Méthodologies d'évaluation et gestion de risques en sécurité

Franck Jeannot

Montréal, Canada, Mai 2018, R518, v1.0

Abstract

A review of some security risk management methodologies and tools references. Risk assessement and risk management methodologies are combined due to their interrelations.

Keywords: COBIT, FAIR, ISO/IEC, InfoSec, MEHARI, méthodes, M_o_R, PUSH, NIST, OCTAVE, ontologie, security risk assessment, risk management, SOBF SOMAP, tools

1 Introduction

2 Contexte et historique

Les éléments comme le *Turnbull report* (1999, USA) [1], le Gramm–Leach–Bliley Act (GLBA) (1999, USA) le **Sarbanes-Oxley Act** (2002, USA) [2], les accords **Basel II, international** (2004) [3], le **FISMA** (Federal Information Security Modernization Act) (2014, USA) ont tous [4] [5] mis une emphase sur le requis de mettre en place et **conduire des analyses de risques de sécurité**.
Aussi, les évolutions en **cybersécurité** [6] requièrent des mises à jour des **lois** afin de mettre en place des stratégies d'adaptation des ressources gouvernementales travaillant en cybersécurité, comme le ***Cybersecurity workforce assessment act (2014)*** aux États-Unis [7] ou le *Executive Order 13800* (Mai 2017, USA). [1]

1. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/executive-order-13800

3 Taxonomie du risque

Il s'agit d'aborder une taxonomie [2] des **facteurs de risque**, de leurs **définitions** et **relations**. On définit le **risque** comme :

- « *la fréquence probable et l'ampleur probable de la perte future* » [3] selon l' *OpenGroup* [4],
- « *l'effet de l'incertitude sur l'atteinte des objectifs* », selon l'ISO Guide 73 :2009 [5]
- « *Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization* » selon le NIST SP 800-30.
- « *The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.* » selon le NIST FIPS 200.
- « un évènement non souhaité qui peut ou pas arriver » « *. . . an unwanted event which may or may not occur* » selon la *Stanford Encyclopedia of Philosophy Archive* [6]

On définit le **management du risque** comme : « *activités coordonnées dans le but de diriger et piloter un organisme vis-a-vis du risque* » (d'après ISO Guide 73 :2009)

4 Ontologies, méthodes et outils de gestions de risques

Il existe de très nombreuses méthodologies et outils de gestion de risques [9] et les chercheurs et organisations diverses sont en constante recherche d'**optimisations**, **généralisations** ou **spécialisations** de ces méthodes *créant ainsi de* ***nouvelles*** *méthodes ou* ***hybrides*** *de manière fréquente.*

2. https://resources.sei.cmu.edu/asset_files/TechnicalReport/1993_005_001_16166.pdf
3. Trad. libre de *"Risk is the probable frequency and probable magnitude of future loss"* selon l'Open Group ; ref page 11 de [8]
4. https://en.wikipedia.org/wiki/The_Open_Group
5. https://www.iso.org/standard/44651.html
6. https://plato.stanford.edu/archives/spr2014/entries/risk/

4.1 Ontologies

FAIR[7][8] ***Factor analysis of information risk*** est une méthode [10] de mesure et de représentation de risques de sécurité ou plus précisément une ontologie[9][10] (au sens technique). Selon *Jack A. Jones*, US patent 2005/0066195A :

> *Method of measuring and representing security risk. The method comprises selecting at least one object within an environment and quantifying the strength of controls of at least one object within that environment(...).*

4.2 Méthodes

Il est abordé ici quelques méthodes de gestion de risques (quelques exemples connus sans pour autant être une liste exhaustive). On retrouve des méthodes d'organisations nationales, internationales, consortiums, universités, gouvernements ...

4.2.1 API-NPRA

Méthodologie **API-NPRA** [13]

4.2.2 AS/NZS 4360

Méthodologie **AS/NZS 4360**

4.2.3 CJA

Méthodologie **CJA**[11][12] du **MITRE**

4.2.4 CORA

Méthodologie **CORA**[13][14] ***C****yber* ***O****perations* ***R****apid* ***A****ssessment* du **MITRE**

---

7. https://en.wikipedia.org/wiki/Factor_analysis_of_information_risk
8. https://www.fairinstitute.org/
9. Voir chap. 3 p 25 de [11]
10. On définira l'***ontologie*** tel qu'un « *ensemble structuré des termes et concepts représentant le sens d'un champ d'informations, que ce soit par les méta-données d'un espace de noms, ou les éléments d'un domaine de connaissances* » [12]
11. https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis
12. https://www.mitre.org/sites/default/files/pdf/crown-jewels-analysis.pdf
13. http://heim.ifi.uio.no/~ketils/kst/Articles/2011.FOSAD.pdf
14. https://www.mitre.org/sites/default/files/publications/pr_15-2971-cyber-operations-rapid-assessment-best-practices_0.pdf

4.2.5 COSO

Méthodologie **COSO Enterprise Risk Management** framework (*COSO ERM*)

4.2.6 COBIT

Méthodologie **COBIT** (Control Objectives for Information and Related Technology) de l'**ISACA**.

4.2.7 CRAMM

Méthodologie **CRAMM** [15] [16] (CCTA Risk Analysis and Management Method) (*Central Computer and Telecommunications Agency*) (1987)

4.2.8 EBIOS

Méthodologie **EBIOS** [17] (ANSSI, ENISA)

4.2.9 FMEA

Méthodologie *Failure Modes and Effect Analysis* (**FMEA**)

4.2.10 FRAP

Méthodologie *Facilitated Risk Analysis Process* (**FRAP**) [18] [19]

4.2.11 ISAMM

Méthodologie **ISAMM** [20] Information Security Assessment & Monitoring Method de l'**ENISA**

4.2.12 IT-Grundschutz

Méthodologie IT-Grundschutz [21]

4.2.13 ITIL

Méthodologie **ITIL** [22]

---

15. https://en.wikipedia.org/wiki/CRAMM
16. https://managementmania.com/en/cramm-ccta-risk-analysis-and-management-method
17. https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite
18. https://en.wikipedia.org/wiki/Risk_analysis_(business)
19. http://ittoday.info/AIMS/DSM/85-01-21.pdf
20. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_isamm.html
21. https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html
22. https://en.wikipedia.org/wiki/ITIL_security_management

4.2.14 ITSG-33

Méthodologie **ITSG-33** [14] (**Canada**), *La gestion des risques liés à la sécurité des TI : une méthode axée sur le cycle de vie* (2012)

4.2.15 MEHARI

Méthodologie **MEHARI** (version 2010) du CLUSIF ou **ME**thode **H**armonisée d'**A**nalyse du **R**isque Informatique [23]

4.2.16 M_o_R

Méthodologie **M_o_R** [24] : a une orientation ***pratique*** de ce qui doit être fait et comment le faire (par opposition par exemple a un standard comme ISO 31000 qui définit ce qui doit être fait et par qui). Selon l'article *Management of Risk : Guidance for Practitioners and the international standard on risk management, ISO 31000 :2009* de *Michael Dallas* [25] :

> *M_o_R describes both what needs to be done, through a set of principles, activities and roles, and how to undertake the activities*

4.2.17 Misuse or Abuse cases

Méthodes des ***Misuse or Abuse cases*** [15] [16] [17]. C'est une méthodologie née dans les années 1990 qui se base sur les cas d'usage UML avec un focus sur les cas qui ne devraient pas arriver.

4.2.18 OECD RAT

Méthode OECD Risk Awareness Tool [26]

4.2.19 OCTAVE

Méthodologie **OCTAVE** (Operationally Critical Threat, Asset and Vulnerability Evaluation) ou *OCTAVE Allegro*, initialement du CERT (cert.org), devenu SEI de *Carnegie Mellon University* [18] [19]

---

23. http://meharipedia.x10host.com/wp/wp-content/uploads/2016/12/MEHARI-2010-Processing-Guide.pdf
24. http://www.vanharen.net/Samplefiles/9789087532116_risk-management-based-on-m_o_r-a-management-guide.pdf
25. page 3 de http://www.educore.com.tr/wp-content/uploads/2014/08/Management_of_Risk_Guidance_for_Practitioners_and_the_International_Standard_on_Risk_Management_ISO31000_2009.pdf
26. https://www.oecd.org/daf/inv/corporateresponsibility/36885821.pdf

4.2.20 ORIMOR

Méthodologie Open Risk Model Repository (ORIMOR) [27]. Voir **SOMAP**.

4.2.21 OSSTM

Méthodologie OSSTM (Open Source Security Testing Methodology) de l'ISECOM

4.2.22 PUSH

Méthodologie **PUSH** (FIPCO) [28] [29]

4.2.23 RAPSA

Méthodologie **RAPSA** [20] [21] [22] de l'*University of Idaho*

4.2.24 Risk IT

Méthodologie **Risk IT** [30] de l'**ISACA**

4.2.25 RiskMAP

Méthodologie **RiskMAP** [31] du **MITRE**

4.2.26 SABSA

Méthodologie **SABSA** (**S**herwood **A**pplied **B**usiness **S**ecurity **A**rchitecture). On peut décrire cette méthodologie comme une application du ***Cadre d'architecture Zachman*** [23] au domaine de la gestion de risques.

4.2.27 Secure Tropos

Secure Tropos (2011) [24] [25] est issu des principes de plusieurs projets et méthodologies en lien à la gestion d'objectifs (*goal modeling*) :

- **Tropos** [26]
- **ISSRM** [27] *Information System Security Risk management*
- **GORE** [28] *Goal-Oriented Requirements Engineering* [32]

Selon le Tropos Project [33], Secure Tropos est une extension de Tropos pour modéliser et analyser les requis de sécurité avec les requis fonctionnels :

27. https://www.somap.org/orimor/
28. https://www.fipco.com/Portals/0/products/IT/itconfpresentation.pdf
29. https://www.fipco.com/Web/Services/ITAuditSecurity/ITRiskAssessment.aspx
30. https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx
31. https://www.mitre.org/sites/default/files/pdf/09_2994.pdf
32. https://en.wikipedia.org/wiki/Goal_modeling
33. http://www.troposproject.eu/node/301

Secure Tropos extends Tropos in order to model and analyze security requirements alongside functional requirements. The methodology provides a requirements analysis process that drives system designers from the acquisition of requirements up to their verification. Two versions of Secure Tropos exist.

Un exemple d'outil de modélisation par objectifs est *OpenOME*[34] [35]

4.2.28 SOMAP

Security Officers Management & Analysis Project - **SOMAP**[36] est un projet et portail regroupant des outils, framework et méthodologies dont notamment :

- *The **OGRCM3** project develops and documents a methodology on how to measure and manage risk.*
- *The **ORIMOR** contains a database model which is used as the basis for our own risk management framework and tool.*
- *The **ORICO** Framework and Tool are the (reference) implementation of our own maturity management methodology.*

Un des outils implémenté par le projet SOMAP est *Security Officers Best Friend* (**SOBF**)[37] :

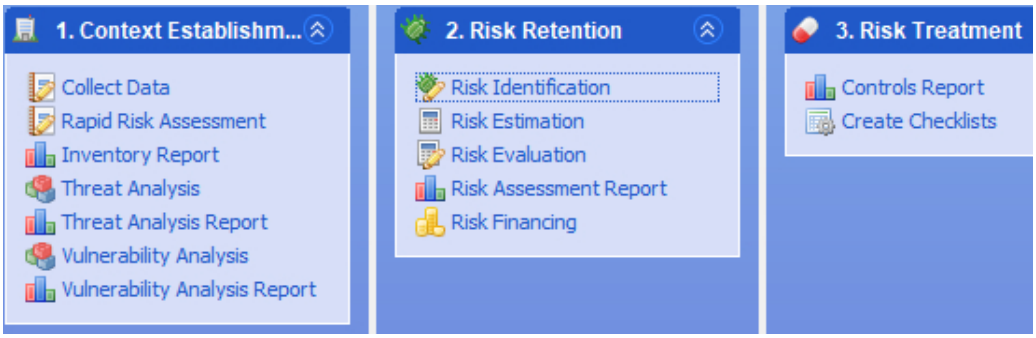

FIGURE *(1): Interface java de SOBF 1.0b1 - projet SOMAP*

34. https://se.cs.toronto.edu/trac/ome
35. ref. GR-Tool dans http://disi.unitn.it/~pgiorgio/papers/CRITIS06.pdf
36. https://www.somap.org
37. https://sourceforge.net/projects/somap/files/SOBF%20Tool/

4.2.29 STS

Méthodologie de type *sytèmes socio-techniques Socio-Technical Systems* (**STS**) [29] [30] [31]. Un exemple est le framework **STEAL** [38] (Socio TEchnical Attack AnaLysis)

4.2.30 TARA

Méthodologie TARA [32] du **MITRE**.

4.2.31 TOGAF-ADM Risk management

Méthodologie **TOGAF ADM** [39] (partie *Risk Management* du TOGAF qui reste avant tout une méthodolgie d'Architecture d'Entreprise)

4.2.32 VAR

Méthodologie *Value at risk* **VAR** : plus une mesure de risques financiers (*avec des critiques à prendre en considération*) [40]

4.2.33 WEA

Méthodologie **WEA** [33], est une méthodologie de risque **orientée alertes** selon le *Wireless Emergency Alerts Cybersecurity Risk Management Strategy for Alert Originators*, Carnegie Mellon

4.3 Standards

- **BS 31100** (BS 31100) *Code of Practice for **Risk Management** and Guidance for ISO 31000*
- ISO/IEC 13335 IT Security techniques – Management of information and communications technology security
- ISO/IEC *15026-1 Systems and software engineering – Systems and software assurance*
- ISO/IEC/IEEE 15288 *Systems and software engineering - System life cycle processes*
- ISO/IEC 17799 *Security techniques - Code of practice for information security management*
- **ISO/IEC 27000** (27002, 27005), *Security techniques — Information security management systems*

38. http://citeseerx.ist.psu.edu/viewdoc/download\?doi=10.1.1.864.2220&rep=rep1&type=pdf
39. https://pdfs.semanticscholar.org/45ba/cad97216e2643c0ee54c16d6e03bccf92336.pdf
40. https://en.wikipedia.org/wiki/Value_at_risk

— ISO/IEC 28000 *Specification for security management systems for the supply chain*
— **ISO/IEC 31000** Famille de standards en lien à la **gestion de risques**
— **NIST 800-30** *Guide for Conducting* ***Risk Assessments*** [34]
— **NIST 800-37** *Guide for Applying the Risk Management Framework to Federal Information Systems*
— **NIST 800-39** *Managing Risk from Information Systems* [41]

4.4 Techniques d'évaluation de risque

Le standard ISO/IEC **31010** définit pas moins de 31 techniques d'évaluation de risque dont notamment **Delphi**, Failure mode and effects analysis (**FMEA**), **SWIFT**.

4.5 Outils génériques

Le registre de risque "***Risk Register***" et le tableau "***Risk heat map***" [42] sont des exemples d' outils génériques standards.

41. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf
42. exemple p 17/26 de https://www.rims.org/Session%20Handouts/RIMS%2016/ERM001/ERM001_2016_RIMS_Presentation_04112016%20Mon.pdf

Références

[1] THE COMBINED CODE ON CORPORATE GOVERNANCE - Turnbull, http://webarchive.loc.gov/all/20050708100512/http://www.fsa.gov.uk/pubs/ukla/lr_comcode2003.pdf.

[2] Sarbanes–Oxley Act, https://en.wikipedia.org/wiki/sarbanes%e2%80%93oxley_act.

[3] Basel II, https://en.wikipedia.org/wiki/basel_ii.

[4] S. Dashti, P. Giorgini, E. Paja, Information Security Risk Management, in : G. Poels, F. Gailly, E. S. Asensio, M. Snoeck (Eds.), 10th IFIP Working Conference on The Practice of Enterprise Modeling (PoEM), Vol. LNBIP-305 of The Practice of Enterprise Modeling, Springer International Publishing, Leuven, Belgium, 2017, pp. 18–33, part 1 : Regular Papers. doi:10.1007/978-3-319-70241-4_2.
URL https://hal.inria.fr/hal-01765266

[5] Operational risk and information security need to co-exist for effective risk management.
URL https://www.continuitycentral.com/feature0189.htm

[6] Brookson et al, Definition of cybersecurity - gaps and overlaps in standardisation.
URL https://www.enisa.europa.eu/publications/definition-of-cybersecurity/at_download/fullReport

[7] United States Congress, Cybersecurity workforce assessment act.
URL https://www.gpo.gov/fdsys/pkg/PLAW-113publ246/pdf/PLAW-113publ246.pdf

[8] The Open Group, Technical standard risk taxonomy.
URL http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf

[9] M. Ghazouani, H. Medromi, A. Sayouti, S. Faris, Information security risk assessment — a practical approach with a mathematical formulation of risk 103 (8).
URL https://www.researchgate.net/publication/292139978_Information_Security_Risk_Assessment_-_A_Practical_Approach_with_a_Mathematical_Formulation_of_Risk

[10] J. A. Jones, Factor analysis of information risk us 2005/0066195a1, uS Patent 2005/0066195A1 (03 2005).
URL https://patentimages.storage.googleapis.com/7a/29/d9/2be12895f14c3c/US20050066195A1.pdf

[11] J. Freund, J. Jones, Measuring and Managing Information Risk: A FAIR Approach, Elsevier Science, 2014.
URL https://books.google.ca/books?id=oAROAwAAQBAJ

[12] Ontologie (informatique), https://fr.wikipedia.org/wiki/Ontologie_(informatique).

[13] American Petroleum Institute, Security vulnerability assessment methodology for the petroleum and petrochemical industries.
URL https://www.nrc.gov/docs/ML0502/ML050260624.pdf

[14] Centre de la sécurité des télécommunications Canada, La gestion des risques liés à la sécurité des ti : une méthode axée sur le cycle de vie.
URL https://www.cse-cst.gc.ca/fr/system/files/pdf_documents/itsg33-overview-apercu-fra_1.pdf

[15] G. Sindre, A. L. Opdahl, Capturing security requirements through misuse cases, 2001.
URL http://hjem.ifi.uio.no/nik/2001/21-sindre.pdf

[16] Wikipedia, Misuse case.
URL https://en.wikipedia.org/wiki/Misuse_case

[17] Guttorm Sindre and Andreas L. Opdahl, Eliciting security requirements with misuse cases, Requirements Engineering 10 (1) (2005) 34–44. doi:10.1007/s00766-004-0194-4.
URL https://resources.sei.cmu.edu/asset_files/SpecialReport/2014_003_001_87729.pdf

[18] R. Caralli, J. Stevens, L. Young, W. Wilson, Introducing octave allegro: Improving the information security risk assessment process, Tech. Rep. CMU/SEI-2007-TR-012, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA (2007).
URL https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

[19] Ian Dobson and Jim Hietala, Risk management - the open group guide, The Open Group.
URL https://pdfs.semanticscholar.org/5292/0882f44cc85df656f7de81cc661a436a7ee8.pdf

[20] Carol Taylor, Axel Krings and Jim Alves-Foss, Risk analysis and probabilistic survivability assessment (rapsa): An assessment approach for power substation hardening.
URL https://www.researchgate.net/publication/228861020_Risk_analysis_and_probabilistic_survivability_assessment_RAPSA_An_assessment_approach_for_power_substation_hardening

[21] S. Ali, T. Balushi, Z. Nadir, O. Hussain, Cyber Security for Cyber Physical Systems, Studies in Computational Intelligence, Springer International Publishing, 2018.
URL https://books.google.ca/books?id=991PDwAAQBAJ

[22] S. Furnell, P. Dowland, B. Thuraisingham, X. Wang, Security Management, Integrity, and Internal Control in Information Systems: IFIP TC-11 WG 11.1 & WG 11.5 Joint Working Conference, IFIP Advances in Information and Communication Technology, Springer US, 2006.
URL https://books.google.ca/books?id=W_jZBwAAQBAJ

[23] Franck Jeannot, Le cadre d'architecture d'entreprise zachman.
URL https://www.franckjeannot.com/wp-content/uploads/zachman.pdf

[24] H. Mouratidis, Secure software systems engineering: The secure tropos approach 6.
URL https://pdfs.semanticscholar.org/5292/0882f44cc85df656f7de81cc661a436a7ee8.pdf

[25] Naved Ahmed and Raimundas Matulevicius and Haralambos Mouratidis, A model transformation from misuse cases to secure tropos, in : Proceedings of the CAiSE'12 Forum at the 24th International Conference on Advanced Information Systems Engineering (CAiSE), Gdansk, Poland, June 28, 2012, 2012, pp. 7–14.
URL http://ceur-ws.org/Vol-855/paper1.pdf

[26] J. B. de Castro, M. Kolp, J. Mylopoulos, Towards requirements-driven information systems engineering: the tropos project, Inf. Syst. 27 (2002) 365–389.
URL http://www.cs.toronto.edu/~jm/Pub/InfoSystems02.pdf

[27] Nicolas Mayer, Model-based management of information system security risk.
URL https://tel.archives-ouvertes.fr/tel-00402996/document

[28] Alexei Lapouchnian , Goal-oriented requirements engineering:an overview of the current research.
URL https://www.cs.utoronto.ca/~alexei/pub/Lapouchnian-Depth.pdf

[29] A. Ferreira and R. Giustolisi and J. L. Huynen and V. Koenig and G. Lenzini, Studies in socio-technical security analysis: Authentication of identities with tls certificates, in : 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013, pp. 1553–1558. doi:10.1109/TrustCom.2013.190.
URL https://pdfs.semanticscholar.org/2478/19c8e316618ecae4989ab451c934ba835de5.pdf

[30] E. Paja, Security requirements engineering:designing secure socio-technical systems.
URL http://www.pacasproject.eu/wp-content/uploads/2016/10/PACAS_Security-Requirements-Engineering_presentation.pdf

[31] P. G. Salimeh Dashti, E. Paja, Information risk management:an example of healthcare domain.
URL http://disi.unitn.it/~pgiorgio/IRM-HealthCareCase.pdf

[32] Jackson Wynn et al., Threat assessment and remediation analysis (tara).
URL https://www.mitre.org/sites/default/files/pdf/11_4982.pdf

[33] WEA Project Team, Wireless Emergency Alerts (WEA) Cybersecurity Risk Management Strategy for Alert Originators, SPECIAL REPORT CMU/SEI-2013-SR-018.
URL https://resources.sei.cmu.edu/asset_files/SpecialReport/2014_003_001_87729.pdf

[34] NIST, Guide for Conducting Risk Assessments.
URL https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf