Gestion des risques en cybersécurité & ISO27005

Hervé Schauer

Herve.Schauer@hs2.fr

@Herve_Schauer @HS2formation

ISD INFORMATION SECURITY DAY 2019

HS2 Hervé Schauer Sécurité

ISDAYS 2019

hébergé par ICT Spring

Luxembourg, 20 mai 2019

Gestion des risques & ISO27005

- Qui suis-je ?
- Vocabulaire

- Gestion des risques
- Approche par les risques
- Quelle méthode ?
- ISO27005
- PIA/EIVP
- Ebios 2010
- Ebios 2018
- Autres (Fair, NIST, Méhari, etc)

- Conclusion

Qui suis-je ?

- Pas celui qui est responsable du contenu de l'ISO27005
- Un des très rares relecteurs/correcteurs/commentateurs de la traduction en français
  - Donc un peu comptable des traductions des versions françaises successives…
  - Ayant du avaler « Gestion des risques » → « Management des risques »…
- Consultant et formateur depuis 1989
  - 102 sessions de formation ISO27005 Risk Manager depuis octobre 2008
- Fondateur HS2

Vocabulaire

- « **Pour bien se comprendre, il faut utiliser le bon vocabulaire** » - Milan Kundera
- Sécurité et Sûreté vs *Security* et *Safety*
  - Connaissiez-vous Sauveté et *Surety* ?
  - Combien de langues ont plusieurs mots ?
- Déposer vs décommisionner, filtrer vs filtrer
- « cybersécurité / *cybersecurity* »
- « *Security control* » = « *safeguard* » = « *countermeasure* » = « Mesure de sécurité » = « protection » = « contre-mesure »
  - Cf ISO27000

Gestion des risques

- Quel que soit le domaine
  - cybersécurité, continuité d'activité, vie privée, etc
- 1) j'ai du **bon sens**, j'applique les **bonnes pratiques**
  - mais cybersécurité, continuité d'activité, vie privée, etc
- 2) ont besoin d'être **ajustées** aux **besoins** et au **contexte** de chaque organisme
- 3) → approche par les **risques**
  - Valable partout
  - SMSI (ISO27001), homologations (RGS, LPM, etc), SMCA (ISO22301), RGPD, PCI-DSS, etc
    - tous basés par une approche par les risques
    - et autres domaines : ISO9001, etc

Approche par les risques

- 1) Application des mesures de sécurité de base
  - Là où leur application semble évidente
- 2) Appréciation des risques
  - Recherche des trous dans la raquette
  - Mise en oeuvre des mesure de sécurité que là où elles sont le plus utile
- → **Optimisation financière**
- → Engagement de la personne responsable
  - parfaitement informée des enjeux et des conséquences
- Qui est la personne responsable ?
  - appelée propriétaire du risque dans les normes
- → **Autorité d'arbitrage budgétaire**

Quelle méthode en gestion des risques ?

- ISO 27005
- PIA ou EIVP
- Ebios 2010
- Ebios 2018 dit "Ebios Risk Manager"
- Nombreux autres référentiels de gestion de risques

ISO 27005

- Méthodologie d'appréciation des risques
  - reconnue internationalement,
  - conforme à la démarche ISO31000 appliquée à la cybersécurité
  - visant une gestion des risques dans le temps, dans la durée
  - préconisée pour toute appréciation des risques dans le cadre d'un SMSI
  - utilisable pour l'appréciation des risques imposée dans SMCA
    - en plus du BIA également imposé
  - s'appliquant sur un système existant
  - déclinant les objectifs de la direction
  - imposant l'engagement du propriétaire du risque
    - celui ayant le pouvoir d'arbitrage budgétaire
  - s'attachant aux conséquences qui touchent son organisme

ISO 27005

- ISO27005 nous dit "je suis une **approche systématique**"
- C'est-à-dire, cf *Business Dictionary* :
  - Approche méthodique,
  - Répétable
  - Apprenable par une procédure pas à pas
- ISO27005 est une **méthode**

ISO 27005

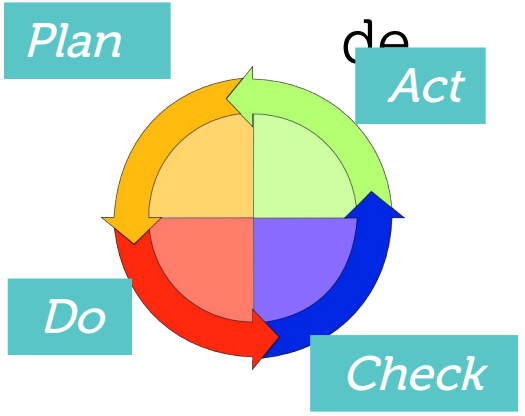
- ISO27005 a 10 ans, son innovation demeure
- C'est quoi la différence avec les méthodes antérieures ?
  - Appréciation des risques une fois pour toutes, à un instant t, « *one shot* »
  - vs
  - Appréciation de risque dans la **durée**
- Dans la durée, c'est beaucoup plus dur !
  - Faire travailler un consultant un mois c'est plus facile

ISO 27005

- Conséquences d'un risque toujours **temporelles**
  - Importance des actifs impactés pour l'organisme, le métier, le projet → temporel
  - Besoin du propriétaire de l'actif → temporel
  - Probabilité d'occurence de la menace → temporel
  - Facilité/difficulté d'exploitation des vulbérabilités → temporel
- Temporalités
  - Toutes **différentes**
  - Toutes **décorellées** les unes des autres
- Quels logiciels de gestion des risques en cybersécurité permettent une appréciation des risques ?
  - Pas une simple conformité à des mesures de sécurité
- Quels logiciels de gestion des risques en cybersécurité intègrent la gestion du temps ?

ISO 27005

- Approche de haut vers le bas
  - Application des orientations choisies par la direction
- Instanciation du PDCA dans le processus de gestion des risques



- Explicite l'ISO27001
  - Appréciation du risque : 6.1.2 & 8.2
  - Traitement du risque : 6.1.3 & 8.3
- Gestion des risques cohérentes avec l'organisation d'entreprise
  - Alignement sur le management des risques en général
  - Pilotage du management des risques en sécurité de l'information par le RSSI

PIA / EIVP

- PIA (*Privacy Impact Assesment*) ou Etude d'Impact sur la vie Privée (EIVP)
- Méthodologie d'étude d'impact
  - reprenant les même concepts qu'ISO27005
  - ayant une approche pragmatique
  - en France généralement inspirée par les guides Cnil
    - eux-mêmes inspirés d'Ebios 2010
  - de plus en plus inspirée de l'ISO29134
  - préconisée pour répondre à l'exigence du RGPD
  - nécessaire pour prouver sa conformité (*accountability*)
  - s'attachant aux conséquences affectant les personnes dont l'organisme détient les données

Ebios 2010

- Méthodologie d'appréciation des risques éditée par l'ANSSI-Fr
  - pas liée aux normes
  - à un instant « t »
  - préconisée pour toute appréciation des risques en lien avec les référentiels de l'administration française (RGS, SIIV (OIV), PIA)
  - préconisée pour toute appréciation des risques orientée projet
  - permettant d'étudier les risques d'un système à construire
  - permettant d'écrire un cahier des charges
  - s'attachant aux conséquences qui touchent
    - soit son organisme
    - soit l'état

Ebios 2018 dite « Ebios Risk Manager »

- Nouvelle méthodologie d'appréciation des risques éditée par l'ANSSI-Fr
  - n'étant pas une nouvelle version d'Ebios 2010 mais une nouvelle méthode qui utilise le même nom afin d'entretenir la confusion
  - prévue pour fonctionner dans la durée
  - prenant en compte que les menaces d'origine malveillantes
  - nécessitant des bases de connaissances (non-fournies)
  - se focalisant sur un panel réduit de risques
  - reprenant le niveau de détail qu'offrait Ebios v2
  - mettant l'accent sur les risques liés aux parties prenantes et à l'externalisation
  - avec beaucoup de réunions successives et itératives
  - Référentiel était sous embargo jusqu'à sa publication en octobre 2018
    - pas encore de retour d'expérience, même quand annoncés (FIC2019)
    - retours à chaud parfois perplexes des experts et formateurs

Référentiels de gestion de risques

- Les plus courants :
  - ISO 31000 Management du risque
    https://www.iso.org/fr/standard/65694.html
  - ISO 27005 Management du risque pour la sécurité de l'information
    https://www.iso.org/fr/standard/75281.html
  - ISO 29134 Evaluation d'impacts sur la vie privée
    https://www.iso.org/fr/standard/62289.html
  - Ebios 2010
    https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/
  - Ebios 2018 dite « Ebios Risk Manager »
    https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide/
  - Fair *Factor Analysis of Information*
    https://publications.opengroup.org/c13g

Référentiels de gestion de risques

- Les plus courants :
  - NIST SP-800-30 Risk Assesment Framework
    https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf
  - NIST SP800-37 Guide for applying the Risk Management Framework to Federal Information Systems
    https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf
  - NIST SP800-39 Managing Information Security Risk
    https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf
  - NIST SP800-53 Security and Privacy Control for Federal Information Systems and Organisations
    https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Référentiels de gestion de risques

- Les plus courants :
  - Octave
    https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8419
  - IRAM2
    https://www.securityforum.org/tool/information-risk-assessment-methodology-ira+m2/
  - Mehari https://clusif.fr/mehari/
  - BSI IT-Grundschutz
    https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzDownloads/itgrundschutzDownloads_node.html
  - Risk-IT (ISACA)
    https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx
  - BSI-Standard 200-3
    https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard203/ITGStandard203_node.html

Référentiels de gestion de risques

- Concepts communs et universels
  - Cf Guide ISO73 et ISO31000
- Inspirations mutuelles au fil des évolutions
  - Notion de scénario
- Toujours des particularités

Référentiels de gestion de risques

- Popularité au 31/12/2018 sur la base du nombre de participants aux formations
  - ISO27005 : 10 ans : 1187
  - PIA/EIVP : 1 an 1/2 : 18
  - EBIOS2010 : 5 ans : 78
  - EBIOS2018 : 0 ans : 0
- Peu de retours d'expérience publics de gestion des risques
  - Ou juste partie des retours d'expérience ISO27001

Référentiels de gestion de risques

- Complémentarité
  - Conséquences
    - pour soi (l'organisme pour lequel on travaille)
    - pour les personnes dont on possède les données
    - pour l'état/la société
  - Base de connaissance des scénarios de Méhari
  - Estimation des risques quantitative de FAIR
  - Promotion de l'approche par les risques d'EBIOS 2018

Conclusion

- A chacun de sélectionner la méthode qui répond à son contexte
- Dans le cas d'un organisme, un métier, un SMSI, un SMCA : ISO27005
- **Questions ?**
  - Herve.Schauer@hs2.fr
  - @Herve_Schauer
  - **www.hs2.fr**
  - **@HS2formation**
  - Stand D7