Survey and Guidelines about Learning Cyber Security Risk Assessment

Christophe Ponsard and Philippe Massonet
CETIC Research Centre, Charleroi, Belgium

Keywords: Cyber Security, Risk Analysis, Education, Standard, Controlled Experiment.

Abstract: Risk assessment is a key part of all cyber security frameworks, standards and related certification schemes. It is a complex process involving both the business domain to assess impact and the technical domain to measure feasibility. It requires to produce a realistic risk matrix based on qualitative information and then to decide about measures aligned with relevant standards. Getting experienced in this area is a difficult learning process with many possible pitfalls. In this paper, we report about our lessons learned based on a controlled experiment of 26 risk analyses across different domains including some operators of essential services. We also provide some methodological recommendations for efficient tool support, including model-based.

1 INTRODUCTION

Nowadays, the ubiquity and tremendous capabilities of connected computer-based systems enable a large range of features and services, but also increase their exposure to cyber security threats. The latest threat reports confirm the importance of malware, web-based attacks and phishing but also their evolution towards more pervasive and targeted forms of attacks (ENISA, 2020). While the information technology (IT) sector has already developed dedicated frameworks such as the NIST Cyber Security Framework (NIST, 2014) and standards such as ISO 27000 series (ISO, 2013), other domains are now increasingly proposing a specific response to integrate cyber security in their core development and operation processes. Examples of dedicated standards are the ISO 63422 for industrial systems (including Operation Technology - OT) and the upcoming ISO 21434 for automotive. A common denominator of all those approaches is that they are all risk-driven and thus require the ability to carry out a risk analysis prior to implementing any kind of countermeasures.

As defined by (ISO, 2009), risk management is the process of identifying, assessing, and treating risks. More specifically, risk management aims at cancelling or at least minimising (mitigating) the adverse impacts and losses that a deliberate attack, a failure/error or an accidental “environmental” threat may cause and, where possible, reduce the probability of such events. To achieve these goals, it should encompass all coordinated activities needed to direct and control an organisation with regard to risk. This definition covers both security and safety dimensions. However, the nature, impacts, timing and risk culture are quite different in each domain. Even if there are benefits in considering and engineering them together, the scope of this paper will only by cyber security but it will consider both IT and OT systems since both can have complex interactions in specific domains and needs to be carefully analysed (BSI, 2020).

Learning risk management is a complex process, especially for cyber security, because it requires to combine many abilities such as:

- domain analysis, in order to identify what are the key assets and properties to ensure and what would be the impact of failing in protecting them.
- technical understanding and modelling of the relevant aspects of the infrastructure in order to identify attack scenarios and assess likelihood.
- thinking like an attacker to identify vulnerabilities and attack paths
- gaining domain specific knowledge about known vulnerabilities and attacks by various means such as interviews, seminars or vulnerability monitoring.
- qualitative reasoning based on partial information.

The learning process can vary depending on the context such as university course or professional training program. This paper considers a typical approach combining the following aspects:

- in depth theoretical introduction to risk analysis and its application to cyber security. A short summary is given in background Section 2.
- technological background about security building

Ponsard, C. and Massonet, P.
Survey and Guidelines about Learning Cyber Security Risk Assessment.
DOI: 10.5220/0010900800003120
In *Proceedings of the 8th International Conference on Information Systems Security and Privacy (ICISSP 2022)*, pages 536-543
ISBN: 978-989-758-553-1; ISSN: 2184-4356

bricks (e.g. cryptography) as well as threats and measures at different design layers (communications, operating systems, application).
- practice for producing a realistic risk analysis in a given domain using a well-defined methodology.

This paper reports about our analysis of a learning process in the above setting using a controlled experiment. It involved people with IT background for at least 5 years and enrolled in a training course to improve their cyber security skills, with a focus on risk analysis. Our aim here was to identify the main difficulties to carry out a cyber security risk analysis in a realistic context and to report about lessons learned in order to improve the acquisition of that expertise.

This paper is structured as follows. Section 2 gives background on the ISO 31000, ISO 27000 standards and the EBIOS implementation used in our experiment. Section 3 describes our validation experiment including its methodology, results and some threats to validity. Section 4 presents lessons learned also making the connection with more specific standards and tool support. Finally, Section 5 draws some conclusion and identifies our future work.

2 BACKGROUND on SECURITY RISK ANALYSIS

2.1 ISO 31000

A generic risk analysis process is specified by the ISO 31000 (ISO, 2018). To follow up with the risk management definition given in the introduction, a basic process of risk management is depicted in Figure 1.

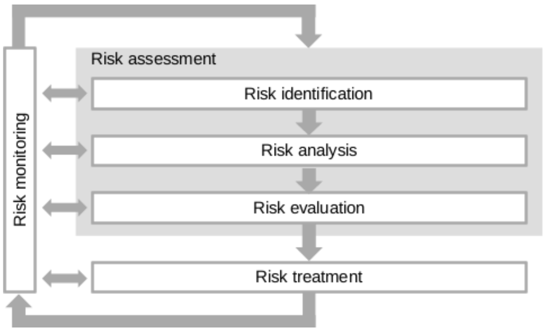


Figure 1: ISO 31000 Reference for Risk Assessment.

The main objective of risk management lies in the assessment of major corporate goals in regards to risk policy strategies. Hence, risks affecting long lasting business success need to be controlled. The global process goes through the following steps:
- **risk identification:** to find/understand/describe risks; considering everything that could hinder, prevent but also help to achieve business goals.
- **risk analysis** aims at understanding the nature of risk and its characteristics. It requires to investigate uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness w.r.t. the materialisation of risks.
- **risk evaluation** is the final phase of the risk assessment. It relies on the risk analysis which is often summarised using a qualitative risk matrix as depicted in Figure 4. At this point, a decision made about refining the analysis, reconsidering objectives or going into risk treatment phase.
- **risk treatment** selects and implements actions considering costs, effort and timing issues to reach an acceptable residual risk. For each risk, possible options are to: do nothing further (accept), consider additional actions (mitigation), share the consequences (transfer), removing the source (avoidance). An actionable plan is then prepared and executed by the management.
- **risk monitoring:** closes the loop by triggering new assessments when the organisation or risk landscape evolve. The monitoring is also internal, resulting in possible adaptation if outcomes are not satisfactory, e.g. quality of risk analysis or unacceptable residual risk.

2.2 ISO27005

The ISO 27000 is a family of standards for related to the deployment of information security risk management system (ISO, 2013). It defines the vocabulary (27000), requirements on the management systems (27001), controls (27002) and a risk-oriented management approach (27005).

The information security risk analysis process is a specialisation of ISO 31000 as shown in Figure 2. The ISO 27005 standard does not impose a methodology but a set of requirements related to:
- **context establishment:** must define scope, boundaries, roles and responsibilities.
- **risk identification:** must identify primary assets to protect and relevant support assets (software, hardware physical infrastructure, staff...). Various source of threats (internal, external) must be identified as well as their impact and existing controls.
- **risk estimation:** must provide an estimate of each risk in terms of likelihood and consequence based on impact on confidentiality, integrity or availability dimensions of information.
- **risk evaluation:** must produce a list of risks prioritized w.r.t the security risk evaluation criteria.

Many implementations of ISO 27005 are available: EBIOS (ANSSI, 2010b), MEHARI (CLUSIF,

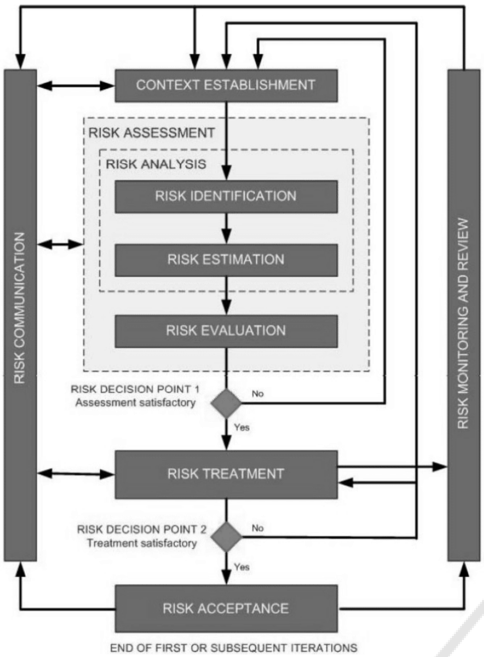


Figure 2: ISO 27005 Threat Analysis and Risk Assessment.

2010) or OCTAVE (SEI, 2007). Our experiment relies on EBIOS which is detailed hereafter.

2.3 EBIOS (ISO 27005 Compliant)

EBIOS (”Expression des Besoins et Identification des Objectifs de Sécurité”) is a French method supported by ANSSI, the national cyber security authority of France. It is compliant with the ISO27005. We consider the 2010 version which is depicted in Figure 3.

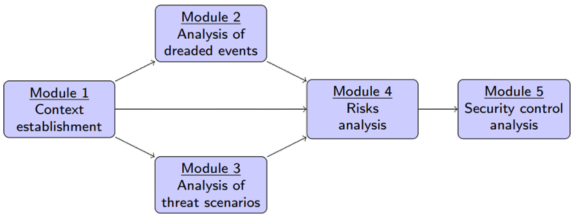
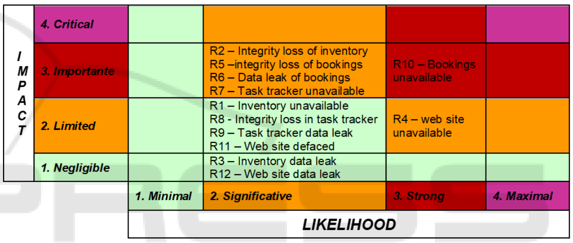


Figure 3: EBIOS Activities.

The implementation mapping with ISO 27005 is as follows:

- **context establishment** requires to state organisation goals and analysis perimeter, to define scales to measure confidentiality, availability and integrity in the organisation context. It also covers identification of primary (i.e. business) and secondary (i.e. support) assets as well as their relationships (i.e. how IT infrastructure supports the business functions). Information flows are depicted through an infrastructure diagram.
- **dreaded event analysis:** is a top-down approach focusing on the business impact when the security of primary assets is threatened by the considered threat sources.
- **threat scenarios analysis** is carried out in parallel with dreaded event analysis. It works bottom-up by considering the threat scenarios affecting the support assets, e.g. phishing attempt, firewall configuration problem allowing some external attacker to reach internal resources, etc. The likelihood is estimated on a qualitative scale defined in the context. Estimates are done before and after the application of existing measures.
- **risk analysis** combines the output of the two previous steps to estimate each risk and produce a risk matrix as depicted in Figure 4. The process can combine multiple scenarios by considering the worst case. Prioritisation is done and action decided among the options proposed in ISO 31000 (avoid, accept, mitigate, transfer).



IMPACT	4. Critical				
	3. Importante		R2 – Integrity loss of inventory R5 –integrity loss of bookings R6 – Data leak of bookings R7 – Task tracker unavailable	R10 – Bookings unavailable	
	2. Limited		R1 – Inventory unavailable R8 - Integrity loss in task tracker R9 – Task tracker data leak R11 – Web site defaced	R4 – web site unavailable	
	1. Negligible		R3 – Inventory data leak R12 – Web site data leak		
		1. Minimal	2. Significative	3. Strong	4. Maximal
		LIKELIHOOD			

Figure 4: Risk Matrix.

- **security control analysis** selects security controls for risk treatment in order to cover all risks requiring additional measures. Those are organised in different lines of defence, i.e. prevention, protection and recovery. Guidance is provided using a knowledge base (ANSSI, 2010a) and a list of controls like ISO27002. Residual risk analysis and planning are done as prescribed by ISO 27005.

3 CONTROLLED EXPERIMENT

3.1 Methodology

Our experiment was conducted in 6 weeks between October 15 and December 31, 2020. It gathered 35 people working in different organisations across a wide range of application domains including public administration, defence, education, game development, healthcare, insurance, manufacturing and telecommunications. All the participants were located in the French speaking part of Belgium with at least 5 years of experience in their domain and a strong IT background. They were given a specific training of about 12 hours in cyber security risk management prior to the experiment to ensure a common background. The training effectiveness was assessed by an examination covering both theoretical concepts and two control points: first about their ability to reason on business and technical assets, and second, to carry our the risk analysis process.

The selected method is EBIOS which was introduced in the previous section. This choice was deliberate for the following reasons:

- it is a generic method with focus on the organisational risk level as well as on security.
- it is easy to learn and provides a good documentation/knowledge base.
- it requires to clearly state domain specific concepts which may be implicit in more advanced methods. So it is easier to identify which and how well they are covered.

Each risk analysis was conducted by the trained people within their organisation with the authorisation and support of the management. Only limited tool support was used, mainly a spreadsheet to manage the data in tabular form. It was then documented in a report following the EBIOS structure. These were approved through an internal review and partially anonymized before we could analyse them. An intermediary review was organised before the final version in order to correct some common flaws and ensure more homogeneity. The documents were then audited by us using a procedure similar to an external certification audit.

Not all risk analyses were kept in our study. Out of the 35 initial candidates, only 26 were selected. The reasons to discard some analyses are the following:

- risk analysis was interrupted or postponed.
- authorisation was not granted by the company management.
- the audit revealed a major issue in conducting the risk analysis process.

3.2 Main Results

Table 1 shows the results of our risk analysis. Each case study is characterised using the following attributes:

- anonymized topic giving an idea of the application domain
- domain classification in the major sectors stated earlier.
- target either corporate or citizen which means a potential GDPR issue.
- NIS: means the case falls under the Network Information System directive (Operator of Essential Service or Digital Service Provider).

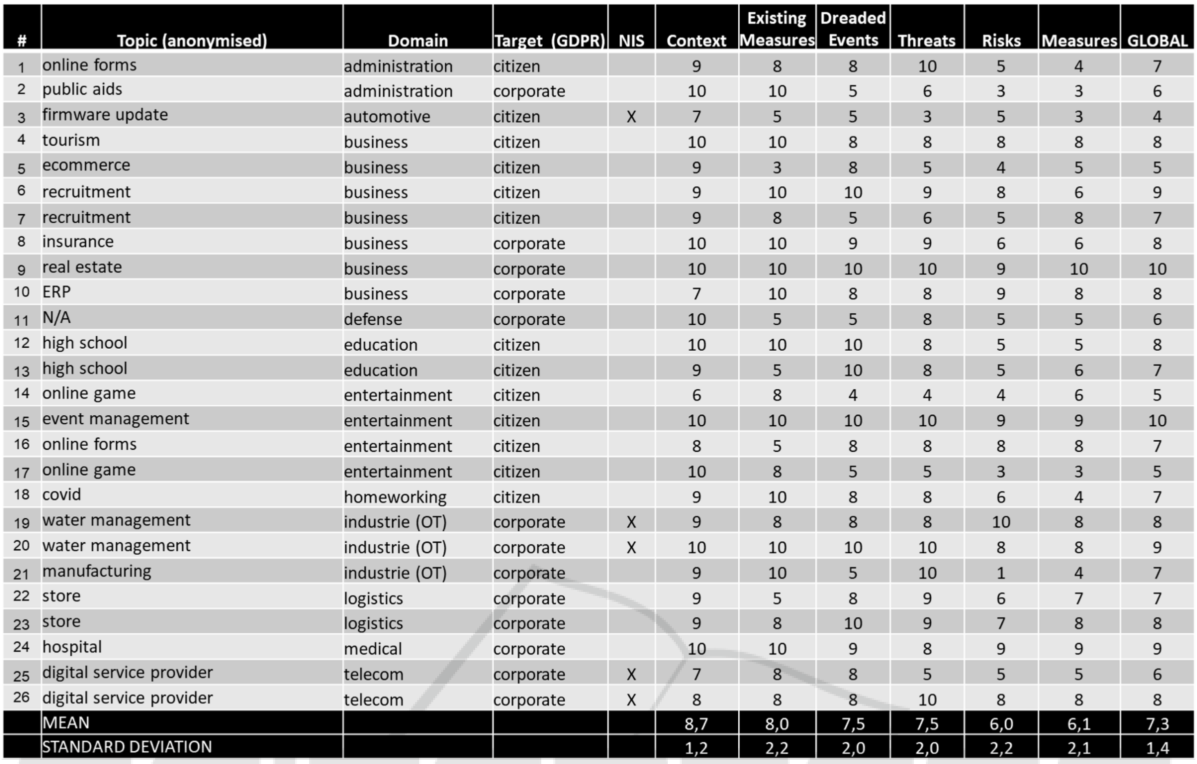
The next columns of the table assesses the quality of each main section of the EBIOS analysis. They are bound to each activity documented in a corresponding chapter of the report. Ranking uses a scale from 0 to 10, based on the evaluation grid detailed hereafter:

- **context:** relevance of primary assets and criteria w.r.t. company goals, level of detail of support assets and traceability to primary assets, identification of existing measure and threat sources.
- **dreaded event:** coverage of primary assets and completeness with respect to security properties.
- **threat analysis:** investigation of common vulnerabilities and common attacks targeting each type of support asset.
- **risk evaluation:** correctness of inference and reduction related to existing measures. Relevance of risk management strategy.
- **risk measures:** coverage of selected risks. Relevance of (single or multiple) actions on different line of defence. Traceability towards reference framework (e.g. ISO 27005, NIST CSF or IEC 62443). Practicability of associated implementation plan.

From Table 1, some interesting trends can be observed:

- globally the quality level is quite satisfactory (above 7) with few problematic audits. Those could be linked either to immature businesses (e.g. early game development) or research topics (e.g. management of firmware updates)
- the level of quality degrades as we progress through the workflow. This can be due to the accumulation of flaws hindering the correct management of next steps. There is also a switch in complexity from more descriptive to more prescriptive tasks in the last part of the analysis.
- the cases involving citizen have a lower global score. This could be related to a more open context of such analysis, including privacy issues. A specific privacy impact analysis could be advised for such security requirements.
- looking at specific domains: business (8), education (8), industry/logistics (8) seem to perform better than administrations (7), gaming (7) and telecom (7). Other fields are not considered because of too few cases. While classical IT domains are favoured, administration and gaming seem less easy to capture. For administration, complex infrastructure result in large analysis. For gaming, deployment can be quite complex and there is also less control and many assumptions over the environment. Digital service providers in telecom area are probably too specific to draw general conclusions.

Table 1: Survey Results.



#	Topic (anonymised)	Domain	Target (GDPR)	NIS	Context	Existing Measures	Dreaded Events	Threats	Risks	Measures	GLOBAL
1	online forms	administration	citizen		9	8	8	10	5	4	7
2	public aids	administration	corporate		10	10	5	6	3	3	6
3	firmware update	automotive	citizen	X	7	5	5	3	5	3	4
4	tourism	business	citizen		10	10	8	8	8	8	8
5	ecommerce	business	citizen		9	3	8	5	4	5	5
6	recruitment	business	citizen		9	10	10	9	8	6	9
7	recruitment	business	citizen		9	8	5	6	5	8	7
8	insurance	business	corporate		10	10	9	9	6	6	8
9	real estate	business	corporate		10	10	10	10	9	10	10
10	ERP	business	corporate		7	10	8	8	9	8	8
11	N/A	defense	corporate		10	5	5	8	5	5	6
12	high school	education	citizen		10	10	10	8	5	5	8
13	high school	education	citizen		9	5	10	8	5	6	7
14	online game	entertainment	citizen		6	8	4	4	4	6	5
15	event management	entertainment	citizen		10	10	10	10	9	9	10
16	online forms	entertainment	citizen		8	5	8	8	8	8	7
17	online game	entertainment	citizen		10	8	5	5	3	3	5
18	covid	homeworking	citizen		9	10	8	8	6	4	7
19	water management	industrie (OT)	corporate	X	9	8	8	8	10	8	8
20	water management	industrie (OT)	corporate	X	10	10	10	10	8	8	9
21	manufacturing	industrie (OT)	corporate		9	10	5	10	1	4	7
22	store	logistics	corporate		9	5	8	9	6	7	7
23	store	logistics	corporate		9	8	10	9	7	8	8
24	hospital	medical	corporate		10	10	9	8	9	9	9
25	digital service provider	telecom	corporate	X	7	8	8	5	5	5	6
26	digital service provider	telecom	corporate	X	8	8	8	10	8	8	8
	MEAN				8,7	8,0	7,5	7,5	6,0	6,1	7,3
	STANDARD DEVIATION				1,2	2,2	2,0	2,0	2,2	2,1	1,4

- except for automotive, NIS cases resulted on assessment scores above average (8), reflecting the ongoing works to comply with the directive, i.e. typically ISO 27000 or IEC 62443 certification.

3.3 Some Threats to Validity

- *Conclusion validity*: globally the sample size is enough to infer global trends but analyses on subsamples need to be treated with caution. For this reason, domains with few cases were not analysed at that level. The sampling can be justified using Cochran's formula (Cochran, 1977) with Z score of 90%, a relatively raw precision of 15% and our estimate that after training, the probability of adoption is quite high and certainly above 75%. We get $size = (1.645^2 \cdot 0.75 \cdot 0.25)/0.15^2 = 23$ which is about the size of our sample (26). Given the small population of risk analysts, this number is slightly overestimated but we will not apply additional corrections here.
- *Internal validity*: the selection of risk analysts was done through a specialised complementary training program in computer security which required to have experience in IT. There was no control on the selection process but some cases were dropped due to resignation or postponement.
- *Construct validity*: the selected risk analyst profiles need to be representative for the role of an analyst inside the organisation. The selection process ensured this through requirements of experience in IT, the registration to the course and the mentioned control points.
- *External validity*: our experiment environment including its timing is representative and can be generalised as it was carried out inside real organisations from different domains.

4 DISCUSSION AND LESSONS LEARNED

This section summarises key lessons learned from our controlled experiment presented in Section 3.

4.1 Avoiding Uncontrolled Growth of the Number of Risks

A frequent issue in our experiments also often pointed out by other users of methods like EBIOS is the uncontrolled explosion of risks due to the need to explore many scenarios for the combination of assets with the considered security properties. Some recommendations are to focus on major assets, to group them or to hide the complexity at presentation level (Club EBIOS, 2020). These are not satisfactory as they result either in a coarser grained analysis or increase the presentation work. A more interesting suggestion is use richer domain knowledge or better prioritization techniques. The following techniques can be helpful:

- making the assumption that specific assets of the system are protected, possibly pushing the responsibility to prove this to another party or relying on a strong protection, or low residual risk (Club EBIOS, 2020).
- taking into account domain knowledge about risk dependencies will reduce the need to explore impossible scenarios. Such approach requires to rely on more structured knowledge representation, i.e. use modelling as discussed later in this section.
- working by refinement levels, i.e. performing a coarse-grained system level analysis and digging further if required. This approach is adopted by the IEC 62443 security risk analysis process for industrial systems (IEC, 2020): the high-level risk analysis (ZCR2) aims at identifying the worst-case unmitigated cyber security risks related to mission critical operations. If unacceptable risks are identified, a detailed cyber security risk assessment (ZCR5) is performed.
- breaking the systems into subsystems is required to support the previous approach and is also proposed by IEC 62443 through segmentation in zones connected by conduits. A particular attention is required on conduit interfaces.
- having an early focus on major risks only. This might seem a dangerous simplification but it will ease and speed up the analysis. The idea is to check the residual risks and to take a more iterative approach. It might be more efficient than a “waterfall” approach because it keeps the complexity under control. Moreover the considered measures may also mitigate less important risks.
- defining security levels to capture which security requirement should be covered in a staged ways. This provides a safer path as the risk profiles can be validated by experts. For example, in the scope of IEC 62443, segmentation is mandatory from the lowest (SL1) level but additional requirements are placed at SL2 to reach physical level segmentation, at SL3, to enforce independence from non-control network, and at SL4, to have logical and physical isolation of critical networks.

4.2 Need for Deeper Modelling

The ISO 27005 assessment process implemented through EBIOS is globally quite flat. It relies on basic, coarse grained, and table-based traceability between relevant elements that need to be matched during the analysis. It is mainly the coverage between support and primary assets to ensure the sound capture of risk attributes and combine them consistently although in a quite simple way, i.e. using the worst case scenario for each kind of risks. In the risk treatment phase, another coverage check is used to make sure all risks are adequately mitigated. Although some modelling is present to support identification, e.g. through attack trees (Schneier, 1999) or infrastructure modelling, it remains limited and lack integration inside a wider form of modelling enabling more precise, powerful and automated analysis. Some emerging trends in this area are the following:

- *infrastructure modelling*: the notion of zone and conduit introduced in IEC 62443 is a way to structure the infrastructure model. It is also present to some extend in IT modelling through the notion of zone (e.g. DMZ). It used in some threat modelling tools like Threat Dragon (OWASP, 2020) or Microsoft Threat Modeller (Microsoft, 2017).
- *attack trees*: can help drive the identification of attacks starting either from high-level scenarios in a top-down approach or from component vulnerabilities in a bottom-up approach. They can also integrate defence elements to integrate risk measures. This can result in a deeper analysis considering higher-order forms of attacks (Roy et al., 2012). Based on this, more quantitative forms of reasoning, including multi-objective optimisation can be considered (Fila and Wideł, 2019)
- *goal-oriented modelling* can provide a global binding by supporting the capture of goals at various level of an organisation together with techniques to reason on obstacles to their achievement which are compatible with both security and safety analyses (van Lamsweerde, 2009). This can help in the analysis of the many impacts of cyber security risks in various kinds of systems, including safety critical systems. We already investigated such an approach in the NIS area (Ponsard et al., 2021a) and in the automotive section, considering the future ISO 21434 standard (Ponsard et al., 2021b).

Modelling could bring many other benefits in the global risk analysis workflow:

- leaving the inefficient document-oriented approach which is still quite widespread in certification. Beyond a certain complexity level, document-based approach becomes impractical limiting either the ability to analyse large systems or the precision level. Using and maintaining the model as the core artefact would enable to generate always up-to-date documents.

- maintaining the model, although at a cost, would enable a more reactive analysis in case of system evolution or new threads. It would also reduce the cost of the new risk analysis and result in a more responsive, agile and risk-proof organisation.
- better collaboration by sharing risk-oriented models in the design phase (e.g. co-engineering safety and security) and later in the certification phase using model as central asset rather than document flows, possibly including third parties, e.g. regulation or controlling bodies.

4.3 Tool Support

Tooling was deliberately not the focus of our experiment although some attack or threat modelling tools were investigated. In relation with the previous topics, it seems interesting to consider modelling tools able to combine infrastructure, goal and threat models. Additionally, the tool should also be quite generic with respect to the risk framework used, i.e. the analysis process should itself be modelled inside the tool. This would ensure the tooling can evolve with the considered standard/certification scheme, or allow one to switch between different schemes, or even to manage different schemes simultaneously, e.g. for safety critical domains requiring also a safety certification. With respect to this, the OpenCert platforms developed by the AMASS project proposes an integrated and holistic solution for assurance and certification management of Cyber-Physical Systems (CPS) spanning the largest safety and security-critical industrial markets (Polarsys, 2018).

Another trend in tooling is to share the model in a collaborative but controlled way across different actors in a global process (here certification), with proper views and rights (e.g. edit, review, approve). This is useful for regulated sectors involving many interacting organisations sharing similar risks that can propagate from one to another, e.g. for specific sectors of the NIS directive. A proposed approach is first to model the ecosystem, then to propagate risk/perform systemic risk, and finally, to get a top level evaluation by a national authority in the considered domain (Mayer. and Sottet., 2020).

4.4 Towards More Lightweight and Incremental Certification

Risk analysis is an iterative process. In the scope of a product certification, when the products evolves, the certification needs to be reacquired. This process can be very expensive when using an heavyweight process. Hence, the emerging trend is to move to more incremental forms of certification, especially in the cyber security area requiring reactivity to face the constantly evolving threat landscape. To support this, DevSecOps techniques are very relevant as they have the ability to integrate security tools across the whole continuous integration DevOps lifecycle, from threat modelling, security by design, penetration testing to operation intrusion detection (IDS) and security information management system (SIEM). They can also provide direct connection to Common Vulnerabilities and Exposures (CVE) databases and alerting mechanisms. A model-based approach is relevant to capture how the certification workflow is deployed on the toolchain and how the impact of changes can be tracked and trigger incremental updates of the risk analysis (Dupont et al., 2021).

As many organisations, especially smaller ones, are often reluctant to consider standards and certifications, it is useful to think about a path that will protect the companies by first raising awareness and encouraging self-assessment or basic protection through labels like Cyber Essentials (UK) or Keep It Secure (Belgium) (Ponsard and Grandclaudon, 2018). In a second stage, as they mature, they can then evolve towards certification schemes providing more confidence but with a minimal gap and overhead from the previous step (Ponsard et al., 2020).

5 CONCLUSION AND PERSPECTIVES

In this work, after presenting existing standardized risk analysis approaches, we conducted a controlled experiment in risk analysis involving adequately trained people from 26 different organisations and across a variety of domains. From the collected results, we could learn about recurring difficulties such as structuring the analysis, reasoning on threats and producing an useful risk estimation. We also proposed recommendations at methodological and tool levels, including in the context of certification.

As on-going and future work, we are considering a second wave of cases relying on a similar introductory course but with the aim to dig into the following directions identified in our lessons learned:

- rely on more specialised methods than the generic EBIOS method used here, especially investigating zone and conduit modelling as proposed in the IEC 62443 or more detailed attack path analysis as described in the ISO 21434.
- implement our recommendations through more advanced model-based tooling, assess their benefits and try to minimize possible drawbacks.

The collected feedback will then be compared to the baseline presented here to assess how effective or enhancements are w.r.t. qualities such as precision, relevance, completeness or readability. Additionally, we also plan to investigate more DevSecOps and incremental techniques through a car platooning case study.

ACKNOWLEDGMENT

This work was partly funded by the CYRUS (grant nr. 8227) and SPARTA projects (grant nr. 830892). We thank the survey participants for their contribution to this study and the anonymous reviewers for their precise comments.

REFERENCES

ANSSI (2010a). EBIOS - Knowledge Base. https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-2-BasesDeConnaissances-2010-01-25.pdf.

ANSSI (2010b). Expression des Besoins et Identification des Objectifs de Sécurité. https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-1-GuideMethodologique-2010-01-25.pdf.

BSI (2020). ICS Cybersecurity Assessment Framework - Suitable standards supporting a hybrid approach to risk management. White paper.

Club EBIOS (2020). EBIOS - Questions & Answers. https://club-ebios.org/site/en/how-to-avoid-the-combinatorial-explosion-of-a-study.

CLUSIF (2010). MEHARI 2010 Information risk management method ISO/IEC 27005 compliant. http://meharipedia.x10host.com/wp.

Cochran, W. G. (1977). *Sampling Techniques, 3rd Edition.* John Wiley.

Dupont, S., Ginis, G., Malacario, M., Porretti, C., Maunero, N., Ponsard, C., and Massonet, P. (2021). Incremental Common Criteria Certification Processes using DevSecOps Practices. In *IEEE European Symposium on Security and Privacy Workshops, EuroS&P 2021, Vienna, Austria*.

ENISA (2020). Threat Landscape 2020 - List of top 15 threats .

Fila, B. and Wideł, W. (2019). Efficient Attack-Defense Tree Analysis using Pareto Attribute Domains. In *IEEE 32nd Computer Security Foundations Symposium (CSF)*.

IEC (2020). 62443 - Industrial communication networks - Network and system security. https://www.iec.ch/blog/understanding-iec-62443.

ISO (2009). Risk management – vocabulary. ISO Guide 73.

ISO (2013). ISO/IEC 27000 Family - Information Security Management Systems. https://www.iso.org/isoiec-27001-information-security.html.

ISO (2018). ISO 31000, Risk management - Guidelines, provides principles, framework. https://www.iso.org/iso-31000-risk-management.html.

Mayer., N. and Sottet., J. (2020). Systemic security risks in the telecommunications sector: An approach for security and integrity of networks and services. In *Proc. of the 5th Int. Conf. on Complexity, Future Information Systems and Risk*.

Microsoft (2017). Threat modelling tool. https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling.

NIST (2014). Cybersecurity Framework. https://www.nist.gov/cyberframework.

OWASP (2020). Threat dragon. https://owasp.org/www-project-threat-dragon.

Polarsys (2018). Open Cert. https://www.eclipse.org/opencert.

Ponsard, C. and Grandclaudon, J. (2018). Survey and guidelines for the design and deployment of a cyber security label for smes. In *4th Int. Conf. on Information Systems Security and Privacy, Funchal, Madeira*.

Ponsard, C., Grandclaudon, J., and Massonet, P. (2021a). A goal-driven approach for the joint deployment of safety and security standards for operators of essential services. *J. Softw. Evol. Process.*, 33(9).

Ponsard, C., Massonet, P., Grandclaudon, J., and Point, N. (2020). From Lightweight Cybersecurity Assessment to SME Certification Scheme in Belgium. In *IEEE European Symposium on Security and Privacy Workshops, EuroS&P Workshops, Genoa, Italy*.

Ponsard, C., Ramon, V., and Deprez, J.-C. (2021b). Goal and Threat Modelling for Driving Automotive Cybersecurity Risk Analysis Conforming to ISO 21434. In *Proc. 18th Int. Conf. on Security and Cryptography*.

Roy, A., Kim, D. S., and Trivedi, K. S. (2012). Attack countermeasure trees (ACT): towards unifying the constructs of attack and defense trees. *Security and Communication Networks*, 5(8).

Schneier, B. (1999). Attack trees. Dr. Dobb's journal.

SEI (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. http://www.cert.org/octave.

van Lamsweerde, A. (2009). *Requirements Engineering - From System Goals to UML Models to Software Specifications*. Wiley.