Enterprise Risk Monitoring Methodology, Part 4

Risk Executive Summary

Everyone involved in the enterprise risk management process has probably had to summarize their work and condense a great deal of information into a short presentation. In doing so, it is often necessary to highlight some information at the expense of other information or to simplify an idea without losing the importance of the overall concept. In the end, there may be a sense of dissatisfaction with the result and the feeling that it could have been done better.

Explaining an array of concepts in a concise and easy-to-understand way is always a challenge. When discussing risk, various other background information must also be presented. For example, the risk concept is connected to a potential event, and this potentiality blurs the contours of a risk's value. To better understand the rationale for the valuation of risk, other information must be considered, such as probability, impact, remediation controls and so on. Also, risk factors are generally ordered on the basis of their value, without taking into account all their components and the correct levels of exposure.

A method of simply and clearly organizing the results of risk assessments and the necessary background information has been proposed. The objective is to obtain high visibility for both high-impact and high-frequency risk factors, while allowing an assessment of remediation plans and a separation between internal and external risk factors. This article is part 4 in a series and continues the risk monitoring methodology presented in the three previous articles.[1, 2, 3]

Risk Monitoring Methodology

To understand what the risk components are and how they are collected, a quick summary of a suitable methodology is in order. Taking a cue from the contributions, principles, methods and ideas derived from a wide variety of works, bodies and standards dealing with the management and control of business processes,[4, 5, 6, 7, 8, 9, 10] a risk assessment methodology based on a previous evaluation of the enterprise maturity model is the starting point.

The evaluation of the maturity model involves compiling a list of all the controls the enterprise has in place and then assessing the maturity of each one. This self-assessment is the first step in the evaluation, but to acquire greater confidence in the results, remote checks are carried out by the process owners, risk managers make on-site visits and an internal audit is performed. A synergistic

Luigi Sbriz, CISM, CRISC, ISO/IEC 27001 LA, ITIL v4, UNI 11697:2017 DPO
Has been the risk-monitoring manager at a multinational automotive company for more than five years. Previously, he was responsible for information and communication operations and resources in the APAC Region (China, Japan and Malaysia) and, before that, was the worldwide information security officer for more than seven years. For internal risk monitoring, he developed an original methodology merging an operational risk analysis with a consequent risk assessment driven by the maturity level of the controls. He also designed a cybermonitoring tool and an integrated system for risk monitoring, maturity model and internal audit. Sbriz was a consultant for business intelligence systems for several years. He can be contacted on LinkedIn (*https://it.linkedin.com/in/luigisbriz*).

cycle comprising the Capability Maturity Model (CMM), the enterprise risk management (ERM) process and the internal audit (IA) process results in mutual benefits (**figure 1**).

An evaluation of the maturity model using a suitable formula allows a determination of the level of risk. As long as each risk defined in the enterprise's risk list is connected to a set of controls in the maturity model, all risk factors will automatically be assessed. The resulting risk map allows the selection of indicators that will trigger an audit. The internal audit corroborates the correctness of the assessment of controls, and the audit remediation plan can be incorporated into the risk treatment plan because it has the same structure and operates in the same context.

The enterprise risk assessment (ERA) is the evaluation of the CMM controls assessment process, which is part of the enterprise risk monitoring methodology. Just as the CMM feeds the enterprise risk model, it can also automatically feed other frameworks (see parts 1–3 of this series for details).

CMM Assessment

Before proceeding to the method of presenting risk data, it is necessary to consider some of the controls that make up the maturity model. One consideration is the evaluation of maturity. Risk assessors must recognize that there is an additional step beyond pure respect of a rule: The rule, as applied, must satisfy the risk analysis.

To do this, the rating levels "Compliant" and "Further Attention" (used in the previous articles in this series) are renamed "Optimized" and "Compliant," respectively. The new Compliant level indicates a state of simple, formal compliance with the rule, while Optimized indicates that the rule has been implemented in full compliance with the risk containment plan (**figure 2**). This change clarifies the distinction between simple compliance with a rule and verification that any decisions have been implemented with a risk-based logic. This distinction is also important to highlight situations that involve value creation and not just potential loss, as is often the case in risk analysis.

Figure 1—Risk Monitoring Model

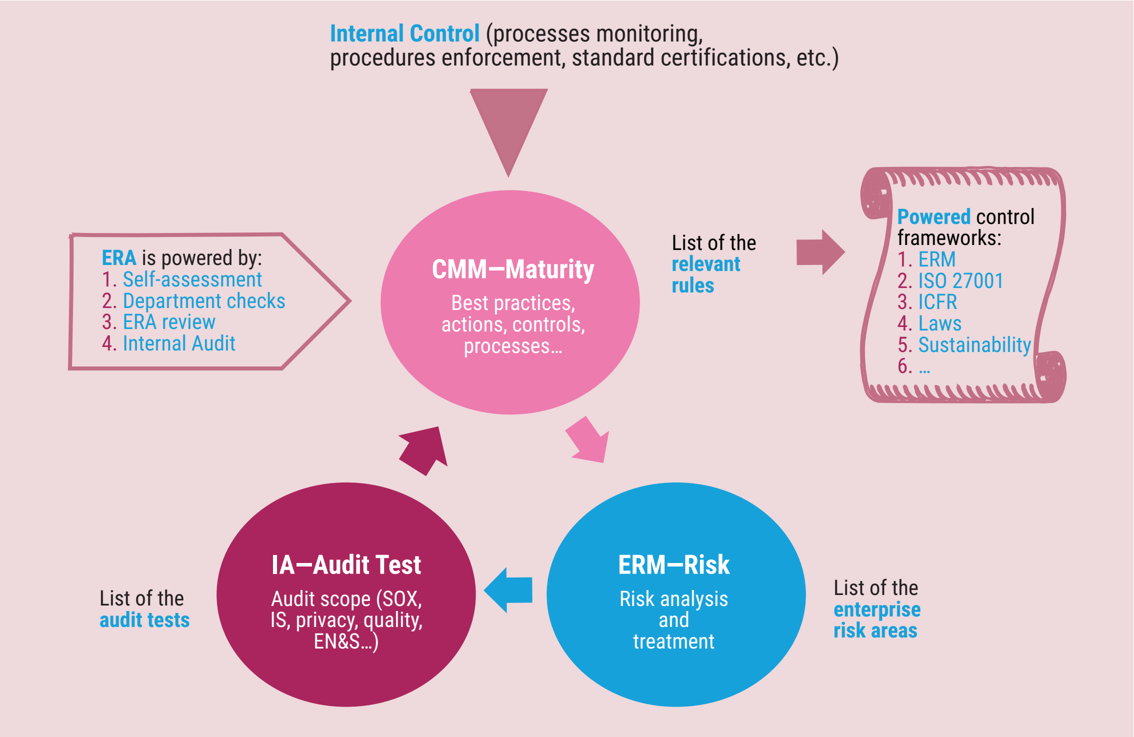

Internal Control (processes monitoring,
procedures enforcement, standard certifications, etc.)
ERA is powered by:
1. Self-assessment
2. Department checks
3. ERA review
4. Internal Audit
CMM—Maturity
Best practices, actions, controls, processes…
List of the relevant rules
Powered control frameworks:
1. ERM
2. ISO 27001
3. ICFR
4. Laws
5. Sustainability
6. …
IA—Audit Test
Audit scope (SOX, IS, privacy, quality, EN&S…)
ERM—Risk
Risk analysis and treatment
List of the audit tests
List of the enterprise risk areas

Figure 2—Evaluation of the Maturity Model

#	Maturity Level Evaluation of the Level of Implementation of the Control Statement	Level	Score
0	No local responsibilities for the topics; the event cannot occur; the rule is not applicable	Not applicable	1.00
1	Appropriate, effective, measured, fully compliant with the declared actions, risk analysis performed	Optimized	1.00
2	Formal respect of rules, but improvements may be needed, no investment for actions, no risk-based measures	Compliant	0.95
3	Work in progress, started but not completed, plan is on time	In progress	0.80
4	Addressed; planned; all resources allocated, but operations have not started	Planning	0.70
5	Evidence of minor issues; misapplication of the rule; corrective actions required, but unplanned	Partially done	0.50
6	Unqualified; not in compliance; explanation is required	Noncompliant	0.30
7	Unknown; missing answer; no information provided	No info	0.10

For a risk analysis to be accepted, two measures must be performed—the first on current controls and the second on all countermeasures up to an admissible risk level. For this reason, a new parameter must be monitored. One way to evaluate countermeasures (i.e., controls planned for the future) is to request a progress report on these remedial measures. A list of job progress qualifiers is presented in **figure 3**.

In assessing the progress of the remediation plan, there is a distinction between the work implemented and the work completed and verified in terms of its effectiveness. Each qualitative level of progress is accompanied by a numerical measurement between 0 and 1 for immediate use in risk calculation formulas (**figure 4**) and its consequent consolidation.

If not effectively implemented, the remediation plan will reduce the maturity level of the control. The risk matrix provides each control with a risk value based on the triad of maturity, loss and likelihood parameters. In structured consolidations, the risk-control relationship allows a weighted average of the control with respect to the other controls (severity) and with respect to the risk itself (risk weight factor).

Maturity Model and Risk Management Concepts

It is useful to graphically represent all the main risk components so that they can be viewed together in a single glance. The level of risk is the first component to consider. It is only a number if it is not compared with other information. Using a

Figure 3—Defining the Progress of the Remediation Plan

#	Remediation Plan Progress Expected Progress of the Remediation Plan	Level	Score
0	Status: No action is required; unnecessary control; missing risk analysis	No action needed	0.90
1	Status: Appropriate; meets risk analysis; performing well; measured	Effective	1.00
2	Status: Running; may need some improvement; no critical issues	Implemented	0.95
3	Status: Work in progress; everything on time	In progress (on time)	0.80
4	Status: Delayed planning; timelines are not respected	In progress (delayed)	0.70
5	Status: Measures addressed but no action yet	Planning	0.50
6	Status: Planning due but lacking	Unplanned	0.10

Figure 4—Risk Calculation Formula

$$risk = f\left[\frac{\sum_{i=1}^{n} risk\ matrix\begin{pmatrix} maturity_i * progress_i, \\ loss_i, \\ likelihood_i \end{pmatrix} * severity_i * risk\_weight_i}{\sum_{i=1}^{n} * severity_i * risk\_weight_i}\right]$$

strengths, weaknesses, opportunities and threats (SWOT) methodology,[11] all critical factors having an internal and an external origin are identified and separated in a context analysis. When a risk factor is internal, remediation is often a matter of improving the performance of a business process; when a risk factor is external, it probably requires new initiatives or innovative solutions. So a graphic distinction between these two typologies is certainly desirable.

> “PRESENTING ALL POTENTIAL IMPACTS IN ONE PLACE MAKES IT EASY TO SEE WHETHER THE PRIORITIZATION OF ACTIVITIES IS GOING IN THE RIGHT DIRECTION.”

A second component is the potential economic loss following the occurrence of the one event with the greatest impact. Presenting all potential impacts in one place makes it easy to see whether the prioritization of activities is going in the right direction—that is, the event with the highest impact must be managed before those with lower impacts. The visual presentation of these impacts must also provide an immediate understanding of whether the impact is an opportunity or a loss.

The third component is the likelihood that the event with the greatest impact will occur. It is vital to use a perspective representation that avoids an overcrowding of points on the graph for high-probability values, ensuring sufficient clarity for the conditions that require greater attention or prompt intervention.

The progress of remediation plans is the fourth main component. It is possible to have situations in which a high risk for the enterprise is addressed by a series of countermeasures, but it is important to know the progress of these remediation measures. In the case of high-impact risk, information about the level of risk does not provide a complete picture of the situation. It is necessary to know whether the countermeasures are working well and whether the implementation plan is proceeding on schedule to determine whether the risk is really being managed.

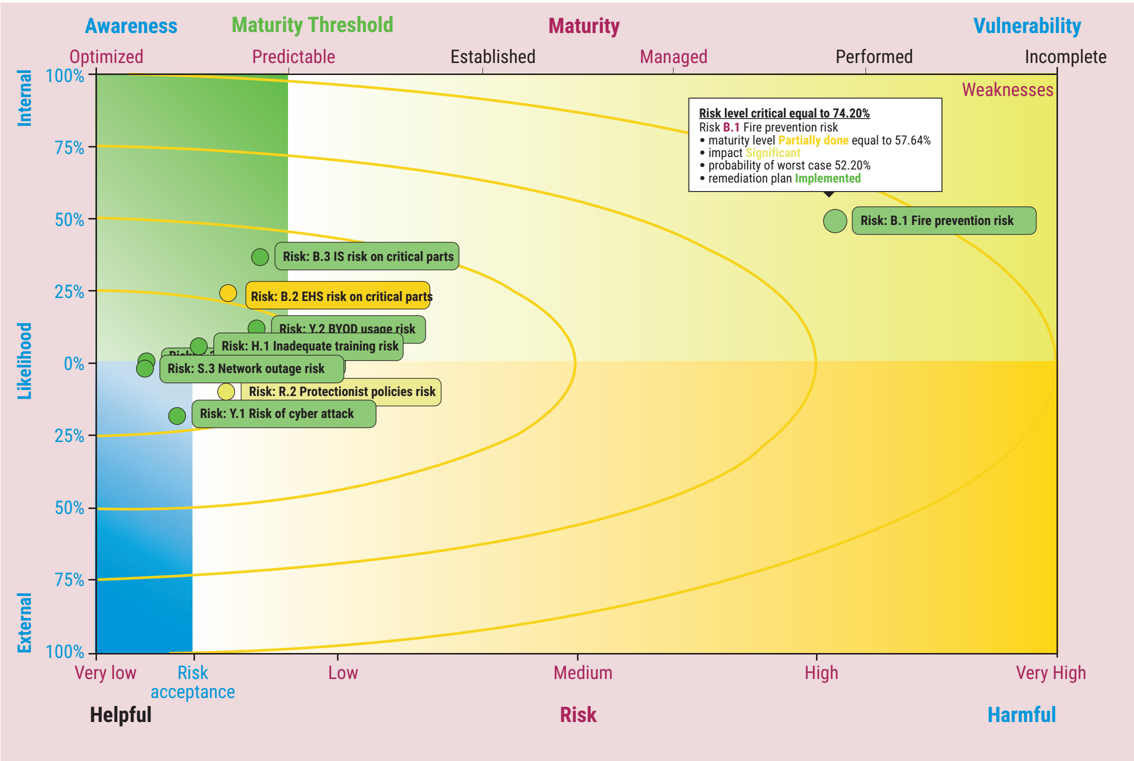
Using the maturity model as a basis for analyzing risk means that this information will be available when details are requested, including all the controls underlying the risk factors being analyzed. The use of the maturity model also allows for the creation of a vulnerability map to justify the level of risk resulting from these assessments. This additional information adds value to the analysis, but it requires the use of a visualization model that is suitable for this purpose and does not introduce confusion in the presentation of data.

Risk Executive Summary Graph

A method of graphically presenting the four components discussed in the preceding section (plus maturity when further details are requested) can be outlined. A layout similar to the SWOT analysis is used to frame all the information. This layout was chosen because the context analysis is the first step in the risk assessment, and it proceeds by investigating the uncertainty factors related to the achievement of business objectives. It is, therefore, reasonable to conclude that this is a suitable method to represent risk factors and causes as a whole.

First, the risk factors are distributed in the graph (**figure 5**). It is obvious that they tend to focus on a

Figure 5—Distribution of Risk Factors and Their Main Components



central point that coincides with the expected situation under control. In this zone, overlaps do not matter because attention is directed where the risk factors create significant impacts. These are more scattered and, therefore, more visible. The layout is derived from a compromise between a bubble scatter chart and the quadrant chart of a SWOT analysis, with some additional information.

The level of risk is uniformly distributed on the abscissa (x-axis), with evidence of the risk acceptance threshold. This acts as a separator, and all risk on the right must be considered for corrective action. The further right a risk appears on the graph, the sooner action must be taken. More than 80 percent of the axis length is dedicated to risk factors that should be observed or acted on, while little space is dedicated to those that are accepted (no action needed).

On the ordinate (y-axis), the probability of the occurrence of events is distributed in double sequence. The upper sequence is for events with internal causes, and the lower one is for those with external causes. This separates risk factors that require a change in internal processes from those that need to be designed or adjusted to deal with external events. The latter will probably require a significant expenditure in both time and money.

Bubbles contain two different types of information. The bubble diameter is linked to the impact value, and the bubble color indicates the progress of work to achieve protection objectives. Bubbles with larger diameters and colors from yellow to red indicate those cases with the greatest impact on enterprise objectives and compromised remediation plans; that is, countermeasures have not been implemented.

The background colors represent the four quadrants of the SWOT analysis. This allows a visual representation of the positioning of risk factors with respect to the improvement or deterioration of the processes. The background color helps identify the nature of the risk and whether it can create value rather than represent an alarm signal for a potential incident.

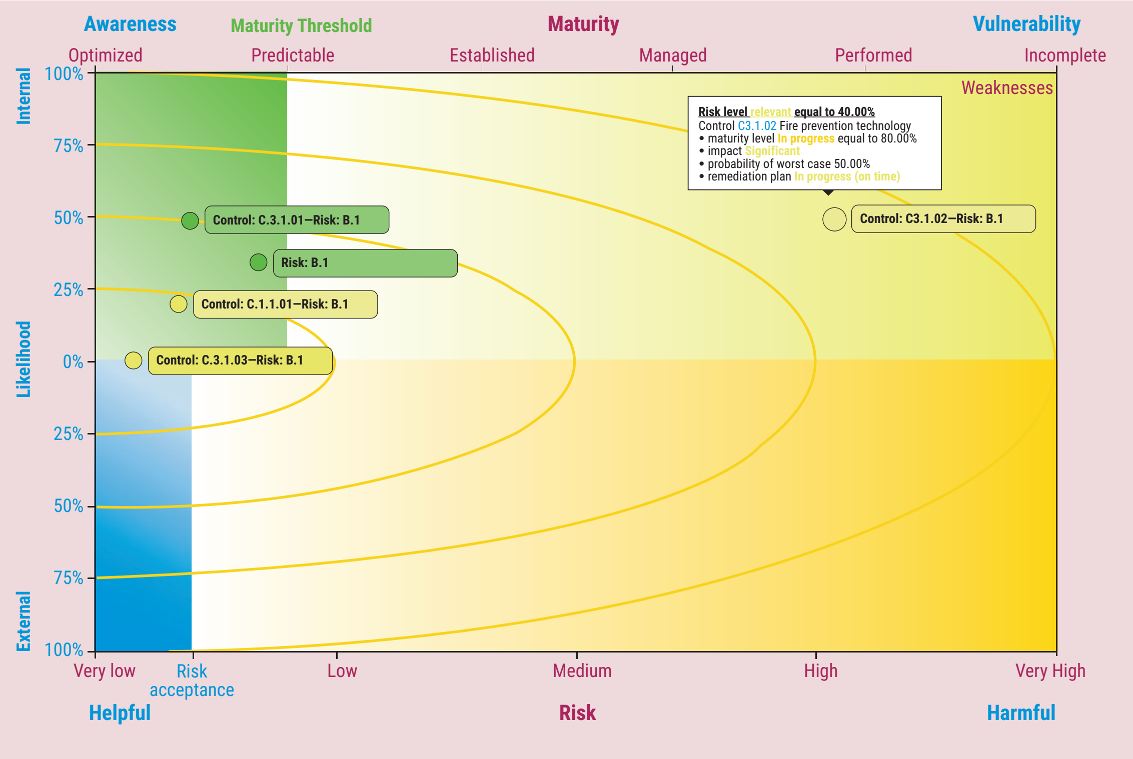
Similar to risk factors, controls are represented by the value of their maturity level (**figure 6**). On the upper ordinate, the maturity level scale is represented, along with a threshold to define the level of expected maturity—in other words, the maturity goal to be achieved. Beyond this threshold, there are opportunities to take advantage of strengths that can be improved to achieve business objectives. The lower levels of maturity are in the domain of vulnerabilities.

Regardless of whether risk factors or the implementation of controls are being presented, this type of graph can provide all the details necessary. The meaning of bubbles in the graph changes slightly when they represent risk factors rather than controls. It is sufficient to refer to the upper abscissa for evidence of the maturity level of controls, whereas the lower abscissa provides the risk-level scale.

Bubbles are likely to concentrate around the zero-probability ordinate, between the expected maturity level and the risk acceptance threshold on the abscissa. This area will be very crowded, making the identification of individual bubbles difficult. This is not a problem, however, because values in that area correspond to the expected situation of normality and the achievement of objectives, thus requiring no attention or intervention. Zero probability represents the chance of the worst case (not the best case) occurring, so enterprises need to start worrying only when the bubbles begin to move away from the center line of the graph, where a large area with great visibility is available to identify both emergency situations and opportunities to be seized.

By means of colors and the positioning of bubbles, this type of graph highlights with great clarity risk situations with significant impacts and problems with the implementation of countermeasures. At the same time, it allows an understanding of whether an activity is aimed at improving internal processes or addressing external factors.

Figure 6—Graph of a Risk and Its Controls



The header area should provide all the data necessary to understand the selected application perimeter (i.e., the portion of the enterprise affected and what risk factors or controls are involved), without invading the area of the graph dedicated to analysis.

Some Implementation Considerations

There is an obvious difference between the scale of maturity levels in the graphs presented and the related maturity levels used in data recording. The graphs use a standard list of reference names for maturity and are built with a linear distribution of values. Data entry is managed by individuals who are not interested in knowing or learning a formal set of names that is irrelevant to their work. To avoid unnecessary training, data entry uses a series of self-explanatory labels with emphasis on some names, but not others (nonlinear distribution).

The formulas use a normalized set of values that range from 0 to 1. A practical method of managing differences in the set of labels is to use two conversion tables equipped with threshold values to define the transition to an upper level (**figure 7**). This choice provides great flexibility in the fine-tuning of the system.

It is possible to introduce additional information, but this is advisable only for particular representations to avoid weighing down the graph. For example, it might be necessary to represent the state of risk at the country level and all the relevant entities, such as production sites, research and development centers, warehouses, offices, and headquarters. This requirement can be met by adding another column in the graph data set to define the bubble shape.

Normally, bubbles contain two pieces of information: the diameter, defining impact and the color, indicating progress of the work. To change the shape, the entity type can be identified by a central icon (e.g., a character with a special font) contained in the bubble rather than using a geometric shape to replace the circumference (such as markers used in maps).

Conclusions

The graphs presented here can display a series of risk factors or controls to top managers, highlighting situations that require action based on the severity of the indicator and reducing the visibility of less significant situations.

Figure 7—Conversion of Labels by Maturity Level

Graph Maturity Level			Data Entry Maturity Level		
Label	**Score**	**Maximum Threshold**	**Maximum Threshold**	**Score**	**Label**
Optimized	1.00			1.00	Optimized
			0.97	0.95	Compliant
Predictable	0.80	0.90	0.85	0.80	In progress
			0.75	0.70	Planning
Established	0.60	0.70			
			0.60	0.50	Partially done
Managed	0.40	0.50			
			0.40	0.30	Noncompliant
Performed	0.20	0.30			
			0.15	0.10	No info
Incomplete	0.00	0.10			

Despite the possibility of a large number of risk factors and controls being presented, with most of the results concentrated around the average value, the clarity and completeness of key information can be guaranteed without falling into excessive complexity. In particular, high-impact information can be presented very effectively.

This same representation technique can be adapted for any control framework starting from the CMM. The technique involves the systematic normalization of all values used in the assessment, ranging from 0 to 1. Then, any control framework can be transferred to this graphic representation.

With this proposed assessment methodology and graphic display technique, it is possible to effectively represent the distribution of risk factors without any loss of detail, while highlighting and giving priority to the main facts.

Endnotes

1 Sbriz, L.; "Enterprise Risk Monitoring Methodology, Part 1," *ISACA® Journal*, vol. 2, 2019, *https://www.isaca.org/archives*

2 Sbriz, L.; "Enterprise Risk Monitoring Methodology, Part 2," *ISACA Journal*, vol. 2, 2019, *https://www.isaca.org/archives*

3 Sbriz, L.; "Enterprise Risk Monitoring Methodology, Part 3," *ISACA Journal*, vol. 6, 2019, *https://www.isaca.org/archives*

4 International Organization for Standardization (ISO), *ISO 31000 Risk Management*, 2018, *https://www.iso.org/iso-31000-risk-management.html/*

5 CMMI Institute, *https://cmmiinstitute.com/*

6 AXELOS, ITIL—IT Service Management, *https://www.axelos.com/best-practice-solutions/itil/*

7 Institute of Internal Auditors North America, Standards and Guidance—International Professional Practices Framework (IPPF), USA, July 2015, *https://na.theiia.org/standards-guidance/*

8 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27001, *Information Technology—Security Techniques—Information Security Management Systems—Requirements*, 2013, *https://www.iso.org/isoiec-27001-information-security.html*

9 German Association of the Automotive Industry (VDA), "Information Security Assessment," *https://www.vda.de/en/services/Publications/information-security-assessment.html*

10 European Union, General Data Protection Regulation (GDPR), 27 April 2016

11 Madsen, D. O.; "SWOT Analysis: A Management Fashion Perspective," *International Journal of Business Research*, vol. 16, iss. 1, 2016, p. 39–56