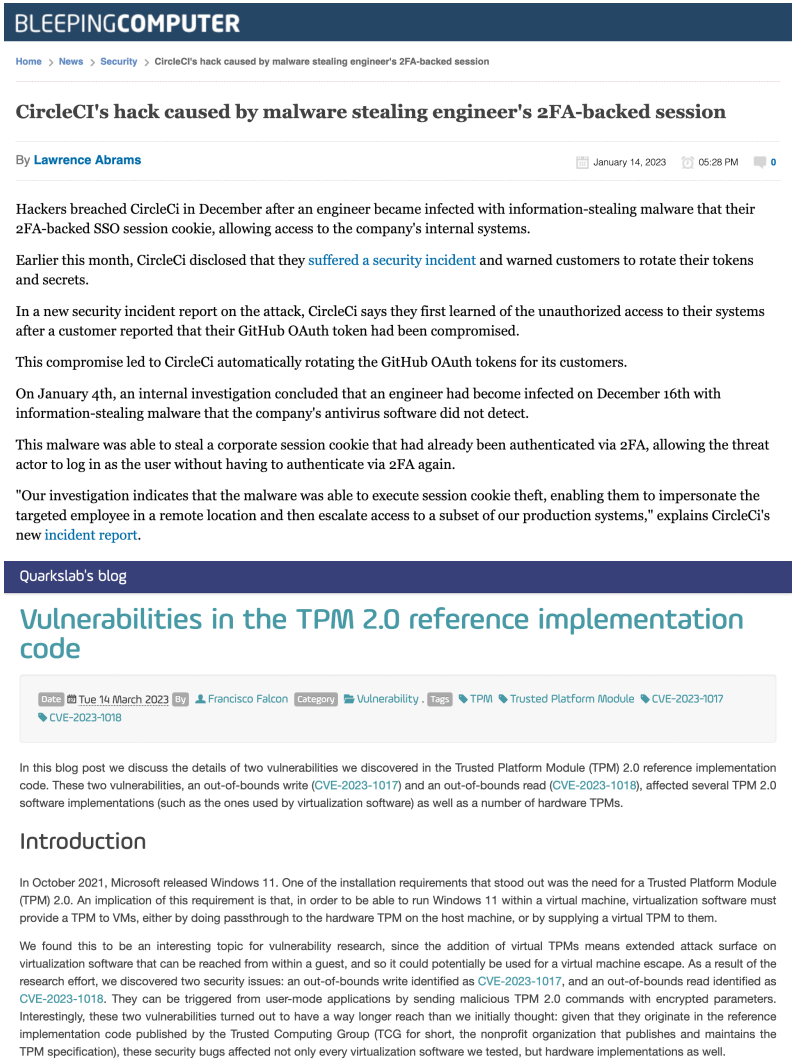
- Incendies de centres de données
- Dégradations fibre

Sûreté et sécurité

- Entrave au fonctionnement des systèmes
- Cause malveillante

Exemples :

- Exploitation de vulnérabilités
- Déni de service



BLEEPINGCOMPUTER

Home > News > Security > CircleCI's hack caused by malware stealing engineer's 2FA-backed session

CircleCI's hack caused by malware stealing engineer's 2FA-backed session

By **Lawrence Abrams** January 14, 2023 05:28 PM 0

Hackers breached CircleCi in December after an engineer became infected with information-stealing malware that their 2FA-backed SSO session cookie, allowing access to the company's internal systems.

Earlier this month, CircleCi disclosed that they suffered a security incident and warned customers to rotate their tokens and secrets.

In a new security incident report on the attack, CircleCi says they first learned of the unauthorized access to their systems after a customer reported that their GitHub OAuth token had been compromised.

This compromise led to CircleCi automatically rotating the GitHub OAuth tokens for its customers.

On January 4th, an internal investigation concluded that an engineer had become infected on December 16th with information-stealing malware that the company's antivirus software did not detect.

This malware was able to steal a corporate session cookie that had already been authenticated via 2FA, allowing the threat actor to log in as the user without having to authenticate via 2FA again.

"Our investigation indicates that the malware was able to execute session cookie theft, enabling them to impersonate the targeted employee in a remote location and then escalate access to a subset of our production systems," explains CircleCi's new incident report.

Quarkslab's blog

Vulnerabilities in the TPM 2.0 reference implementation code

Date Tue 14 March 2023 By Francisco Falcon Category Vulnerability . Tags TPM Trusted Platform Module CVE-2023-1017 CVE-2023-1018

In this blog post we discuss the details of two vulnerabilities we discovered in the Trusted Platform Module (TPM) 2.0 reference implementation code. These two vulnerabilities, an out-of-bounds write (CVE-2023-1017) and an out-of-bounds read (CVE-2023-1018), affected several TPM 2.0 software implementations (such as the ones used by virtualization software) as well as a number of hardware TPMs.

Introduction

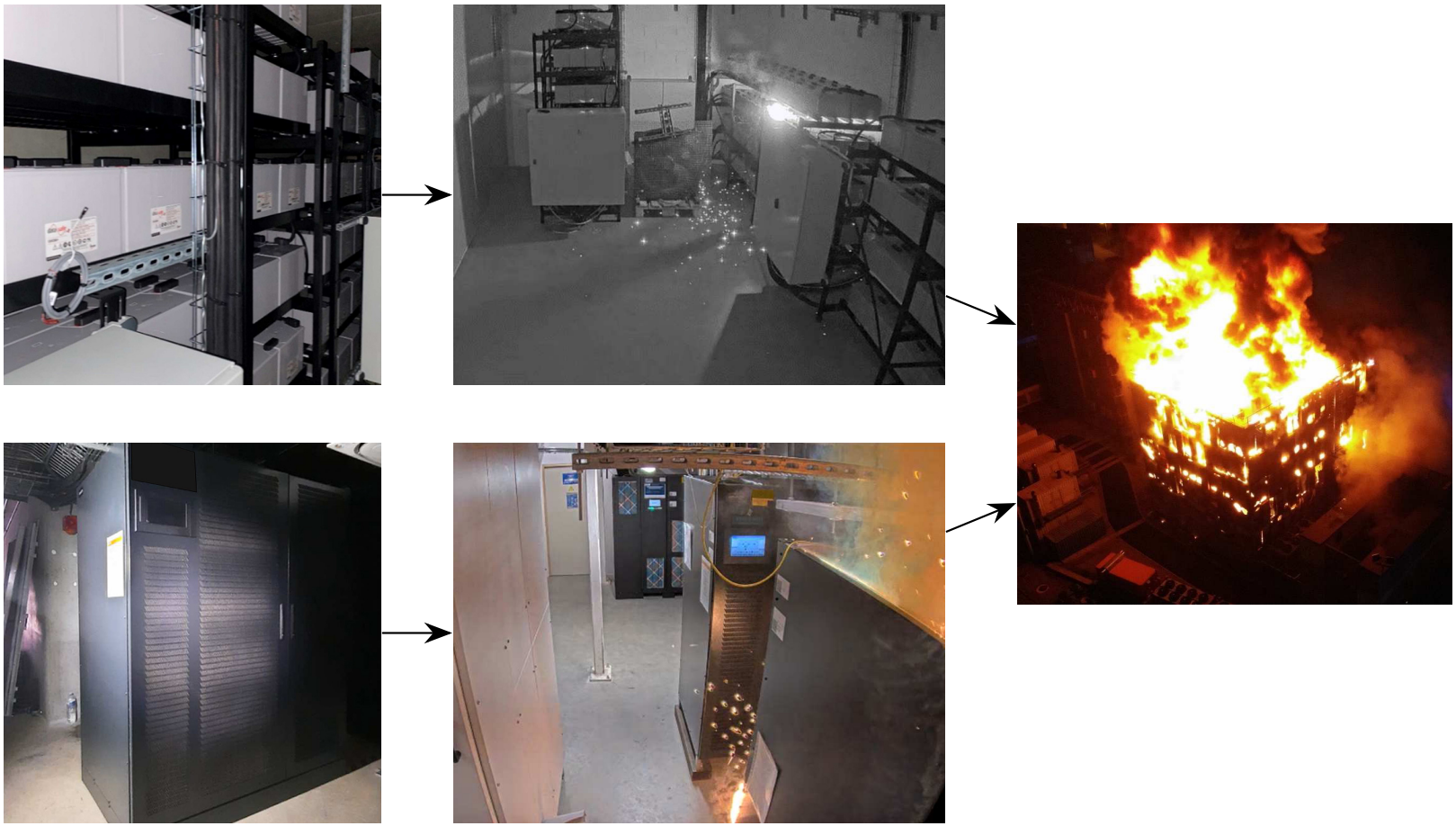
In October 2021, Microsoft released Windows 11. One of the installation requirements that stood out was the need for a Trusted Platform Module (TPM) 2.0. An implication of this requirement is that, in order to be able to run Windows 11 within a virtual machine, virtualization software must provide a TPM to VMs, either by doing passthrough to the hardware TPM on the host machine, or by supplying a virtual TPM to them.

We found this to be an interesting topic for vulnerability research, since the addition of virtual TPMs means extended attack surface on virtualization software that can be reached from within a guest, and so it could potentially be used for a virtual machine escape. As a result of the research effort, we discovered two security issues: an out-of-bounds write identified as CVE-2023-1017, and an out-of-bounds read identified as CVE-2023-1018. They can be triggered from user-mode applications by sending malicious TPM 2.0 commands with encrypted parameters. Interestingly, these two vulnerabilities turned out to have a way longer reach than we initially thought: given that they originate in the reference implementation code published by the Trusted Computing Group (TCG for short, the nonprofit organization that publishes and maintains the TPM specification), these security bugs affected not only every virtualization software we tested, but hardware implementations as well.

Risque de sécurité

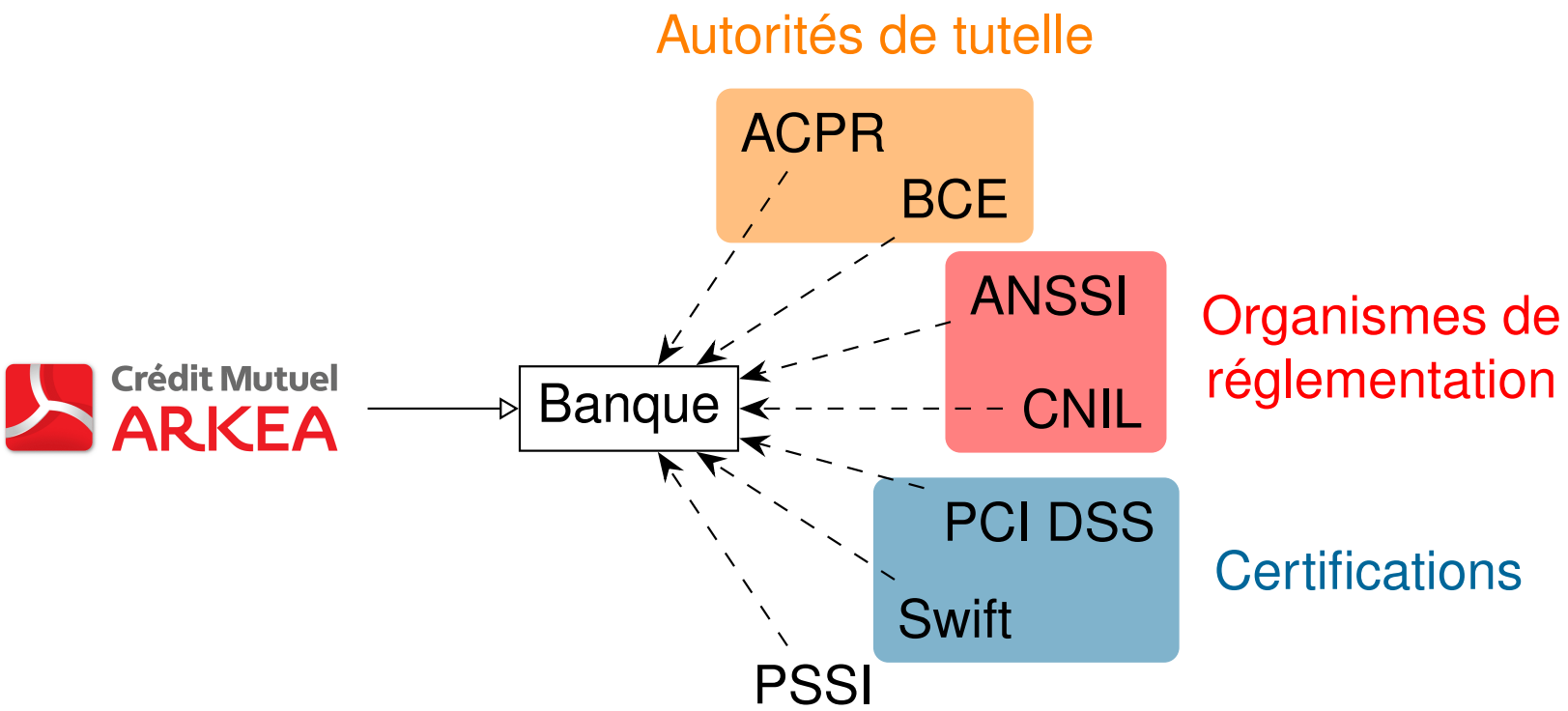
Contexte

- Des cascades de défaillances catastrophiques difficiles à prévoir



Contexte

- Des cascades de défaillances catastrophiques difficiles à prévoir
- Un grand nombre d'audits et certifications...



Contexte

- Des cascades de défaillances catastrophiques difficiles à prévoir
- Un grand nombre d'audits et certifications décrits en langage naturels et effectués manuellement

Contexte

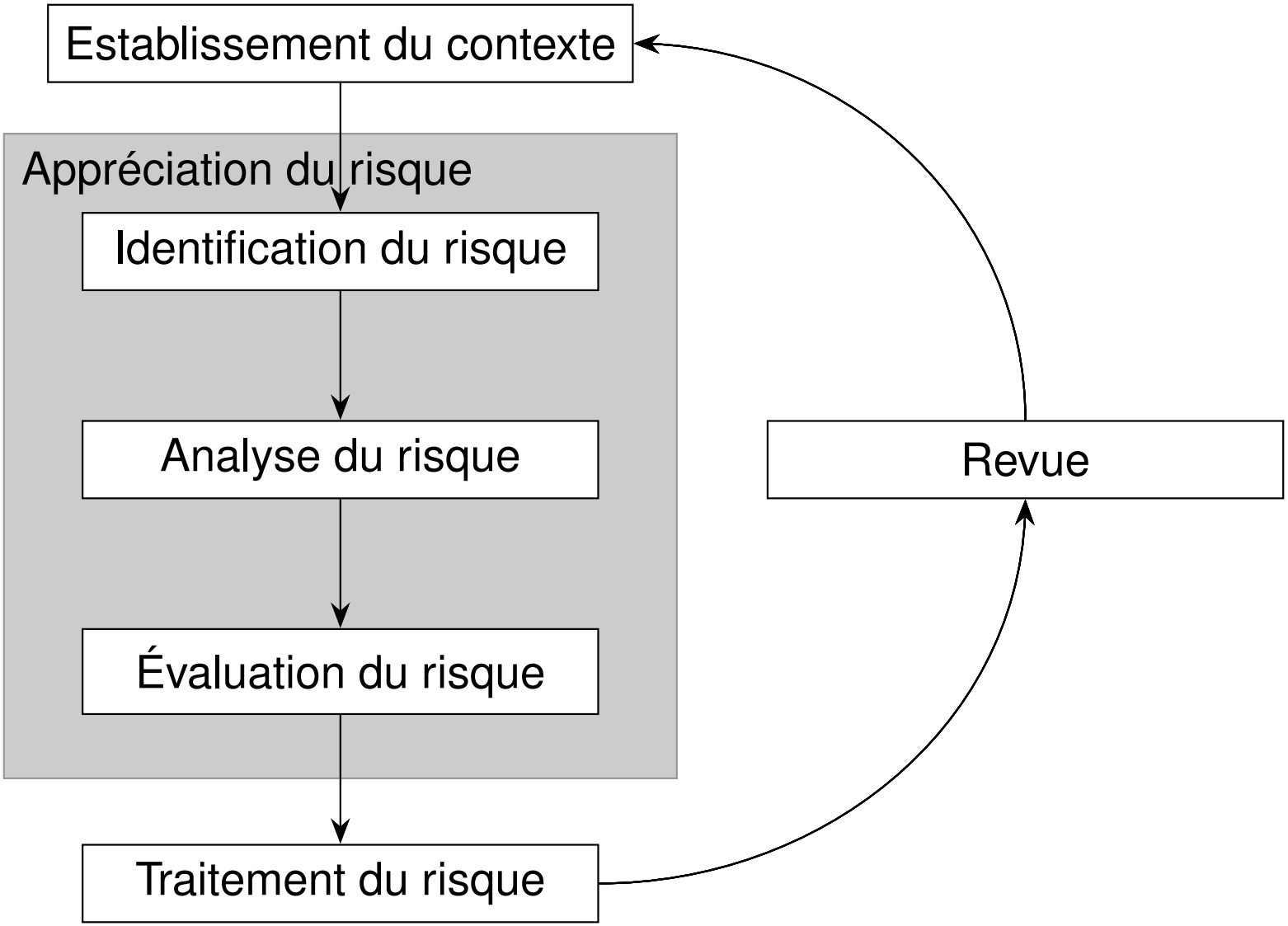
- Des cascades de défaillances catastrophiques difficiles à prévoir
- Un grand nombre d'audits et certifications décrits en langage naturels et effectués manuellement
- Une connaissance des infrastructures morcelée...

Contexte

- Des cascades de défaillances catastrophiques difficiles à prévoir
- Un grand nombre d'audits et certifications décrits en langage naturels et effectués manuellement
- Une connaissance des infrastructures morcelée présentant de nombreux décalages sémantiques

Sommaire

L'Évangile selon ISO 31000



L'Évangile selon P4S

- Modélisation d'infrastructure
- Fédération des modèles produits
- Vérification formelle de propriétés

L'Évangile selon ~~P4S~~ moi

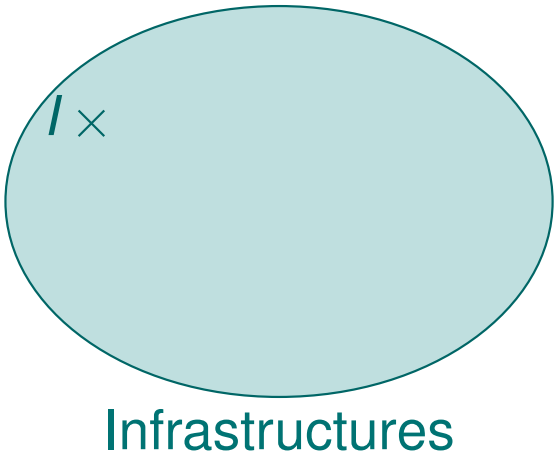
- Modélisation d'infrastructure
  - Un grand nombre d'employés, de départements, de métiers
  - Des propriétés qui traversent les domaines
  - Des modèles très liés aux propriétés à prouver
- Fédération des modèles produits
  - Une démarche collaborative des employés
  - Une réconciliation « agile » des modèles
  - Une intégration aux *workflows* collaboratifs des développeurs
- Vérification formelle de propriétés
  - Des propriétés très diverses
  - Des liens directs avec le risque...
  - ... mais avec d'importants décalages sémantiques

Les livres de chevet de l'analyste de risque IT

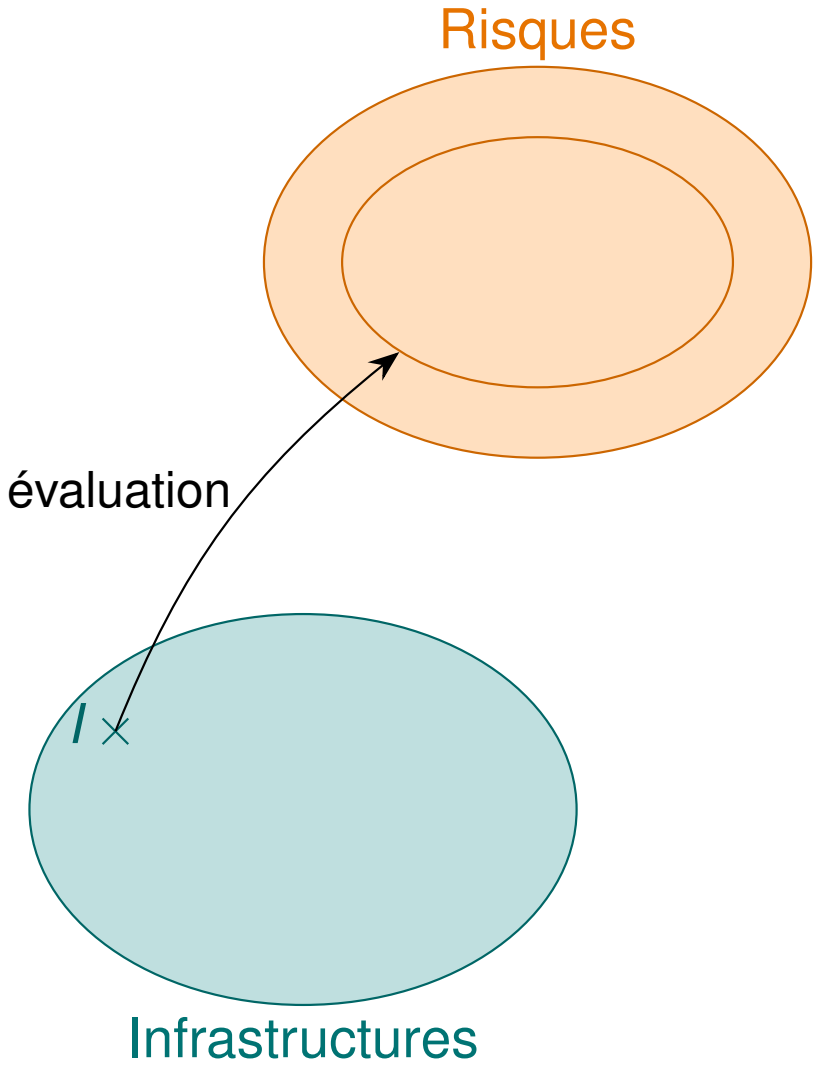
- ANSSI DAT-NT-028
- ARP4761
- EBIOS-RM
- Eurocode 8
- GR-63-CORE
- ISO 14258
- ISO/IEC/IEEE 15288
- ISO 19439
- ISO/IEC 27005
- ISO 31000
- NIST SP 800-53
- NIS 2 (soon^{TM})
- RGPD
- TOGAF

Oh mais j'ai aussi de quoi remplir cette colonne!

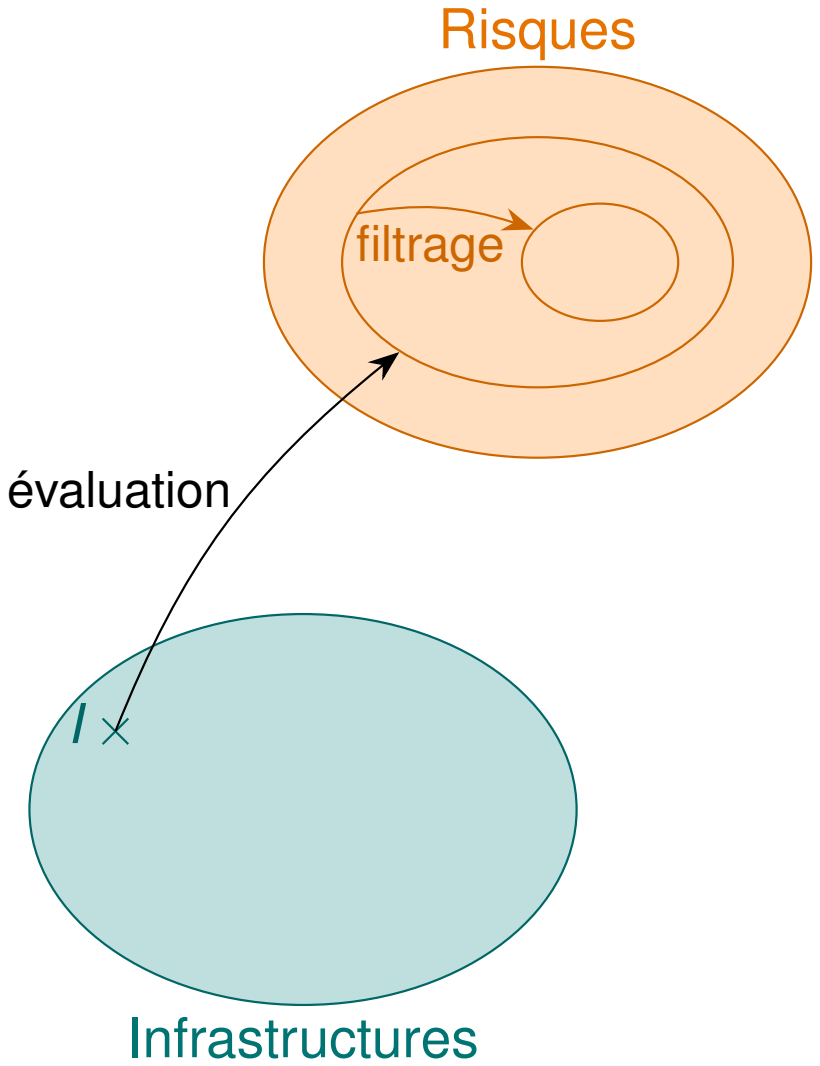
Cycle de gestion du risque



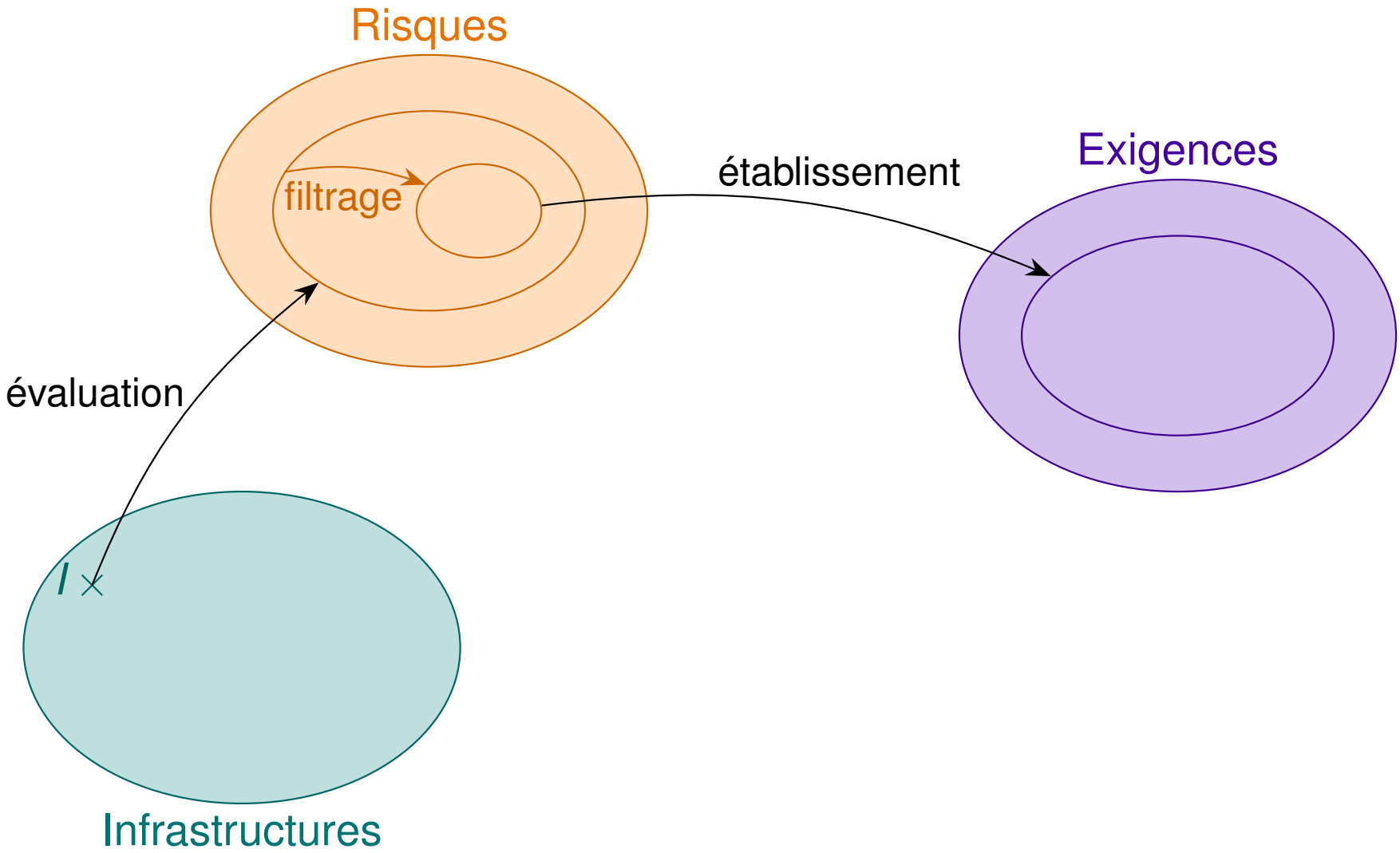
Cycle de gestion du risque



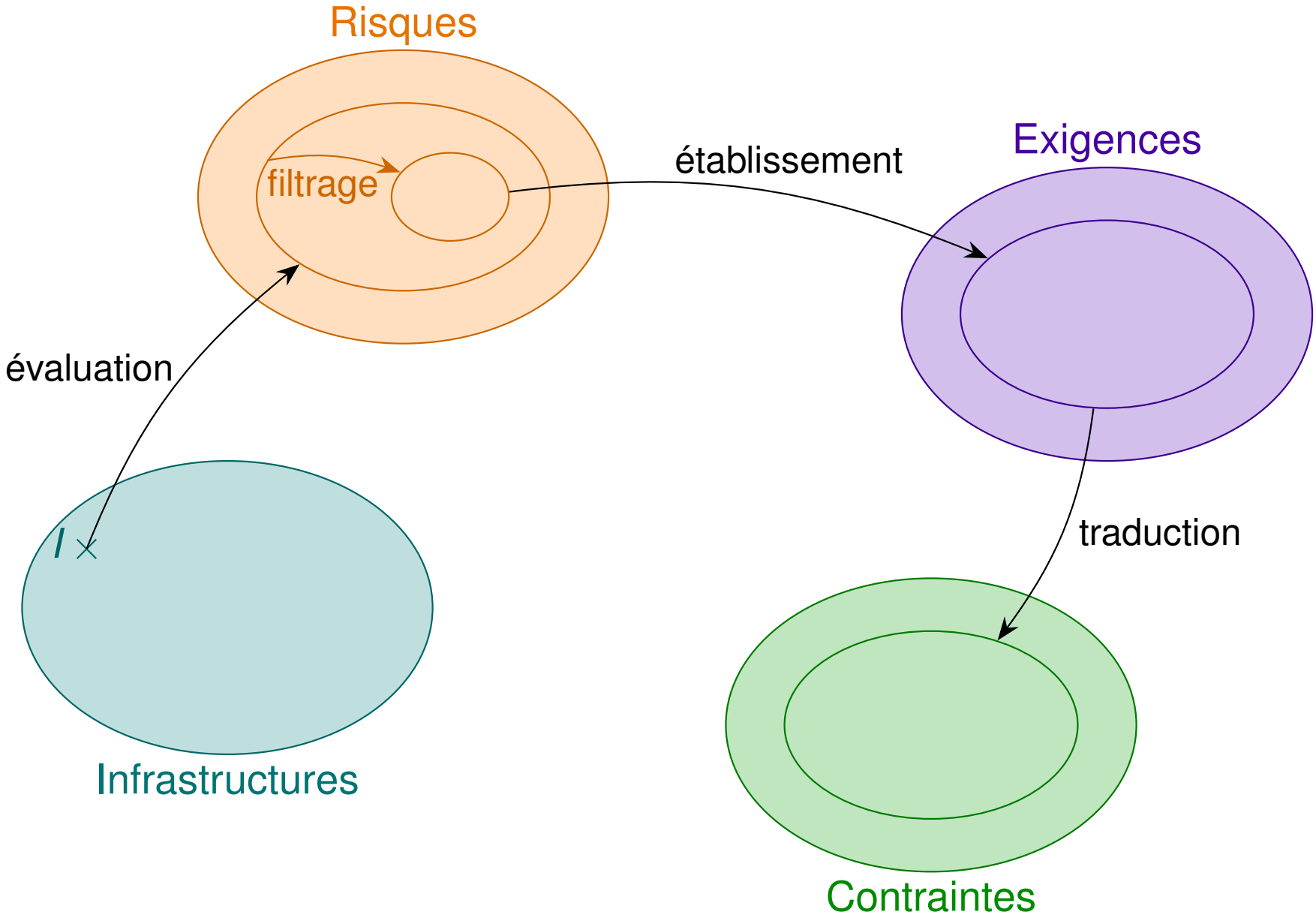
Cycle de gestion du risque



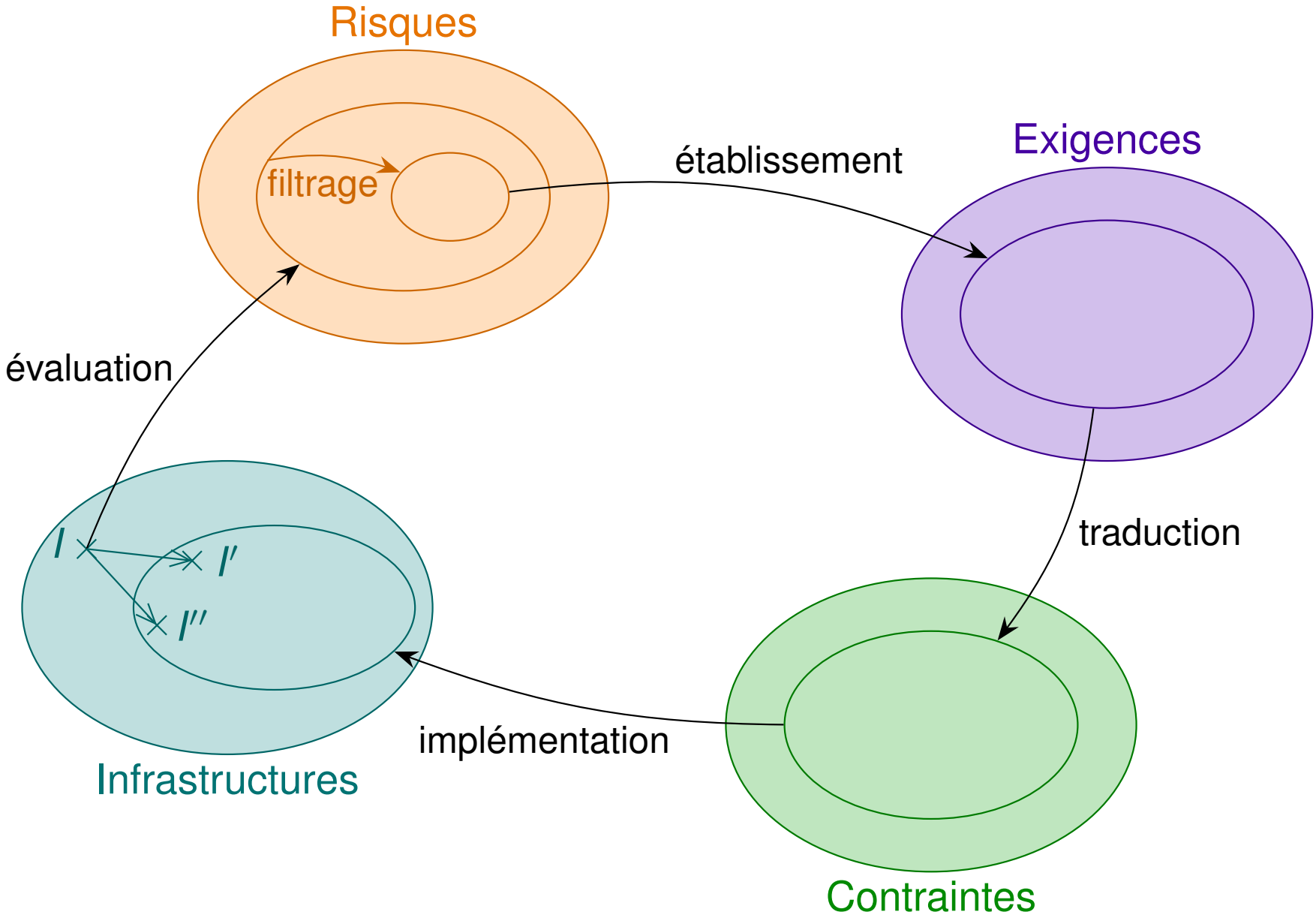
Cycle de gestion du risque



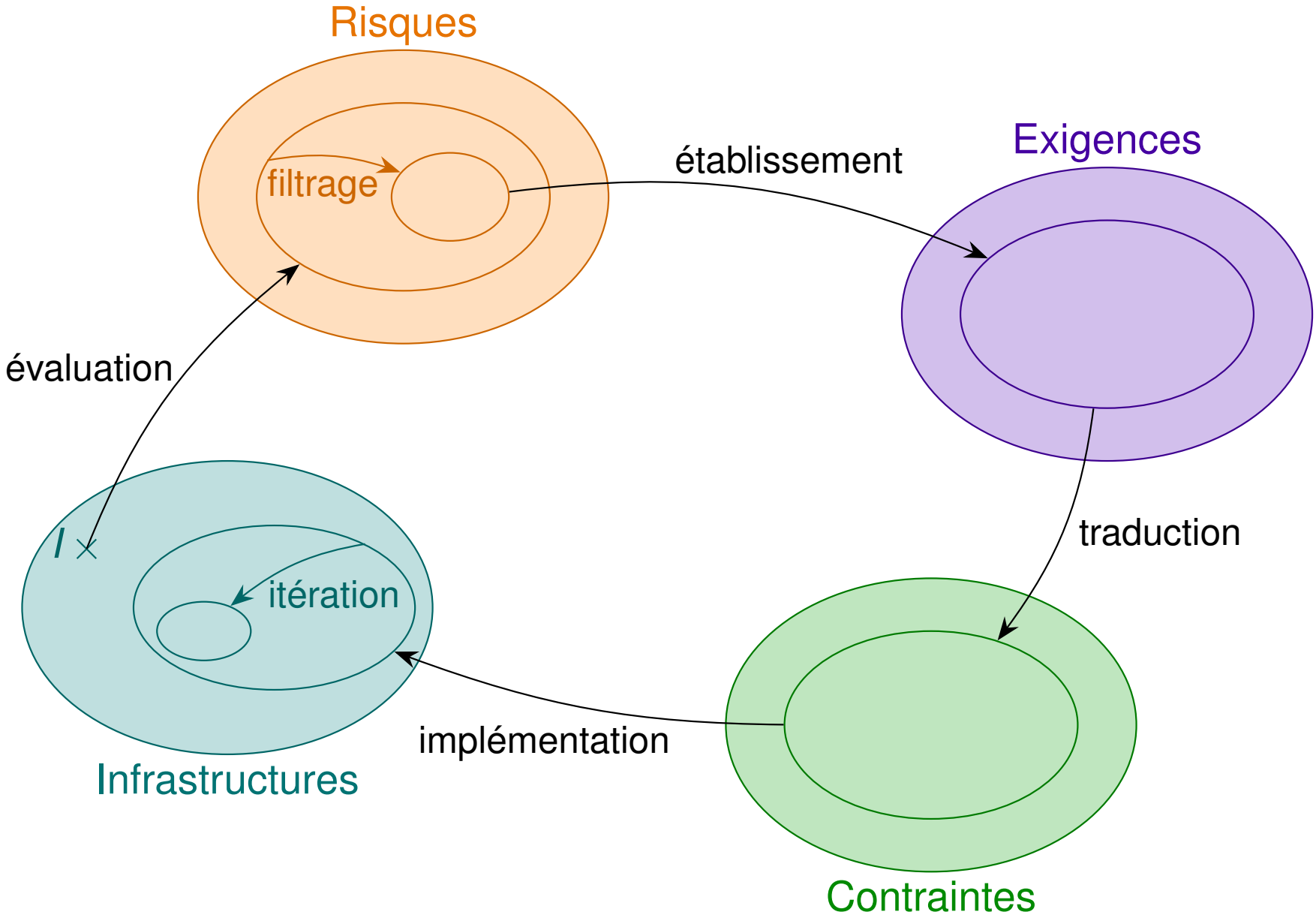
Cycle de gestion du risque



Cycle de gestion du risque



Cycle de gestion du risque



Sommaire

Des modèles techniques...

Démo parce que je n'ai pas de slides

... associés à des modèles experts

Démo parce que je n'ai toujours pas de slides

CL/I, un langage pivot de modélisation

Vous connaissez la chanson