Fraunhofer
IAO

FRAUNHOFER-INSTITUT FÜR ARBEITSWIRTSCHAFT UND ORGANISATION IAO

RISK VARIANCE IN IT SECURITY RISK ASSESSMENTS

Causes and mitigation possibilities

RISK VARIANCE IN IT SECURITY RISK ASSESSMENTS

Findings from nine interviews with security professionals and executives

Sebastian Kurowski, M.Sc. CISSP

Dr. Christian Schunck

Vivekanand, Vivekanand, B.Sc.

Fraunhofer-Institute for Industrial Engineering IAO
in Stuttgart.

Project number: 270013
Project partner: Zero Outage Industry Standard Ltd.

Table of Content

1
Management Summary

This report highlights the findings of nine interviews with IT-security professionals of IT driven companies. We have highlighted their risk assessment routines, influences of their risk assessments, the issue of risk variance, and how their organizations address this issue.

We found that all organizations employ risk assessments through a quasi-standardized way. Even when organizations did not use any public standards or good practices they relied on a repeatable, quasi-formalized way of conducting risk assessments. This was only not the case with one interviewee.

Risk assessments however seem to have a lasting impact on business and budget decision with all interviewees. All organizations showed impacts of the risk assessment outcomes on loss projections, and money reserve allocations. Some interviewees even mentioned that poor risk assessment outcomes can lead to the refusal of projects. Apart from this, risk assessments were also used for insurance and investment decisions. The assessment of IT-security risks therefore already reaches far beyond the domain of IT-security into the way business is being conducted.

This however can enhance the possible consequences of risk variances. Risk variance is the problem of varying outcomes e.g. due to situational or personnel changes in the risk assessment stakeholders (usually the assessors). And it has been observed by all interviewees in their organization as part of their risk assessment routines. The reasons for risk variance however varied based on the interviewee's role in the organization and their professional experience. We could identify the following reasons for risk variance:

- Affinity or aversion towards risks
- Domain of the assessor
- Knowledge of the domain affected by the risk
- Contextual understanding of the risk scenario
- Situation of the risk assessment

With varying reasons, mitigation mechanisms in the organization varied as well. However, we could identify four different groups of mitigation mechanisms. All four groups can together potentially reduce the amount of risk variance in the organization. Those four groups are:

- Capability streamlining
- Process generalization
- Quality control of outcomes
- Inter-disciplinary communication

Capability streamlining can be achieved using assessment centers for selecting the risk assessors, or by training the assessors.

Process generalization can be achieved by standardizing the risk assessment process, strongly formalizing this process, applying supporting tools, defining thresholds & metrics, and by applying good practices.

Quality control of outcomes could be supported through the regular review of processes, the yearly recurrence of the assessment against a documented baseline, the

ultimate decision making by the CEO, or the bias identification and adjustment by the senior management.

Finally, inter-disciplinary communication in the risk assessment can be supported through meetings on discrepancy resolving, or through pro and con discussions with domain experts in which the experts try to take the point of view of other domains.

There may be further mitigation mechanisms and reasons for risk variance in organizations. With nine interviews the sample has been comparatively small. However, the professional experience of the interviewees and the different professional experiences involved indicate generalizability of these findings. So while the reasons and mitigation mechanisms may be incomplete, it is probable that future research may not contradict our findings.

2
Study methodology

2.1
Goals of this study

The main purpose of this study was to shed light on the problem of risk variance. Risk variance describes the variation of assessed risks based on contextual, individual, and other factors. Such factors can for instance be related to the assessors, changing situations (e.g. changing threat landscape, changing customers) or the presentation of risk classes.

This problem has been, as to our knowledge, not yet examined. Therefore, this study should contribute to shed light on the existence of, reasons, and mitigating mechanisms for risk variance in organizations.

2.2
Data capturing methodology

We used semi-structured interviews in order to achieve this goal. Semi-structured interviews follow a clear guideline but allow interviewers and interviewees to deviate from the topics slightly. This entangles the very nature of explorative research into confirmatory research. Rather than focusing on whether our original assumptions regarding risk variance are right or wrong, we were thus able to further discuss how this issue is dealt with in organizations, and capture further aspects of risk variance that we were not able to see before the interviews.

The interviews were conducted with nine interviewees with expertise on their organisations risk management procedures from managerial and executive backgrounds in nine different companies.

2.3
Analysis methodology

All interviews were recorded with the consent of the interviewees and transcribed. Interviewees were provided with their interview transcripts for approval. After approval of the transcripts the recordings were deleted.

Analysis of the interviews was done through Qualitative Content Analysis[1]. This method foresees that the interview transcripts are analysed with pre-defined categories in mind. These categories are shown in Figure 1. This results in the reduction of interview content towards the most relevant content for further analytical use. However, such reductions may always yield the danger of relevant information being lost. In order to minimize this danger, content analysis of all interview transcripts was carried out

[1] Margrit Schreier u. a., „Qualitative Content Analysis: Conceptualizations and Challenges in Research Practice—Introduction to the FQS Special Issue" Qualitative Content Analysis I" ", in *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, Bd. 20, 2019; J Glaser und G Laudel, *Life with and without coding: Two methods for early-stage data analysis in qualitative research aiming at causal explanations. Forum: Social Qualitative Research, 14 (2). ISSN 1438-5627*, 2013.

independently by two separate researchers. Both researchers identified information for the pre-defined classifications. These were then consolidated.

Question no	Question Phrasing	Classification	
		Name	**Description**
Risk assessment procedures in the organization			
1	*How are business and information security risks assessed in your organization?*	Used Standards	Name of the standards that are used as part of the risk assessment
		Use of Standards	Role that these standards play in the risk assessment (e.g. as a baseline)
		Risk aspects at play	Parts that are considered as related to the IT security risk
		Weight / size of risk	Quantified or Qualified risk values
		Process	Participants, tasks and their execution order
2	*What conditions trigger a risk assessment?*	Irregular triggers	Irregular events that result in a (re-)assessment of risks
		Regular triggers	Regularly occuring events that result in a (re-)assessment of risks
3	*How regular are risk assessments of the same risk or the same matter repeated?*	Timespan	Regularity of reassessments
4	*What impact do the risk assessments have on general money matters in your organization? (E.g. the organization's profit and loss statements, balance sheets, or budgets)*	Influencing relationship	Is there an influence on any money matters?
		Type of influence on money matters	How are money matters influenced?
		Influenced aspects of money matters	What kind of money matters are influenced?
5	*For what other purposes are risk assessments used in your organization? (E.g. selection of countermeasures, or design of implementation projects)*	Name of Purpose	Name of the purpose for which a risk assessment is used
Risk variances in the risk assessment procedures			
6	*Could the outcomes of your risk assessments vary depending on the assessing individuals? (For instance due to loss aversion, risk affinity, or uncertainty avoidance)*	Existence of Risk Variance	Existence or in the past observed variances of risk assessments
		Reason for Risk Variance	Assumed reasons for varying risk assessments
6a)	*If yes, how does your organization deal with varying risk assessments?*	Name of Measure	Measure to limit the outcome of varying risk assessments
6b)	*If no, can you point us to the characteristics of your risk assessment process that avoid variations in assessments?*	Name of Measure	Measure to avoid the outcome of varying risk assessments
7 .. 8	**Questions on security behaviors outside of the scope of this analysis**		
Demographic questions			
9	*How do you describe your current role and responsibilities in your organization?*	Name of Role	Name of the role
		Information security related tasks	Tasks with relation to security if not implied by the role
10	*Could you briefly summarize your professional experience?*	Information security or IT Experience	Experience in years on security/IT or security/IT related topics
11	*How important is information security for your organization in light of other business aspects, such as business goals, drivers, shareholders, etc.?*	Relevance of information security	Order of relevance of information security in the organization
		Relativization of information security	Relativization of information security relevance order in light of other topics or personal opinion of the interviewee

Figure 1 Categories used for content analysis of the interview transcripts

Additionally, demographic questions regarding the value of information security in the organization, and the professional experience and role of the interviewee were analysed. We assume that observable continuity of risk variances, reasons and mitigation mechanisms under different security values and / or professional backgrounds could contribute to the generalizability of these results even in spite of the small observed sample (n = 9). However, even if continuity is not observable, demographic properties of interviewees could possibly provide an insight into whether these properties influenced their responses.

2.4 Questionnaire layout

The questionnaire was structured by four different topics: (A) Risk assessment procedures in the organization, (B) Risk variances in the risk assessment procedures, (C) Security behaviours, and a demographic section (D).

(A) included questions on how the organization conducts their IT security related risk assessments, including relevant standards, quantification or qualification, organizational impact, recurrence, etc. Accordingly, the questions included in this category were:

- How are business and information security risks assessed in your organization?
- What conditions trigger a risk assessment in your organization?
- How regular are risk assessments of the same risk or the same matter repeated?
- What impact do the risk assessments have on general money matters in your organization? (E.g. the organization's profit and loss statements, balance sheets, or budgets)
- For what other purposes are risk assessments used in your organization? (E.g. selection of countermeasures, or design of implementation projects)

(B) targeted the existence of varying risks, and interviewees opinions on reasons for risk variances. The main question in this category was:

- Could the outcomes of your risk assessments vary depending on the assessing individuals? (For instance, due to loss aversion, risk affinity, or uncertainty avoidance)

If interviewees had observed varying risks in their organization in the past, they were additionally asked the following question in order to identify any measures able to minimize risk variances:

- If yes, how does your organization deal with varying risk assessments?

If, however an interviewee had not observed varying risks in their organization, they were asked to characterize what may prevent their risk assessments to vary:

- If no, can you point us to the characteristics of your risk assessment process that avoid variations in assessments?

But this question was not asked since all respondents claimed to have observed risk variances in their risk assessments.

(C) included questions on security behaviours, which are not used as part of this analysis and therefore omitted in this report.

Finally, (D) included demographic questions which were asked at the end of an interview. These questions aimed at gathering information on the domain knowledge and the current role of the participant in the organization, since views on processes, people and IT may be subject to change based on who is looking at them. Additionally, participants were asked to put the emphasis on security in their organization in relation to other business goals. With this approach we wanted to find out about the importance of security in the organization, while avoiding false over-emphasizing of the importance by interviewees by relating it to other, possibly more valuable or tangible goals.

Therefore, the demographic questions included the following items:

- How do you describe your current role and responsibilities in your organization?
- Could you briefly summarize your professional experience?
- How important is information security for your organization in light of other business aspects, such as business goals, drivers, shareholders, etc.?

3
Risk assessments within the participating organizations

3.1
The role of standards in risk management

Standards and good practices only seemed to play a minor role when participants described risk management in their organization. One interviewee mentioned the ISO 27001 as a foundational standard of their risk management, however also remarked that it is insufficient ("We found out that if you look into customer requirements and map these to 27k ISOs, it's very weak. You know, it wasn't good enough."). Another interviewee mentioned the ISO 27001 and 31000 standards along with the COBIT risk tool and scenarios as foundational parts of their risk assessments.

Standardized risk management processes, although not explicitly driven by public standards and good practices, still seem to be prevalent in most interviewed organizations. For instance one interviewee mentioned that they apply their clients risk management procedures, and another one referred to company good practices. Another one described a hierarchical abstraction and consolidation scheme, which sounded similar to the recommendations of the NIST Special Publication 800-30.

Only one interviewee mentioned that their risk assessments are not standardized but that "…actually we invent the wheel when [conducting risk assessments] every time again, so to say.".

3.2
Risk assessment processes in the participating organizations

Interviewees were asked to describe how their organization conducts risk assessments. The following Table 1 provides an overview of the responses. Most organizations conduct risk assessments with different risk aspects in mind. Except for three interviewees all mentioned multiple risk aspects including business risks, organizational risks, market risks and customer risks to be taken into account when conducting IT security related risks.

Of those three interviewees that did not mention multiple risk aspects, two interviewees referred to risk aspects such as application downtime and business continuity which was the main driver of damages to their business model. Therefore, the focus on only one risk aspect in this case does not seem to be due to immaturity of the risk assessment process itself, but due to the organizations business model.

This shows that most participating organizations do not regard the assessment of IT security related risks as an isolated issue in their organization but take the relationship between IT security risks and business model focused risks into account. Accordingly, business impact, financial impact, or liability driven financial impacts where mentioned by most interviewees as impact definitions.

Quantitative assessments are preferred over qualitative assessments. However, when these are conducted through expert judgement, e.g. as a percentage value, the value of quantitative over qualitative impact definitions probably lies in the ease of communication of the impact assessment. After all numbers are usually known as part of basic literacy. Therefore their (interval) definition must not be communicated along with the impact assessment in order to be understandable.

The same holds for the probability definitions. These are mostly quantitative, however two interviewees mentioned that they use mostly expert judgement and only rely on data if it is available.

Definition of Risk			
Impact	**Probability**	**Risk aspects**	**Process**
Based on Business Impact	Quantitative under national legislation rules	Business risk, IT security risk, Organization specific integration	ISO 27k based process
Financial Impact	No information	Security risk, Privacy risk, Financial risk, Price risk	No information
Financial Impact whenever possible	Semi-quantitative / Quantitative when possible	IT Security risk	Streamlined reporting through third party tool up to supervisory board
Quantitative based on expert judgement or data if available	Quantitative based on expert judgement or data if available	IT Security risk, Business risk regarding customer service, Internal risk, Sales service risk, Delivery risk, Production risk, Marketing risk, Quality risk, IT risk	Unit based reporting through standardized spreadsheet solution; Consolidation along hierarchy
Qualitative	Qualitative	IT security risk, Business risk, Merging of risks from middle management upwards	Peer review of assessments; re-assessment at next level; report compilation at highes level
Depending on client risk management procedures	Depending on client risk management procedures	Application downtime	Depending on client risk management procedures
Financial through liability	No information	Technical risk, Financial risk	No standardized process
No information	No information	Supplier risk, Partner risk	Bottom up risk analysis, Top down structural analysis
Financial	Percentage point value through expert judgement	Business continuity risk	Checklists and templates

Table 1 Characteristics of the risk assessment process in the participating organizations

Most of the organizations conduct regular re-occurring risk assessments (see Table 2). The regularity of risk assessments varies between quarterly and annual assessments. However, two organizations do not foresee a regular occurring risk assessment. One interviewee mentioned that risk assessments are done with every task type change and every project initiation, meaning that they are done irregular but often. Another interviewee mentioned that assessments are conducted in the case of product vulnerabilities, product bugs, and the on- and off-boarding of clients which indicate a rather often occurring assessment as well.

Therefore, all participating organizations seem to conduct risk assessments often. But what about risk assessments for changing circumstances? Only one interviewee told us that they do not conduct any risk assessments in the case of changing circumstances, but only conduct their assessments as part of an annually re-occurring process. All other interviewees indicated that external events, e.g. new threats, process changes,

employee-based risk identifications, and basic changes in client relationships (on- and off-boarding) lead to risks being re-assessed.

Triggers for risk assessments		Influence of assessment outcomes on…	
Conditions	**Regularity**	**…money matters**	**…other uses**
ISO Re-assessment; External events; Customer requirements;	Annually	Yes but not consistent across the company	Security technology investment decisions; Architecture design
Project initiation; Task type changes	Irregular	Influence on project acceptance or refusal decision	Security technology investment decisions; Chinese wall policy implementation
Change management; Incident management; … Every process event	At least yearly; Monthly discussion	Only for top risks but currently in expansion	Security technology investment decisions; Security budget decision; Data privacy decisions; Compliance decisions;
None	Annually	Direct influence on P&L[1]	Security technology investment decisions; Business decisions; Budget decisions; Privacy decisions
Risk identification by employees	Regularly within undefined period of time	Financial impact definition	Securiy technology investment decisions; Insurance decisions; IT infrastructure change decisions
Depends on clients	Depends on clients	Financial impact definition	Decisions on high availability; Disaster recovery decisions (e.g. on RPO[2] and RTO[3])
Product vulnerabilites; Product bugs; On- and off-boarding of clients	Irregular	Influence via money reserves	Mitigation method adjustments; Service offering design
No information	Quarterly	Influence on projected lossess	Organizational matters
On-boarding of clients	Bi-annually	Budget allocation for risks	Security technology investment decisions; Budget decisions; Insurance decisions;

Table 2 Risk assessment regularity, triggers, and the use of outcomes

All organizations use their risk assessment to determine losses. These losses are mostly directly applied to budget decisions. One interviewee even mentioned that a risk assessment could potentially "…make a loss-company out of a profit-company". Only

[1] Profit & Loss – Usually statements that indicate the companies profits and (projected) lossess

[2] Return-Point-Objective – A definition of the maximum temporal amount of tolerable data loss

[3] Return-Time-Objective – A definition of the maximum required timespan until a service or application should be recovered

Risk assessments within the participating organizations

few companies apply their assessment inconsistently or only for the top risks on their profit and loss projections.

Additionally, most organizations use their risk assessment outcomes for security technology investment decisions and budget decisions. Decisions regarding disaster recovery procedures were mentioned by one interviewee. And some interviewees mentioned that the risk assessments are actively used in business decisions. For instance, an interviewee told us projects can even be refused based on poor outcomes of a risk assessment.

This shows that risk assessments play a central role in organizations, with influences into the organization far beyond the domain of IT-security. This however could increase the significance of unreliable risk assessment outcomes, e.g. due to individual biases.

4
On varying risk assessments

4.1
A definition of risk variance

Risk variance describes the varying outcomes of risk assessments based on dispositional and situational factors. Prior to the interviews we assumed possible reasons for varying risk assessments could be due to the…

- …presentation of risk classes and / or risk scenario orders and overviews[1],
- …individual affinity or aversion towards specific risk scenarios[2],
- …tendency of regarding known risk scenarios as more significant than those that are unknown[3],
- …tendency of regarding risks that apply to oneself or those around oneself as less likely than those that apply to others[4].

We further assumed that any risk assessment, at least due to the interpretivistic character of any assessment regarding a future event[5], should be biased by observable variances between different assessments of the same risk. The interviews proved this assumption to be correct. Table 3 shows that all interviewees have observed risk assessments to be varying.

4.2
Reasons for varying risks

The factors which interviewees saw as reasons for the varying risk assessments however included risk affinity or aversion, knowledge of the domain, understanding of psychology, empathy, professional background, domain of work, contextual understanding, personality and the situation of decision-making.

Surprisingly the professional domain was mentioned as a reason for risk variance by three different interviewees. One interviewee mentioned that IT security people might have a focus on exploits but not on topics like emergency crisis management or

[1] Robert M Nosofsky, „Information integration and the identification of stimulus noise and criterial noise in absolute judgment.", *Journal of Experimental Psychology: Human Perception and Performance* 9, Nr. 2 (1983): 299; Aaron S Benjamin, Michael Diaz, und Serena Wee, „Signal detection with criterion noise: applications to recognition memory.", *Psychological review* 116, Nr. 1 (2009): 84.

[2] Daniel Kahneman und Amos Tversky, „Prospect Theory: An Analysis of Decision under Risk", *Econometrica* 47, Nr. 2 (März 1979): 263, https://doi.org/10.2307/1914185; Konstantinos Mersinas, „Risk Perception and Attitude in Information Security Decision-making" (PhD Thesis, Royal Holloway, University of London, 2017).

[3] Itzhak Gilboa und David Schmeidler, „Maxmin Expected Utility with Non-Unique Prior", *Journal of Mathematical Economics* 18, Nr. 2 (Januar 1989): 141–53, https://doi.org/10.1016/0304-4068(89)90018-9; Mersinas, „Risk Perception and Attitude in Information Security Decision-making".

[4] Danièle Hermand u. a., „Risk target: An interactive context factor in risk perception", *Risk Analysis* 23, Nr. 4 (2003): 821–828.

[5] Richard Baskerville, „Risk analysis as a source of professional knowledge", *Computers & Security* 10, Nr. 8 (1991): 749–764; Niklas Luhmann, „Technology, environment and social risk: a systems perspective", *Organization & Environment* 4, Nr. 3 (1990): 223–231.

business continuity. Other interviewees stressed the different views between Chief Financial Officers (CFO) and Chief Information Security Officers (CISO) stressing that the CFO "…didn't see the importance of the security as the [CISO] did." Instead the"…CFO was more interested in reducing […] expenses related to what the [CISO] office was demanding.".

On varying risk assessments

The contextual understanding of a risk scenario was mentioned by two interviewees. One mentioned that a risk assessor can have a different understanding on the services that are provided to customers, how valued the customers are, etc. Another interviewee even mentioned that "sometimes business and sales tell you this is a must win. So then risk is looked at differently.".

Risk variance observed?	Reasons
Yes	Risk affinity; Domain knowledge; Situation of risk assessment
Yes	Individuals
Yes	Domain
Yes	Individuals; Domain
Yes	Contextual understanding
Yes	Domain
Yes	Risk aversion; Contextual understanding
Yes	Risk aversion
Yes	Personality; Situation of risk assessment

Table 3 Interviewee responses on risk variance observations and reasons for varying risk assessments

Knowledge of the domain which is affected by the risk scenario, and an understanding of psychology and empathy in order to "…ask the right questions in the right way and the right times" was mentioned by one interviewee. Interestingly domain knowledge was not mentioned by any other interviewee. However, being able to ask the right questions seems to be related with the situation of decision-making, that has been mentioned by another interviewee. This interviewee claimed that the risks vary based on who it is and also how the decision is made, e.g. after detailed discussions or as an ad-hoc decision. We therefore noted the understanding of psychology and the situation of decision making both as the situation of the risk assessment in Table 3.

Finally, individual differences and personality was mentioned by three different interviewees without further details on the specific traits. For instance, one interviewee mentioned that "…managers have very different personalities…", another one told us that the assessment itself is an "…individual decision.".

4.3 Generalizability of risk variance occurrence and reasons

So, can we assume that varying outcomes of risk assessments is a general issue in risk assessments? There are multiple indications that point towards this assumption. For instance, Baskerville argues in his stance on organizational risk assessments, that these are interpretivist in nature[1] which includes that the outcomes of these assessment depend (at least partly) on the assessors.

One possibility to argue for the general prevalence of risk variance in assessments would be through selectively sampling the respondents. However, these interviews were conducted among volunteering interviewees from companies associated with the Zero Outage Association. Thus, the sample mainly involves companies which emphasize

[1] Baskerville, „Risk analysis as a source of professional knowledge".

security in some ways. Selectively sampling interview partners would increase the timespan of the conducted interviews. The finding of risk variance is significant, it constitutes a problem, however it does not hold any prescriptive or descriptive character of risk variance. So, the value in generalizing risk variance occurrence methodologically would be limited.

This is different for the reasons of risk variance. They hold a descriptive character and can provide an insight into the influencing factors of risk assessment quality. In order to provide a stance on generalizing risk variance reasons, we will thus focus on the differences in the sample. The questionnaire layout (see Section 2.4) included demographic questions for this reason.

Table 4 shows the differences in the demographic responses of the interviewees with regard to the reasons for risk variance they mentioned.

Risk affinity or risk aversion is being mentioned by most interviewees. However, it is only mentioned with high, very high, and in one case an unclear assessment of the importance of security in the organization. It is also independent from the IT security focus of these interviewees' professional experiences. It seems hardly surprising that risk affinity or risk aversion seems to play a role when observing risk variances in organizations with high and very high importance of security. The breadth of possible discussed risk scenarios could be much larger in these companies, unveiling risk affinity or aversion towards certain scenarios more easily.

Interestingly, knowledge of the domain of a risk scenario was only mentioned by one interviewee from a security framework implementation perspective in a company with high importance of security. But if considered together with the contextual understanding of a risk scenario, it spans beyond IT scenarios and is observed with organizations that emphasize security both highly and very highly. It could be that domain-unknowing risk assessors that assess risk scenarios under naïve or overly pessimistic scenarios are more observed with organizations that put more emphasis of risk assessments in more parts of the company, due to the high or very high importance of security. This would also explain why the contextual understanding is also observed by the interviewee with customer representative and management of outsourcing experience.

Reason for Risk Variance	**Professional Experiences of Interviewees**	**Importance of Security**	**Roles**
Risk affinity / Risk aversion	Infrastructure Management, IT, Security Management; Customer representative, Management of outsourcing; Executive Level Consultant	High, among top priorities; Very high, almost religious; Unclear;	Global Transformation manager concerned with security framework implementation; Global client director; Executive Level Consultant
Domain knowledge	Infrastructure Management, IT, Security Management	High, among top priorities	Global Transformation manager concerned with security framework implementation
Contextual Understanding	IT-Security in industry, Teaching IT-Security as professor; Customer representative, Management of outsourcing	High, among top priorities; Very high, almost religious	Security framework designer; Global client director
Situation of risk assessment	Infrastructure Management, IT, Security Management;	High, among top priorities; Very high, existential	Global Transformation manager concerned with security framework implementation; CEO and founder

Reason for Risk Variance	Professional Experiences of Interviewees	Importance of Security	Roles
	Software Development, Software Testing, Quality Assurance		
Domain	Process Management, Change Management, Incident Response, Security Management; IT, Enterprise Architect, High Availability Computing; Software development, Project Management, IT Management, CIO	High, among top priorities; High with relation to clients; Medium	Security Officer; Owner; Vice president
Individuals	C-Level Management, Directory of Security Institute; Software development, Project Management, IT Management, CIO	High, among top priorities; Medium	Senior manager with security background; Vice president
Personality	Software Development, Software Testing, Quality Assurance	Very high, existential	CEO and founder

Table 4 Mentioned reasons for risk variance and demographics of the interviewees

The processual situation in which the risk assessment (Situation of risk assessment) is conducted in, is also mentioned together with a high and very high importance of security and by interviewees with management and quality assurance experience. The professionally influenced focus on processes of these interviewees may lead to this observation.

The domain of the assessors on the other hand also played a role with medium, high, and customer-focused high importance of security in the companies. It is observed by security management, Enterprise Architecture, and executive level management professionals. Such professions usually cooperate with various individuals from different domains. The different thought approaches, e.g. of law, psychology, sociology, business management and computer science could yield different conclusions. This however can only be observed by individuals that have worked with different domains as for instance security managers, executive managers, or enterprise architecture managers.

All mentioned reasons for risk variance so far seem to be attributable to the interviewees capability of observing them. The variance between the different professional experiences and the importance of security all align well with the mentioned reasons. The claim of generalizability thus is almost of esoteric nature. Since we can conclude that:

> *Risk affinity or aversion towards risk scenarios, knowledge of the domain that a risk scenario affects, contextual understanding of the risk scenario, the processual environment of the risk assessment, and the domain of the assessor seem to be general reasons for risk variance. If they are not observable it currently seems plausible that the reason for this lack of observation may be the lense of the observer and not the non-existence of the reason.*

With individuals, a less specific reason for risk variances was provided by two different interviewees from companies which regard security as high and medium important. Both are from executive management levels. Individuals as a reason for risk variance, however could include aspects such as risk affinity / aversion, knowledge of the

domain, the contextual understanding, the domain of the assessor, etc. As it possibly includes one or many of those aspects, varying with regards to the focus of the observer, individuals as a reason for risk variance is probably generalizable. But as its usefulness is limited, we have omitted this reason from further use.

The same holds for personality. This could encompass the mentioned reasons along with character traits. This lack of detail makes the personality probably a generalizable, but not useful, reason for risk variance. Therefore, this reason is omitted as well from further analysis.

4.4 Conclusion – Why do risk assessments vary?

The argument on the generalizability of risk variance reasons leaves the individuals affinity or aversion towards risks, the professional domain of the assessor, the assessors knowledge of the domain that is affected by the risk, the contextual understanding of the risk scenario by the assessor, and the processual situation that has led to the risk assessment. These reasons are visualized in Figure 2.

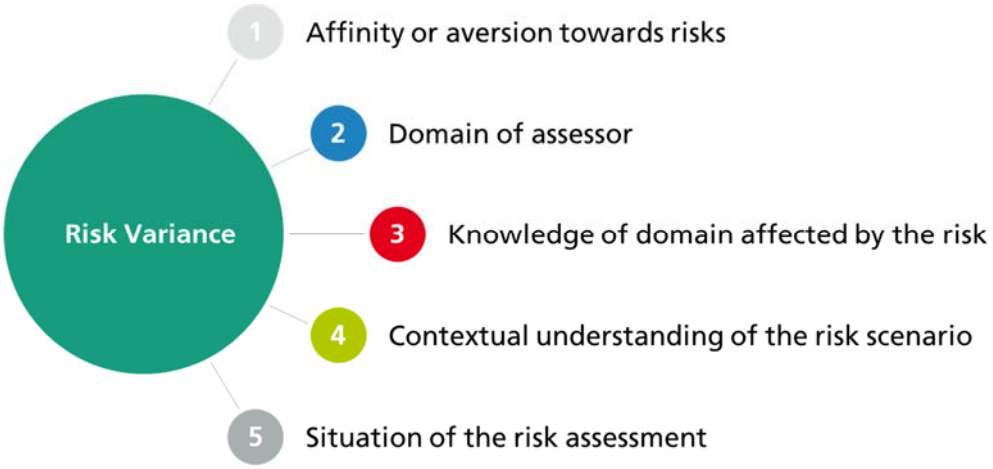

Figure 2 Reasons for risk variances

5
Mitigating risk variance

5.1
Mitigation mechanisms for risk variances

Along with the reasons for observed risk variances, interviewees where asked how their organization deals with varying risk assessments. Table 5 lists the mentioned mitigation mechanisms. The interviewee responses can be categorized in people focused, process focused and managerial mitigation mechanisms.

People focused mechanisms were seen in the use of assessment centers. This can streamline the expertise and competencies of the risk assessors. Also training of the assessors follows the same goal.

The risk assessment process should be standardized in order to avoid biases. This can also be achieved by a strong formalization of the assessment. Standardization and formalization can be supported using tools, defining thresholds, metrics, and by applying good practices.

The risk assessment process should foresee that decisions made in risk assessments are reviewed in case of organizational change.

Recurrence of risk assessments, e.g. a yearly recurrence again a documented baseline of past assessed risks could decrease risk variance. Finally, distinguishing between risk assessments of different risk parts was mentioned as a possibility to decrease risk variance. For instance, an assessment of continuity risks, could be done separately from assessments of privacy risks.

Type of mitigation mechanism	Mentioned mitigation mechanisms
People focused	Assessment centre
	Training of the assessors
Process focused	Standardization of the assessment
	Strong formalization of the assessment
	Review of decisions
	Use of Tools
	Definition of Thresholds & Metrics
	Application of Good Practices
	Risk type specific analysis
	Regular review of processes
	Yearly recurrence against documented baseline
	Meetings on discrepancy resolving
	Pro and Con discussions with domain experts
Managerial	Ultimate decision by the CEO
	Senior management bias identification and adjustment

Table 5 Mentioned mitigation mechanisms by participants

Process quality impacting mitigation mechanisms were also mentioned. For instance, an interviewee mentioned weekly meetings of the stakeholders in order to resolve discrepancies that came up through a risk assessment. Another interviewee mentioned that the outcomes of risk assessments were discussed in a pro and con discussion with domain experts. The CISO would argue on the financial viability of an assessed risk, while the CFO would reflect on its security impact. This dialectic inspired approach of

domain experts taking the point of view of the contradicting domain could help to resolve conflicts due to overly or underly assessed risks.

The managerial use of the CEO by letting him/her have the ultimate decision on the height of risks would transfer the risk variance problem towards a single, company leading party. On a broader scale, the senior management could be tasked with identifying biasing trends in the assessments and adjusting them.

None of the interviewees named the same mitigation mechanisms, although some similarities occurred. For instance, the definition of thresholds and the definition of metrics were each mentioned by one interviewee. This impacts the generalizability of mitigation mechanisms.

5.2 Generalizability of mitigation mechanisms

When comparing the mitigation mechanisms with the roles, professional experiences and importance of security in the interviewee's organizations, we were not able to identify any meaningful relationship. However, the risk variance reasons seem to be related to the mitigation mechanisms. The following Table 6 shows that mentioned mitigation mechanisms are implied well by the risk variance reasons. Reasons that concern the assessor's capabilities, such as domain knowledge are met with mitigation mechanisms such as assessment centres. Reasons that concern the assessor's characteristics, e.g. their professional domain are met with mitigation mechanisms, such as risk type specific analysis, discrepancy resolving meetings, or pro and con discussions.

This makes sense. Mentioned risk variance reasons were related to the interviewees professional experience, as section 4.3 suggests.

Mitigation mechanism	Risk Variance Reasons
Assessment centre	Risk affinity; Domain knowledge; Situation of risk assessment
Training of the assessors	Individuals
Standardization of the assessment	Risk aversion; Contextual understanding
Strong formalization of the assessment	Individuals
Review of decisions	Individuals
Use of Tools	Contextual understanding
Definition of Thresholds & Metrics	Domain; Contextual understanding
Application of Good Practices	Domain
Risk type specific analysis	Domain
Regular review of processes	Domain
Yearly recurrence against documented baseline	Individuals; Domain
Meetings on discrepancy resolving	Individuals; Contextual understanding; Domain
Pro and Con discussions with domain experts	Domain
Ultimate decision by the CEO	Risk aversion
Senior management bias identification and adjustment	Individuals; Domain

Table 6 Relationship between risk variance reasons and mitigation mechanisms

The reasons for risk variance may depend on the interviewees professional point-of-view on the organization. The observed mitigation mechanism may as well be shaped by this. However, some mitigation mechanisms share a common purpose such as assessment centres for assessor selection and training of the assessors. And thus, we cannot conclude on a generalizing effort with these mitigation mechanisms.

But by using the purpose of a mechanism for abstraction, we may provide a generalizable view on risk variance mitigation. Table 7 shows the mitigation mechanisms abstracted by their purpose.

Mitigation mechanism	Purpose
Assessment centre	Capability streamlining
Training of the assessors	Capability streamlining
Standardization of the assessment	Process generalization
Strong formalization of the assessment	Process generalization
Review of decisions	Quality control of outcomes
Use of Tools	Process generalization
Definition of Thresholds & Metrics	Process generalization
Application of Good Practices	Process generalization
Risk type specific analysis	Capability streamlining
Regular review of processes	Quality control of outcomes
Yearly recurrence against documented baseline	Quality control of outcomes
Meetings on discrepancy resolving	Inter-disciplinary communication
Pro and Con discussions with domain experts	Inter-disciplinary communication
Ultimate decision by the CEO	Quality control of outcomes
Senior management bias identification and adjustment	Quality control of outcomes

Table 7 Purposes of the mitigation mechanisms

These purposes are again aligned with the mentioned reasons for observed risk variance in Table 8. This shows a clearer indication between the purpose of the mitigation mechanisms and the risk variance reasons. Capability streamlining seems to be associated with the situation of risk assessments and domain knowledge. Of course, this also means that it is associated with the domain of the risk assessor.

Process generalization and inter-disciplinary communication both share joint risk variance reasons. However, process generalization seems to be further concerned with addressing risk aversion and individuals. Individual characteristics are also a focus of quality control of the outcomes of assessor decisions in risk assessments, therefore it makes sense that risk aversion, the domain of assessors and the individuals assessing are behind this purpose.

Purpose	Risk Variance Reasons
Capability streamlining	Risk affinity; Domain knowledge; Situation of risk assessment; Individuals; Domain
Process generalization	Risk aversion; Contextual understanding; Individuals; Domain
Quality control of outcomes	Risk aversion; Domain; Individuals
Inter-disciplinary communication	Individuals; Contextual understanding; Domain

Table 8 Relationship of mitigation mechanism purposes and risk variance reasons

While all singular risk variance reasons may not be individual to the mechanism purposes, some are (e.g. domain knowledge or the situation of risk assessment). Others are mutual between two purposes (such as Contextual understanding). Finally, the combination of risk variance reasons certainly is.

Therefore, we assume that Capability streamlining, process generalization, quality control of outcomes and inter-disciplinary communication provide a generalizable view on the risk mitigation mechanisms.

5.3 Conclusion – How can risk variance be addressed?

Mitigating risk variance

Risk variance can therefore be addressed by streamlining the capabilities of risk assessors, generalizing the process, controlling the quality of outcomes, and ensuring successful inter-disciplinary communication. Figure 3 shows how risk variance could be addressed. This problem should be approached by mitigation mechanisms for all four purposes. The named mitigiation mechanisms however are optional of course.

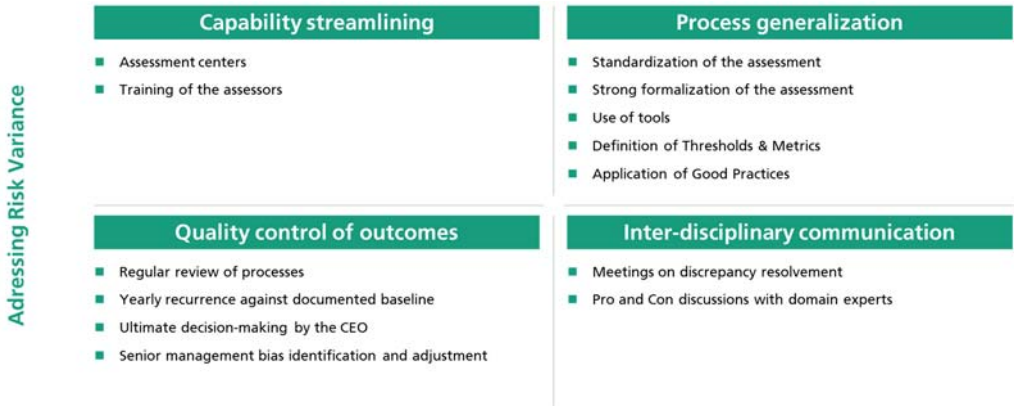

Figure 3 Mechanisms to adress risk variance