Séance 1 – Introduction au risque dans l'écosystème numérique global

Management du risque (tronc commun)
EPITA 2025 – F. Giuliani

Dans quels secteurs d'activité les professionnels de l'IT doivent-ils gérer des risques ?

Un risque IT omniprésent

Tous les secteurs d'activités peuvent être touchés :

- Finance, santé, énergie, industrie, commerce…
- Impacts multiples : pertes financières, atteinte à la réputation, interruptions d'activité, fuite de données…

Data breach CYBERSÉCURITÉ \ SECTEUR PUBLIC \ SANTÉ

Cyberattaque à l'hôpital de Cannes : les hackers de LockBit publient 61 gigaoctets de données

L'hôpital Simone-Veil, à Cannes, avait été touché le 16 avril par une cyberattaque. Le groupe de hackers LockBit avait revendiqué l'opération et émis une demande de rançon expirant le 1er mai au soir. Ce matin, 61 gigaoctets de données personnelles de patients et d'agents pubics, et de données relatives au fonctionnement de l'hôpital, ont été publiés sur le dark web.

Yoann Bourgin

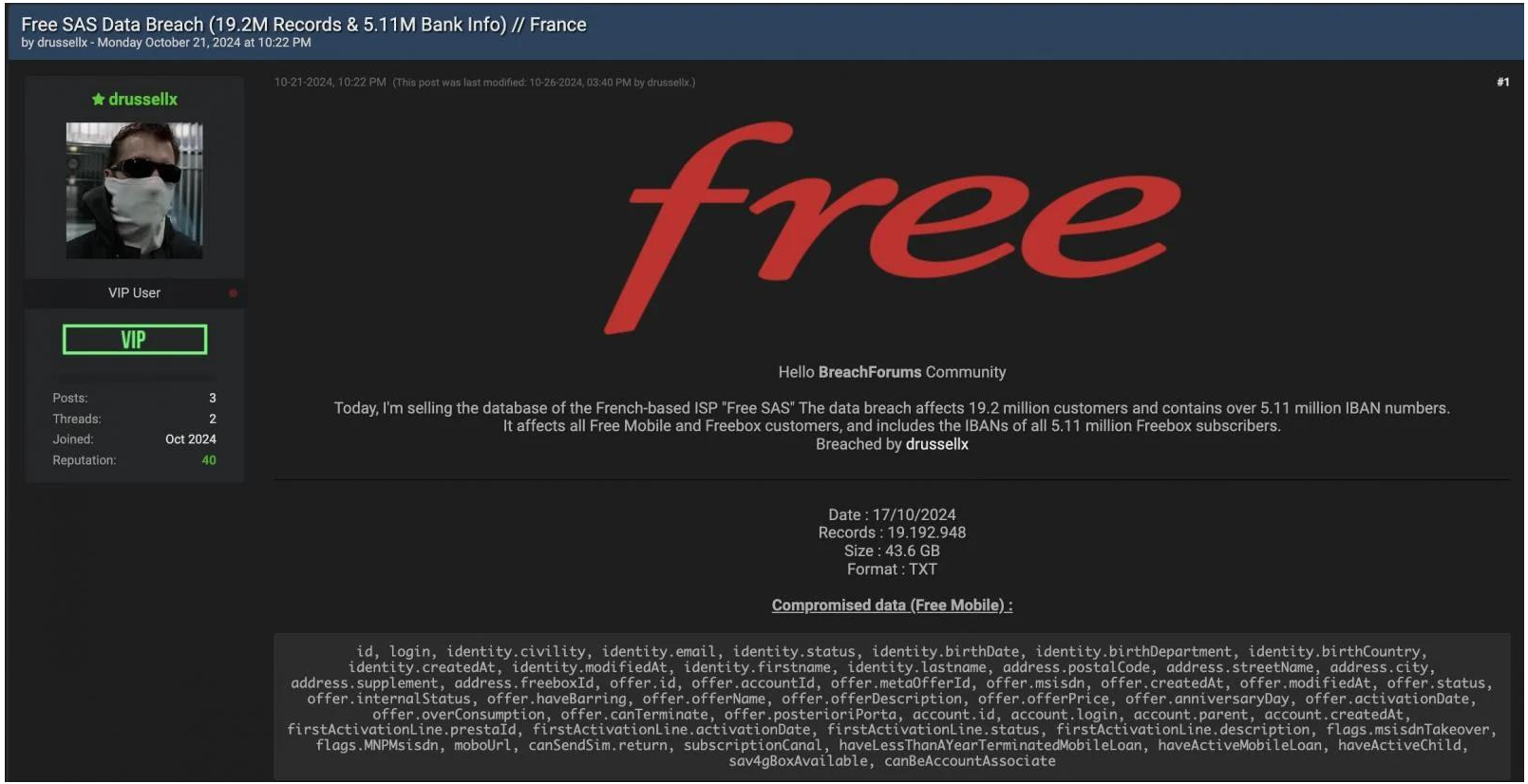
02 mai 2024 \ 17h35

3 min. de lecture

Réagir →

Source : l'Usine Digitale – 02/05/2024

Un niveau de gestion du risque très fluctuant



Free SAS Data Breach (19.2M Records & 5.11M Bank Info) // France
by drussellx - Monday October 21, 2024 at 10:22 PM

drussellx

VIP User

VIP

Posts:	3
Threads:	2
Joined:	Oct 2024
Reputation:	40

10-21-2024, 10:22 PM (This post was last modified: 10-26-2024, 03:40 PM by drussellx.) #1

Hello **BreachForums** Community

Today, I'm selling the database of the French-based ISP "Free SAS" The data breach affects 19.2 million customers and contains over 5.11 million IBAN numbers.
It affects all Free Mobile and Freebox customers, and includes the IBANs of all 5.11 million Freebox subscribers.
Breached by **drussellx**

Date : 17/10/2024
Records : 19.192.948
Size : 43.6 GB
Format : TXT

Compromised data (Free Mobile) :

```
id, login, identity.civility, identity.email, identity.status, identity.birthDate, identity.birthDepartment, identity.birthCountry,
identity.createdAt, identity.modifiedAt, identity.firstname, identity.lastname, address.postalCode, address.streetName, address.city,
address.supplement, address.freeboxId, offer.id, offer.accountId, offer.metaOfferId, offer.msisdn, offer.createdAt, offer.modifiedAt, offer.status,
offer.internalStatus, offer.haveBarring, offer.offerName, offer.offerDescription, offer.offerPrice, offer.anniversaryDay, offer.activationDate,
offer.overConsumption, offer.canTerminate, offer.posterioriPorta, account.id, account.login, account.parent, account.createdAt,
firstActivationLine.prestaId, firstActivationLine.activationDate, firstActivationLine.status, firstActivationLine.description, flags.msisdnTakeover,
flags.MNPMsisdn, moboUrl, canSendSim.return, subscriptionCanal, haveLessThanAYearTerminatedMobileLoan, haveActiveMobileLoan, haveActiveChild,
sav4gBoxAvailable, canBeAccountAssociate
```

Gestion du risque : un enjeu global pour les tous professionnels de l'IT

- **Experts en cybersécurité** : surveiller, anticiper et répondre aux menaces en temps réel
- **Développeurs** : éviter les vulnérabilités dans le code et intégrer la sécurité dès la conception
- **Administrateurs systèmes et réseaux** : protéger les infrastructures contre les attaques
- **Managers et décideurs IT** : arbitrer entre sécurité, coûts et performance

Risques et arbitrages dans l’allocation des ressources

Quels problèmes pose le Mur de Game of Thrones aux habitants de Westeros ?

« Le Mur » de Game of Thrones : un cauchemar en termes de gestion du risque

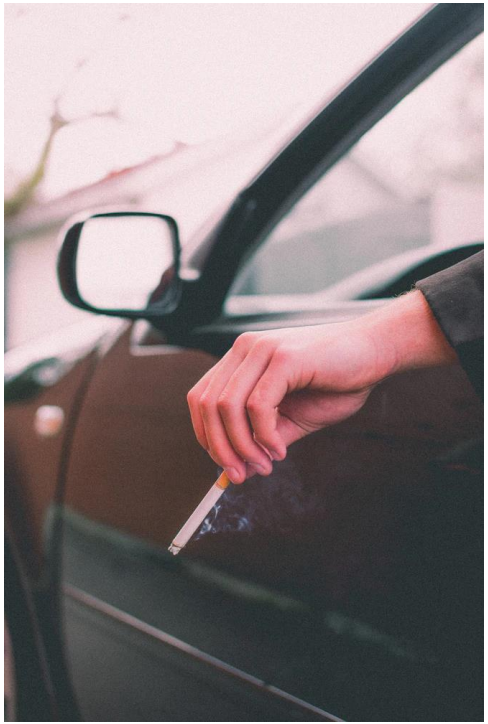
1. Énormes ressources mobilisées pour la construction et l'entretien du dispositif
2. Rend très difficile les interactions avec l'environnement
3. Conduit à sous-estimer le risque (« *icewall* » inviolable)
4. D'où manque chronique de ressources (« *si rien ne se produit, pourquoi investir ?* »)
5. Délégation du risque sur une minorité de spécialiste (« *Garde de Nuit* »)
6. Centralisation des forces adverses sur un point unique et immobile
7. Implique que les outsiders (« *sauvageons* » / « *peuples libres* ») soient catégorisés comme ennemis
8. Dispositif qui exacerbe des jeux politiques qui lui sont défavorables

Gestion du risque = problème complexe

- Choix des modalités de gestion du risque = interaction avec l'environnement
- Implique des arbitrages
  - Tension entre recherches d'interactions et de contrôle
  - Tension entre prévention et préservation de capacités dynamiques
  - Laisser certains accidents se produire
  - Laisser certaines menaces adverses se concrétiser
- **D'où recherche active de guidelines chez les professionnels**

EPITA

Difficultés à comprendre le concept [risque]

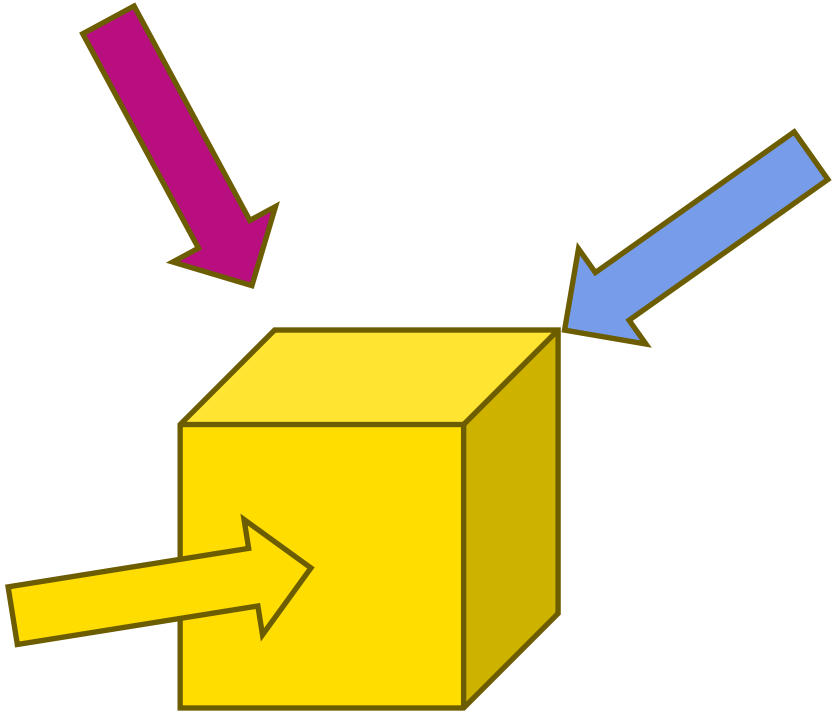


- Terme polysémique / rarement défini
- Degré de connaissance et de compréhension des probabilités
- Biais d'actualisation / difficulté à prendre en compte le long terme
- Incertitude sur les effets
- Évolution constante des systèmes humains
- ...

Qu'est-ce qui est plus risqué pour votre santé : fumer, manger des OGM , habiter en zone inondable ou travailler dans une centrale nucléaire ?

Difficulté à comprendre les organisations

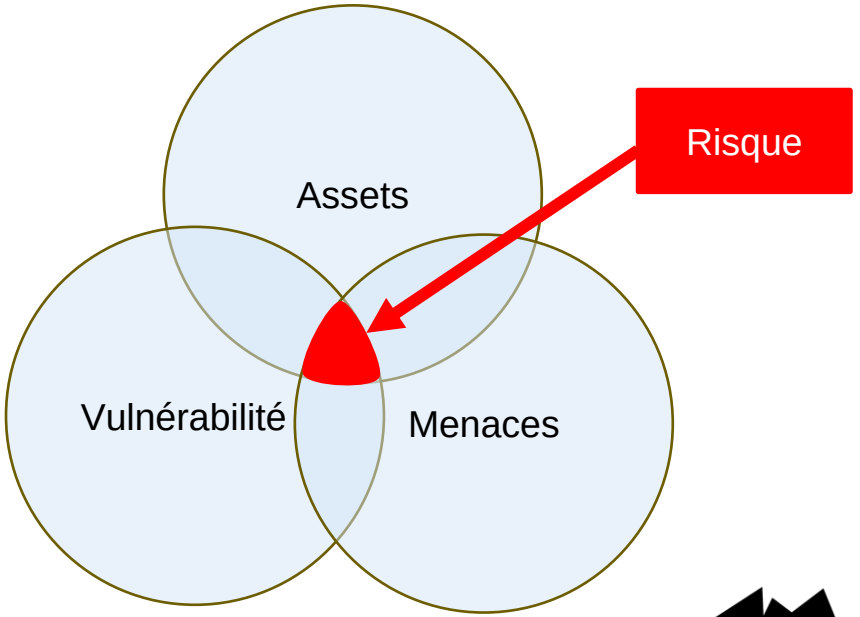
- Organisation : cadre permettant des interactions hyper-complexes entre :
  - Outils de production (dont IT)
  - Outils de gestion (dont IT)
  - Activité de production
  - Activité de coordination / de support
  - Hiérarchie et management
  - Liens sociaux formels / réseaux informels
  - Environnement
  - …
- Résultats :
  - Dynamique d'interaction avec l'environnement
  - Apprentissage
  - Emergences



Le discours sur le risque dépend de la perspective
(et toutes les perspectives ne se valent pas…)

Définir le risque (1/2) : une perspective cyber / IT

- **Assets :** tout ce qui a de la valeur pour une organisation
- **Vulnérabilités** : les faiblesses internes d'un système de production
- **Menaces :** tout ce qui peut nuire, endommager, compromettre un asset
- **Risque :** probabilité de la réalisation d'une menace

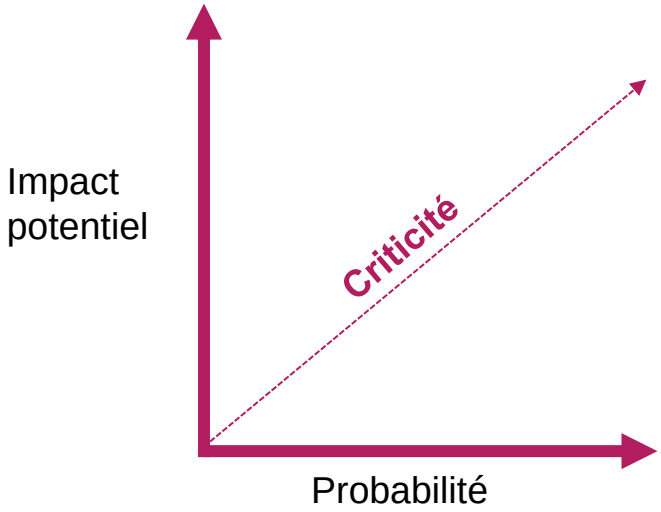


Définir le risque (2/2) : perspective managériale

- « *Séquence plus ou moins vraisemblables d'événements, de décisions, d'actions, non souhaitée, qui peut influencer l'atteinte d'un objectif du système. Un risque peut se manifester sous forme d'un accident, d'un incident.* »
  Deleuze et Ipperti, 2013, p. 20

- Deux grands axes de travail :
  1. Sécurité au travail
  2. Risques liés aux processus

- **Criticité du risque = impact x probabilité**



Concepts fondamentaux de la gestion du risque

Risque, incertitude, danger, dommage, arbitrage

EPITA

Définir le risque ?

Définition générique du risque

« ***Probabilité*** ***qu'un événement ou une situation ait des conséquences négatives pour l'atteinte d'un objectif donné*** »

Selon Kaplan &Garrick, 1981 (adaptation par nos soins)

Conséquences (1/2) : objectivation

- **Le risque dépend des objectifs**
  - Sécurité des données
  - Qualité logicielle
  - Conformité réglementaire / normative (RGPD, ISO 27001…)
  - Temps de déploiement
  - Rentabilité
  - …
- **Objectifs d'un système : arbitraires et contextuels**
  - Construction sociale
  - Varient dans le temps (*exemple : RGPD et protection des données*)

Conséquences (2/2) : incertitude

1. Le risque est une probabilité
   - « Risque 0 » → Ø
   - Évaluation statistique rétrospective
   - Statistique ≠ probabilité
   - Réalisation du risque incertaine
2. Compréhension des probabilités très fluctuante
   - Dépend de la capacité d'abstraction logique
   - Dépend du contexte (stress, charge de travail, pression temporelle…)

[Risque] : phénomène incertain et concept difficile à appréhender

EPITA

Quels sont, de votre point de vue, les facteurs d'incertitude dans les systèmes informatiques ?

Risque & incertitude

- **D'après ISO 31000 : risque = effet de l'incertitude sur l'atteinte des objectifs**
- Incertitude : manque d'informations ou d'outils permettant d'évaluer précisément ce qui pourrait se produire
- Sources d'incertitude
  - Technique / technologie
  - Humains
  - Organisations
  - Réglementations
  - Environnement
  - ...

Définir simplement le danger et les dommages

- **Danger :** « *source potentielle de dommages à laquelle une activité nous expose* »
- **Dommage :** « *conséquence concrète et négative / préjudice qui résulte de la réalisation du risque* »

Exemples de types de dommages liés à l'IT

- **Dommages matériels :** défaillance de serveurs, pannes de composants, dégradation d'équipements réseaux (switch, routeurs) entrainant l'interruption du service…
- **Dommages environnementaux :** surconsommation d'énergie, production de déchet électroniques…
- **Dommages sur les résultats :** corruption / perte de données, erreur de traitement ou de calcul, mauvaise interprétation des indicateurs…
- **Dommages économiques :** interruption de service conduisant à la perte de clients (panne, cyberattaque), amendes réglementaires…
- **Dommages réputationnels :** dégradation de l'image de l'entreprise…

EPITA

Rôle des référentiels normatifs

Normes et gestion du risque

EPITA

À quoi servent les référentiels en gestion de risque

Objectifs :

- Structurer les pratiques de gestion des risques
  - Créer un vocabulaire commun
  - Offrir un cadre pour identifier, analyser et atténuer les risques
- Alignements sur les **meilleures pratiques = [isomorphisme] (DiMaggio & Powell, 1983)**
  - Au sens large : **tendance des organisations appartenant à un même secteur d'activité à adopter des pratiques, des structures ou des comportements similaires** sous l'effet de pressions externes et internes.
  - **En particulier « isomorphisme coercitif » :** pressions formelles et informelles exercées par des entités influentes (État, régulateurs, grandes entreprises clientes) sur la conformité à certaines normes

EPITA

ISO 27005 : 2022 – Gestion des risques en cybersécurité

- **Objectif :** définir une méthodologie pour gérer les risques liés à la sécurité de l'information
- **Principaux concepts :**
  - Identification et évaluation des menaces et vulnérabilités
  - Définition des impacts et probabilité d'occurrence
  - Choix des stratégies de traitement du risque (accepter, atténuer, transférer, éviter)
- **Application :** utilisée par les RSSI et experts en cybersécurité pour structurer leur approche

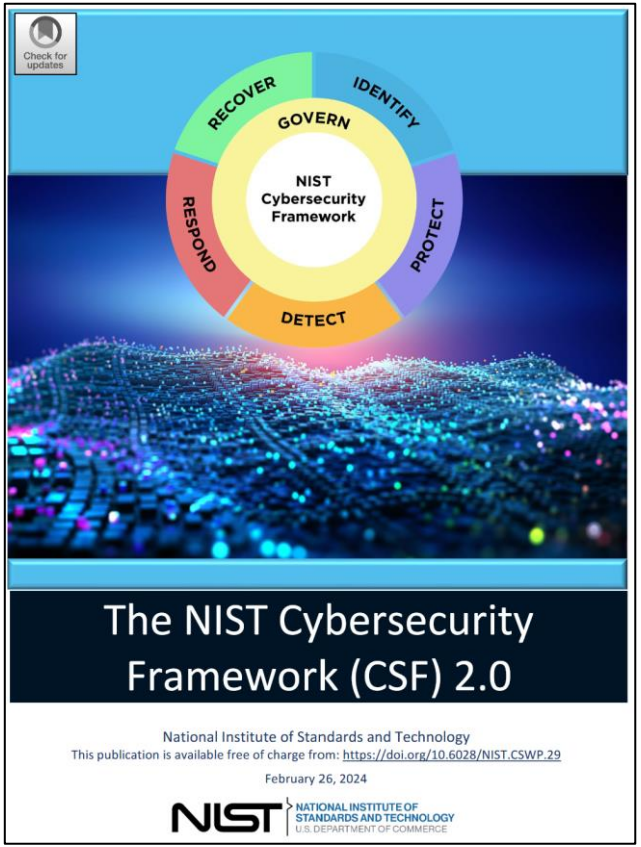
EPITA

NIST CSF 2.0 – Un cadre structurant pour la cybersécurité

Développé par National Institute of Standards and Technology (NIST, USA).

Cinq objectifs-clés :

- **Identifier** les assets et les risques
- **Protéger** : mettre en place des mesures préventives
- **Détecter** les activités suspectes
- **Répondre** rapidement aux incidents
- **Récupérer** : restaurer les services et améliorer la résilience



En pratique (1/3) : un rôle structurant

- **Référentiels : des outils structurants qui définissent…**
  - Des processus
  - Des catégories de risques
  - Des modalités de contrôles
  - Une architecture de gouvernance
- Outils régulièrement mis en avant par les praticiens…
  - Revendication de l'utilisation des référentiels (effet label)
  - Parfois certifications des organisations (ISO/IEC 27 001, ISO/IEC 27 701 sur la protection des données personnelles, ISO 27 018 pour la sécurité des services cloud ; etc.)
  - « **Support politique » pour susciter des investissements dans la gestion des risques**
- **Favorisent l'adoption des bonnes pratiques de base**

En pratique (2/3) : standardisation approximative

- **Forte variance dans la compréhension des référentiels et les pratiques**
  - **Entre les organisations d'un même secteur :** gage de sérieux ou vernis de respectabilité pour satisfaire à des approches contractuelles ?
  - **Au sein des organisations :** vision DG Vs. vision équipes IT
  - **Au sein des équipes IT :** priorisation des risques ?
- Uniformisation des pratiques
  - Créé des comportements similaires d'une organisation à l'autre : ajoute du risque systémique
  - *Quick wins* à l'implémentation…
  - …Mais valeur ajoutée limitée sur des enjeux émergents
  - *Exemple : appliquée seule ISO/IEC 27001 n'aide pas forcément à anticiper les attaques sur la supply chain logicielle*

EPITA

En pratique (3/3) : réduction de l'incertitude Vs. Résolution des arbitrages

- Utilité première des référentiels : réduire l'incertitude (évaluer les risques, mettre en place des contrôles, vérifier périodiquement l'efficacité…)
- Assurent des pratiques convenables
- Mais ne servent pas à trancher les besoins d'arbitrage
  - Définisse comment construire, entretenir et surveiller Le Mur
  - **N'adressent pas les bonnes questions : « Avons-nous besoin du Mur ? Quelles autres options avons-nous ? »**

[Risque] : un concept qui pose d'énormes difficultés pratiques

- Rappel définitions :
  - « *Probabilité qu'un événement ou une situation ait des conséquences négatives pour l'atteinte d'un objectif donné* »
  - « *Effet de l'incertitude sur les objectifs* »
- Prise en compte du [risque] suppose…
  1. Connaissance des statistiques (log d'exploitation)
  2. **Abstraction de probabilité à partir de statistiques (reconnaissance de patterns, impact de la modification de l'architecture IT…)**
  3. Anticipation des dommages potentiels

EPITA

Réponse des organisations : utilisation de référentiels

- Normes ISO / AFNOR / NIST CSF etc.
- Portent sur :
  - Architecture
  - Process
  - Compétences internes
- Limites
  - Qualité de la mise en œuvre
  - Dynamique organisationnelle
  - Ressources disponibles (temps, expertise, attention…)
  - Standardisation implique des risques en elle-même

À la fin de ce cours

- Vous maitriserez les grands concepts de la gestion du risque
- Vous connaitrez les référentiels de gestion du risque IT et leurs limites
- Vous serez capable de critiquer référentiels et pratiques
- Vous aurez mené une étude de terrain sur les pratiques réelles de gestion du risque

RDV en TD pour que nous en discutions