DANUBE UNIVERSITY KREMS

Department for E-Governance and Administration
Dr.-Karl-Dorrek-Straße 30
A - 3500 Krems

Master's Thesis
in the study programme
Professional MSc Management & IT
with a special focus on
Information Security Management

Working Title:

How to Design a Simple, Practical, and Probabilistic Assessment Method to Compute the Potential Financial Impact of Cyber and Information Security Risks?

SUPPLEMENTAL INFORMATION TO ENABLE EXPERT EVALUATION

created by
DI Gernot Kielhauser
gernot.kielhauser@edu.donau-uni.ac.at

TABLE OF CONTENTS

INTRODUCTION

In the field of IT risk management, various risk assessment methods are endorsed and promoted by several major organisations, frameworks, and standards, including (in random order) ISO/IEC 27005, NIST Risk Management Framework, ISACA's Risk IT Practitioner Guide, the Open Factor Analysis of Information Risk (FAIR), Risk Analysis based on IT Grundschutz, OWASP Risk Rating Methodology, or Center for Internet Security Risk Assessment Method (CIS RAM).

The majority of the extant approaches promote a qualitative assessment method which uses two different ordinal scales of qualifying attributes to describe the magnitude of potential consequences (for example, "Very Low", "Low", "Medium", "High" and "Very High" in Exhibit 1) and the likelihood that those consequences will occur (for example, "Rare", "Unlikely", "Possible", "Probable", "Highly Probable" in Exhibit 1).

Even if numbers are used to describe ordinal labels (i.e. use the number "4" instead of a verbal label like "high"), using them in mathematical operations (e.g. multiplying frequency and impact) to obtain a single risk score is misleading because they carry no real meaning except a quantitative scale/range. Therefore, a widely used approach to present risk is the creation of a two-dimensional diagram where the likelihood scale and the impact scale represent one dimension each. This diagram is usually called risk matrix and an example is visualised in Exhibit 1.

Ordinal Impact Scale	**Very High**	Moderate	Major	Major	Severe	Severe
	High	Moderate	Moderate	Major	Major	Severe
	Medium	Minor	Moderate	Moderate	Major	Major
	Low	Minor	Moderate	Moderate	Moderate	Major
	Very Low	Minor	Minor	Minor	Moderate	Moderate
		Rare	**Unlikely**	**Possible**	**Probable**	**Highly Probable**
		Ordinal Probability Scale				

Exhibit 1: An illustrative example of a risk matrix.

Risk matrices are deemed to be easy to create and easy to understand. They are used to communicate risks to senior management, as the outcomes of risk assessments usually inform some kind of business decisions (e.g. how much to spend on risk mitigation? How to prioritize the allocation of limited resources for an expanding list of risks? etc.). However, risk matrices do not provide any information related to the degree of certainty that risk estimations are accurate. When organisations rely on qualitative estimation methods, they have to realize that even with the establishment of explicit criteria, risk assessments are influenced by organizational culture and the personal experiences and accumulated knowledge of the individuals conducting the assessments. As a result, assessors of risk can reach different conclusions from the same information. This diversity of perspective can enrich the risk assessment process and provide decision makers with a greater array of information and potentially fewer biases. However, such diversity may also lead to inconsistent risk assessments.

It follows that the key factor that influences qualitative assessment results (and thus good decision making) is the accuracy of estimations done by assessors.

Research in the field of psychology has shown that there are different cognitive biases which influence the mental process of conducting an estimation and have a negative effect on the accuracy of the estimations. A few selected research results shall illustrate some unexpected implications when dealing with ordinal scales:

- For example, one illustrative study shows that the partition scheme of the scale has an effect on responses: On a scale of 1 to 5, the value 1 is chosen more frequently than on a scale of 1 to 10, even if "1" is defined identically in both cases.

- Another study showed that the verbal and numerical labelling of the answering categories has an effect on a respondent's likelihood of providing biased responses.

• Furthermore, the mere order in which scale labels are presented has an effect on respondent's choices even if the labels have a standard, objective, and context-free meaning.

Research in the field of decision analysis showed that the effectiveness of expert predictions can be improved even when no additional data is available: The decomposition of a problem statement (i.e. to split the problem into smaller segments; to make estimations for each segment; and to recombine these estimations in order to create an estimation of the superordinate problem statement) can improve the estimation accuracy for problem statements with high to extreme target values (i.e. any number having more than seven digits) when subjects were highly uncertain about the target value.

SCOPE OF THE MASTER'S THESIS

In this Master's Thesis the insights described above shall be used to propose and evaluate a **semi-quantitative, probabilistic Cyber and Information Security Risk impact assessment method** (see Exhibit 2 for a breakdown of I&T-related risk categories) in which problem decomposition and expert opinion is used to estimate the potential financial impact of given risk scenarios.

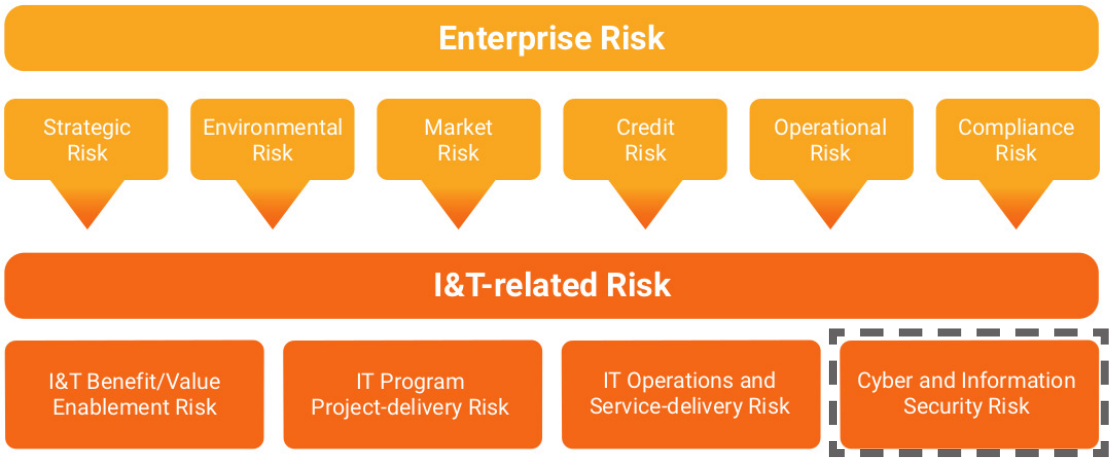


Exhibit 2: Scope of I&T-related Risk Relative to Other Major Categories of Risk
(retrieved from: ISACA Risk IT Framework 2nd Edition, Figure 1.1; emphasis added).

The proposed risk impact assessment method logically fits into any IT risk management process that, in general, conforms to the high-level process visualized in Exhibit 3.

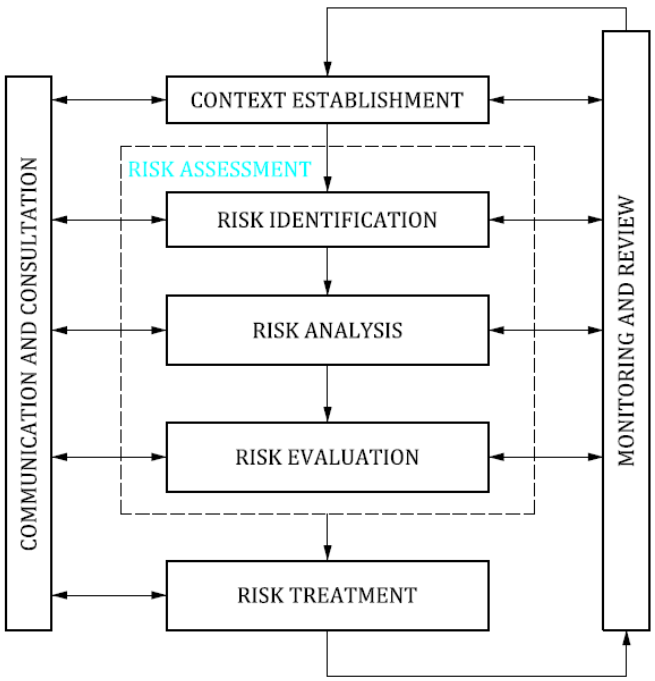


Exhibit 3: A high-level risk management process (retrieved from ISO/IEC 27005:2018, Figure 1).

Exhibit 4 shows a generic workflow of the tasks to be executed in such a risk management process. The tasks numbered 2.2 and 5.2 (highlighted with a solid blue frame in Exhibit 4) are in the direct scope of this study and further explained below. The tasks numbered 4 and 7 (highlighted with a dashed blue frame in Exhibit 4) are impacted by the proposed assessment method. Note that in tasks 2.2 and 5.2 also other forms of impact could (or should) be assessed, but for the purpose of this study the scope is limited to *financial* impact.

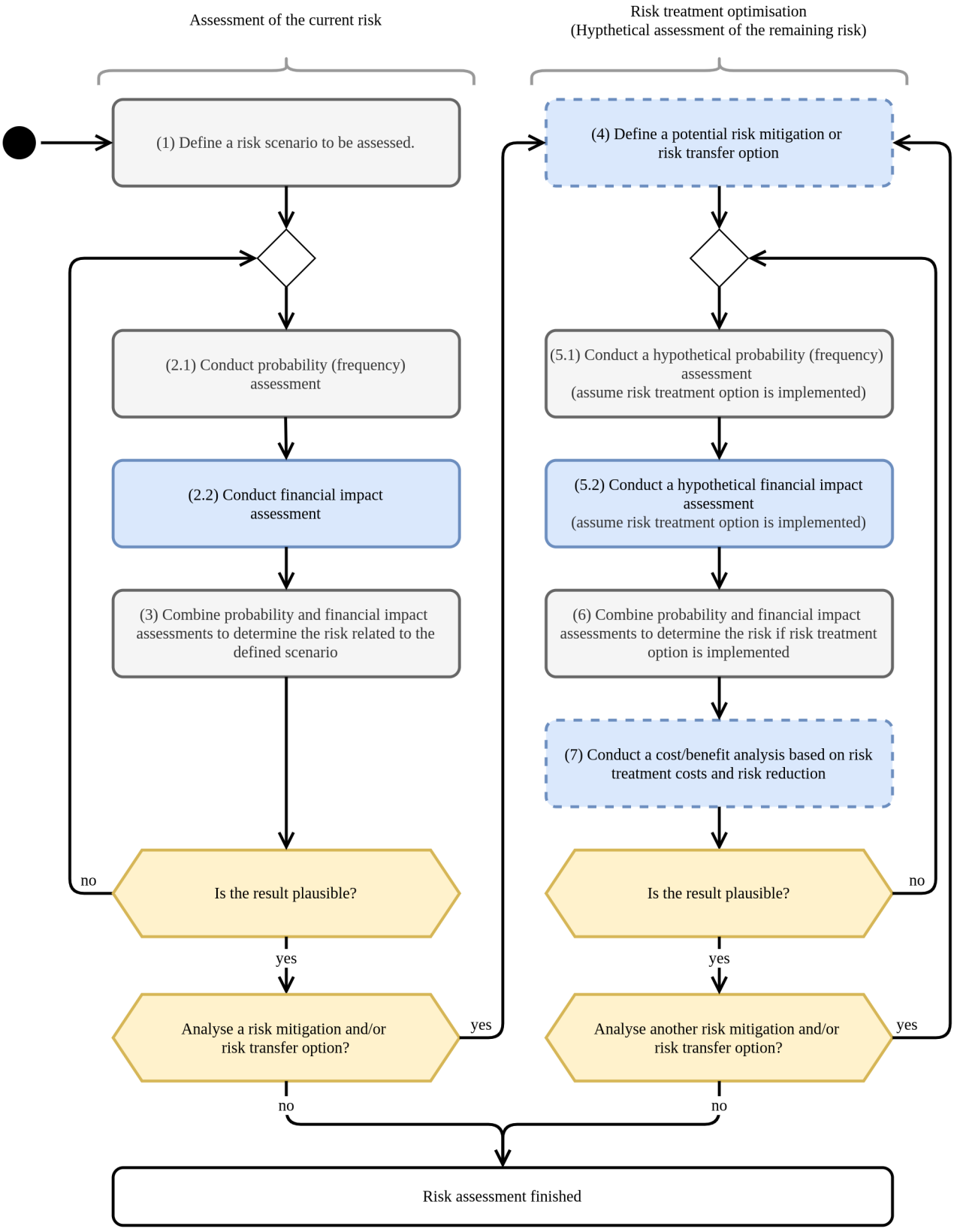


Exhibit 4: A generic task list to be carried out in the risk assessment process.

Tasks 2.1, 2.2, and 3 are used to assess the current risk related to the scenario specified in task 1. For each potential risk mitigation or risk transfer option available (defined in task 4), tasks 5.1, 5.2, and 6 are used to assess the respective remaining risk. Tasks 2.2. and 5.2 employ the very same assessment steps (details are discussed in the next section of this document) and the result of both tasks is a *quantitative measure of the financial impact* (one for the current and one for each risk mitigation or risk transfer option). The value of the assessed risk mitigation or risk transfer option equals the amount of risk reduction. In task 7 this value is determined and compared to the cost of the assessed risk mitigation or risk transfer option. This information may be used to support decisions on the selection and implementation of risk treatment options.

THE PROPOSED FINANCIAL RISK IMPACT ASSESSMENT METHOD

It was already stated above that the proposed financial risk impact assessment method shall use problem decomposition and probabilistic expert estimations to express the potential financial impact of given risk scenarios. The method shall be used to assess the impact of cyber and information security related risk (cf. Exhibit 2) which generally means the loss of confidentiality, integrity, and availability.

Proposed Decomposition Structure for Financial Risk Impact Assessment

Exhibit 5 on the next page visualises the proposed decomposition structure to be used for financial risk impact assessment. The structure was created in the following manner:

- A literature review was conducted to collect contributing factors that could be considered when estimating the financial impact of a risk scenario.
- The identified factors where clustered in order to obtain a streamlined set of factors.
- The result was a "flat" list which was used to create an initial draft of a hierarchical structure.
- Subsequently, the initial draft of the hierarchical structure was logically enhanced by the author resulting in the final decomposition structure shown in Exhibit 5.

The decomposition model clusters individual impact factors into three pillars, namely (1) costs related to incident response, (2) adverse business impact caused by the incident, and (3) violation of legal obligations.

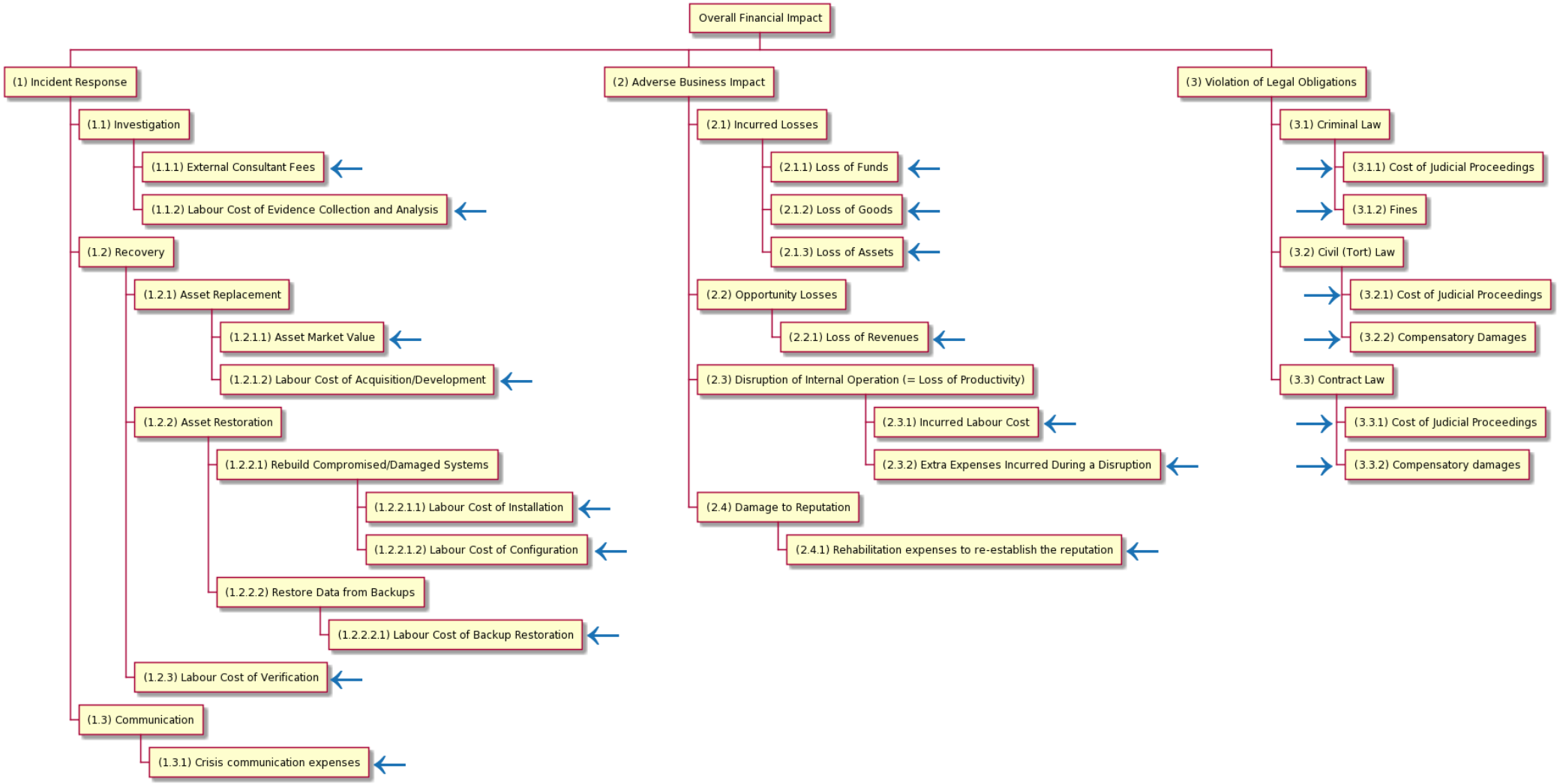
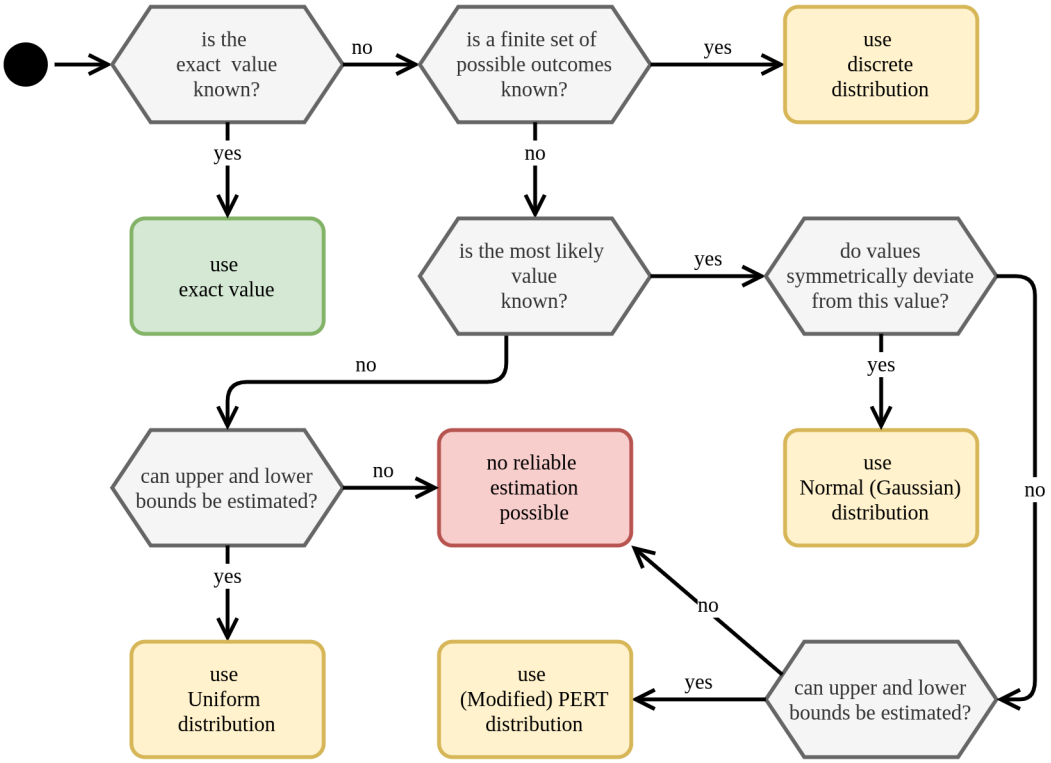


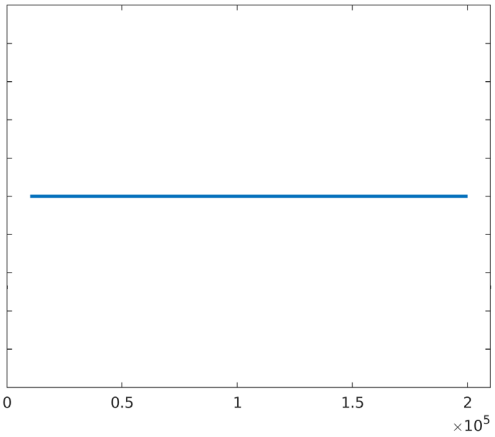
Exhibit 5: The proposed decomposition structure for financial risk impact estimation.

Available Probability Distributions to Express Expert Opinion

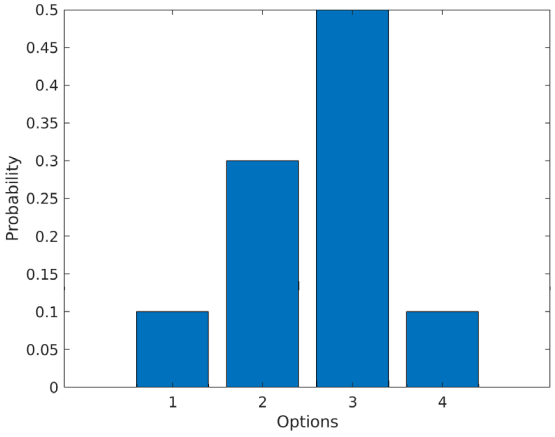
The available probability distributions are chosen based on the following decision flow:



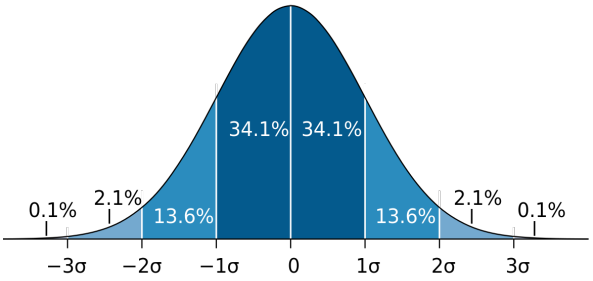
Uniform Distribution The uniform distribution is used when only an upper and lower bound can be estimated. Every value in the interval between these bounds is equally likely to occur. For example, if the subject matter experts estimates a lower bound of € 10,000 for the financial impact and an upper bound of € 200,000 each of these impact values (and all values in between) has the same likelihood to occur. For multiple iterations in the Monte Carlo simulation the impact value may vary up to ± € 190,000. Consequently, an increasing interval length (limited by the lower and upper bounds) implies an increasing uncertainty.



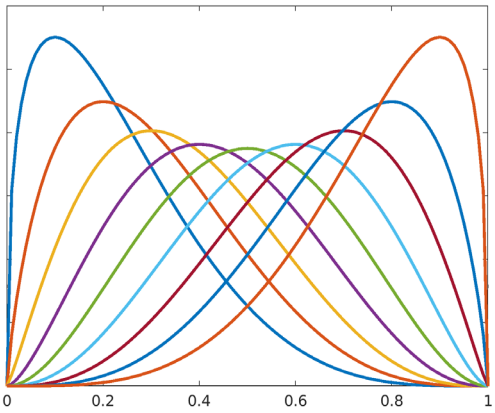
Discrete Distribution The discrete probability distribution is used when the financial impact can take on a finite mutually exclusive number of exactly known values and each value has a fixed probability of success. For example, Option 1 is a 10 % probability that the financial impact equals € 50,000; Option 2 is a 30 % probability that the financial impact equals € 75,000; Option 3 is a 50 % probability that the financial impact equals € 100,000; and Option 4 is a 10 % probability that the financial impact equals € 150,000.



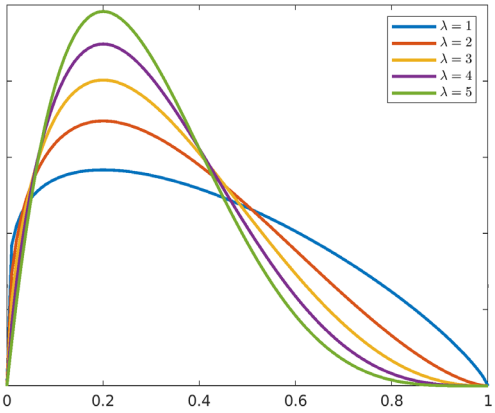
Normal (Gaussian) Distribution The normal distribution is used when a most likely value (the maximum of the graph) can be estimated. The standard deviation σ describes the degree of uncertainty: About 68 % of values drawn from a normal distribution are within ± 1σ away from the most likely value. About 95 % of values drawn from a normal distribution are within ± 2σ away from the most likely value and about 99.7% are within ± 3σ. If σ is relatively small compared to the most likely value, the graph is steep and implies a high degree of certainty. If σ is relatively large compared to the most likely value, the graph is flat and implies a high degree of uncertainty.



(Modified) PERT The PERT distribution is used when a lower bound (i.e. minimum financial impact), a most likely financial impact, and an upper bound (i.e. maximum financial impact) can be estimated. The visualisation on the right shows various density function shapes that occur as the most likely value varies from 0.1 to 0.9 when the minimum value equals 0 and the maximum value equals 1.



The degree of certainty can be expressed by varying λ values which significantly changes the tail of the distribution: If λ = 1 this implies a high degree of uncertainty, giving values close to the upper or lower bound a higher probability to occur. Increasing values for λ imply an increasing degree of certainty. This means that values close to the estimated "most likely" value have a higher probability to occur whereas values close to the upper or lower bound have a lower probability to occur



Combining the Decomposition Structure and Expert Estimations

The financial risk impact assessment according the proposed method is illustrated in Exhibit 6 and follows this logic:

• Step 2.2.1: For each terminal node (i.e. any tree node that does not have child nodes; highlighted with a blue arrow in Exhibit 5) in the decomposition model shown in Exhibit 5, check whether this impact factor is applicable or not.

• Step 2.2.2: For each applicable impact factor, ask a subject matter expert to conduct an *probabilistic* estimation of the respective factor's potential financial impact (by using one of the previously defined probability distributions).

▪ The expert's opinion concerning the financial impact is a belief statement.

▪ Therefore, subject matter experts express their opinion in a probabilistic manner, this means that they use probability distributions which simultaneously allow to describe the expert's opinion and degree of uncertainty.

• Step 2.2.3: The estimations for each applicable impact factor are aggregated bottom-up with a Monte Carlo simulation to compute the overall estimation for the potential financial impact of the risk scenario under investigation.

▪ In order to assure that the aggregation based on Monte Carlo simulations computes meaningful, accurate, and trustworthy results, it is inevitable that the design of the decomposition model enforces disjoint estimation factors to the greatest extent possible.

▪ Note that the result is *not* a single financial figure, but an *interval* that indicates with a high degree of confidence, that the true value lies in this interval (e.g. a 90 % confidence interval indicates a 90 % chance that the interval covers the true financial impact).

▪ The computed confidence interval is accurate if and only if the individual expert estimations are accurate (i.e. "garbage in / garbage out")

▪ The needed confidence can be defined by each organisation. In many real-world situations the 90 % confidence interval is used.

• Step 2.2.4: A sensitivity analysis shows for each factor its relative contribution to the overall financial risk impact. This information provides deeper insight into "impact drivers" and may help to identify adequate risk treatment options.

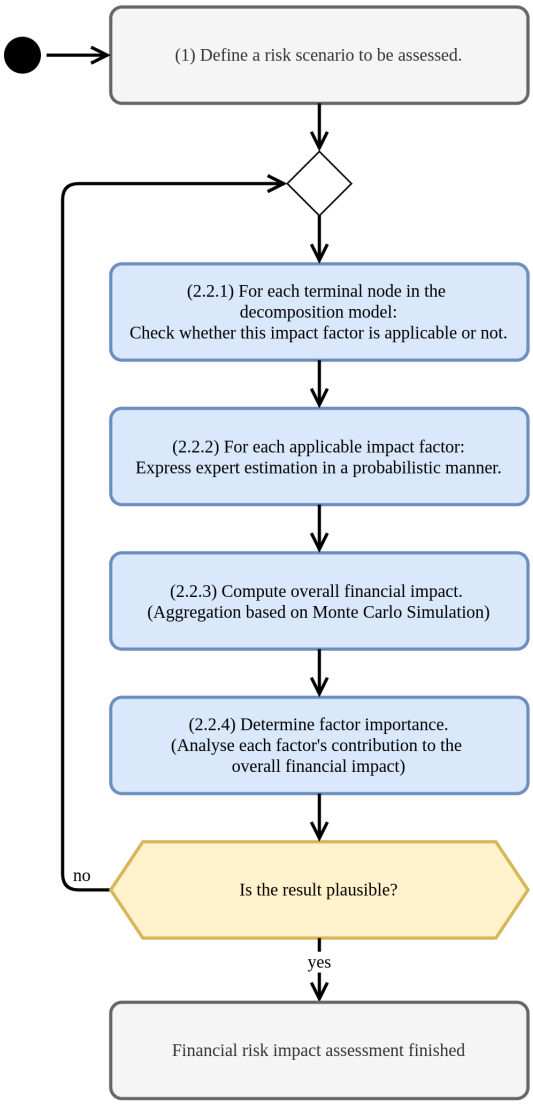


Exhibit 6: The proposed financial risk impact assessment method.

DEMONSTRATION

Step 1: Hypothetical IT Risk Scenario[1]

Title	Successful Logical Attack
Scenario	The organisation has a public web site and online shop, through which a group of hackers takes down the organisation's business systems. This is done by breaching the network perimeter and penetrating the network, and then introducing malware that takes down all 20 hardware servers (running 200 virtual servers in total) and results in a successful attack, which denies users access to applications. Normal business operations are disrupted. The attack takes place on "Black Friday" which is the most important sales day for the company.
Scenario Components	
Threat Type	The nature of the event is a **malicious** attack by hackers, which takes down the servers, denying users access to applications and information.
Threat Actor	The actors that generate the threat that exploits the vulnerability are the **external** hackers.
Event	The event is **interruption** of IT services so that users cannot access the applications and information and, therefore, normal business processes/operations are interrupted and sales cannot be processed over the company's web site.
Asset/Resource (Cause)	The asset/resource that leads to the business impact are **people** - the hackers.
Asset/Resource (Effect)	The asset/resources that are affected are mainly the interrupted business operations. However, because access is denied to the enterprise's **IT infrastructure**, **information** and **applications** are also affected.
Time	Response to the DOS attack is **critical** to restore access to business systems quickly and so sales can be issued again. The duration is **extended** because it may take quite some time to restore the official web site. Detection of the event is **immediate**, and the time lag between the event and the consequence is also **immediate**.

Step 2.2.1: Identify Impact Factors not Applicable for this Assessment

(1.1.2) Cost of evidence collection and analysis	Included in external consultant fees for incident investigation in (1.1.1).
(1.2.1.2) Cost of acquisition	Negligible, because vendor contracts are in place, the order just needs to be placed.
(1.3.1) Crisis communication expenses	Negligible, because there are no relevant external stakeholders who need to be kept updated. The communication with internal stakeholders also does not require this factor to be considered in the context of the given scenario.

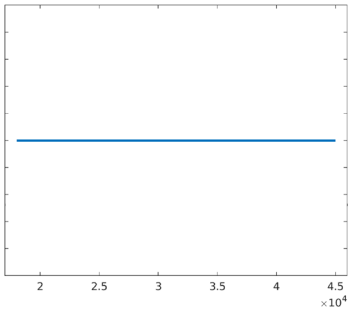
1 Adapted from ISACA „Risk Scenarios using COBIT 5"

Incurred Losses of **(2.1.1) Funds** **(2.1.2) Goods** **(2.1.3) Assets**	The organisation does not incur any loss of funds, goods, or assets.
(2.3.2) Extra expenses incurred during a disruption	The organisation does not incur any extra expenses during the disruption.
(2.4.1) Rehabilitation expenses to re-establish the reputation	The attack only takes down the servers, no customer data etc. are stolen. Therefore, the damage to the company's reputation is negligible, because the company is a victim. No rehabilitation expenses to re-establish the reputation.
(3.1.1) **(3.1.2)** **Violation of legal obligations / criminal law**	The organisation does not violate legal obligations based on criminal law.
(3.2.1) **(3.2.2)** **Violation of legal obligations / civil (tort) law**	The organisation does not violate legal obligations based on civil (tort) law.

Step 2.2.2: Financial Impact Assessment (Current Risk)

The given IT risk scenario shall be assessed in the organisation in order to determine the current risk exposure the organisation faces with respect to this scenario. Subject matter experts are selected and they describe their opinion based on the decomposition model shown in Exhibit 5:

(1.1.1) External consultant fees for incident investigation



The organisation will try to prosecute the attackers. To obtain a criminal conviction, the organisation must present evidence in court, but in order to be admissible in court, evidence must be preserved and handled to ensure that it hasn't been changed. Therefore, the organisation will use a forensic investigator (FI) to preserve digital evidence and to find out what the organisation needs to do to harden the systems so that a similar attack will not happen again.
The FI is expected to charge € 225 per hour. Considering the number of network appliances and servers that where compromised and the need to identify and correlate digital evidence the assessor estimates that the FI will need at least 80 hours, but no more than 200 hours to get the job done. The assessor assumes that both the lower bound and the upper bound effort have the same chance to occur, therefore she decides to use the uniform distribution to describe her opinion.

Estimation:
Uniform distribution.
Lower bound = € 225 x 80 = € 18,000
Upper bound = € 225 x 200 = € 45,000

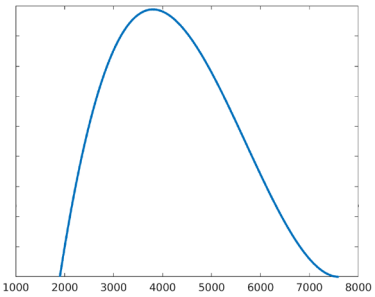
(1.2.1.1) Asset market value

The hardware firewall appliance located between the DMZ and the internal network does not frequently receive security patches, therefore it should be replaced.
As the internal network is not adequately segmented into zones, additional firewall appliances to create and protect individual network segments are needed.

Estimation:
1 appliance to separate the DMZ from the internal network: € 14,500
3 appliances to separate the internal network into zones: € 27,000

(1.2.2.1.1) Reinstall compromised systems

The malware may have installed a rootkit and it is unknown when the infection happened. Therefore at least the 20 hardware servers must be re-installed from scratch using original installation media, because it may be the case that the malicious rootkit is persisted to system backups.
The provisioning of new virtual servers is fully automated, the same mechanism can be used to rebuild the existing virtual servers. During day-to-day operations, hardware servers must be occasionally re-installed, for example, due to hardware failures. There is enough experience available and the expert is quite confident about his estimations.

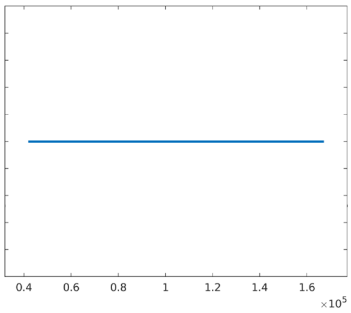


Estimation:
PERT distribution
Internal rate: € 95 per hour incl. overhead.
Min. effort to reinstall one hardware server incl. patching: 1 hour.
Likely: 2 hours.
Maximum: 4 hours.
Number of servers: 20

Lower = € 95 x 20 x 1 = € 1,900
Likely = € 95 x 20 x 2 = € 3,800
Upper = € 95 x 20 x 4 = € 7,600

(1.2.2.1.2) Reconfigure compromised systems

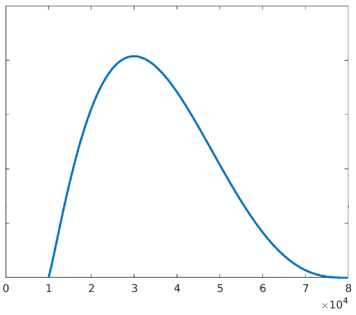
Reconfiguration tasks include the installation of additional server services (e.g. Database Management Systems) and security hardening (e.g. deinstallation of unneeded server services, change of default passwords, etc.). "Above" the operating system (OS) level, there are no baselines defined and each server must be manually reconfigured to match the target state. It is assumed that the majority of the configuration documentations are not up-to-date. A complete recovery of entire business systems was never really tested.



Estimation:
Uniform distribution
Internal rate: € 95 per hour incl. overhead.
Min. effort to reconfigure one server: 2 hours
Maximum: 8 hours.
Number of servers: 220
Lower = € 95 x 220 x 2 = € 41,800
Upper = € 95 x 220 x 8 = € 167,200

(1.2.2.2.1) Cost of backup restoration

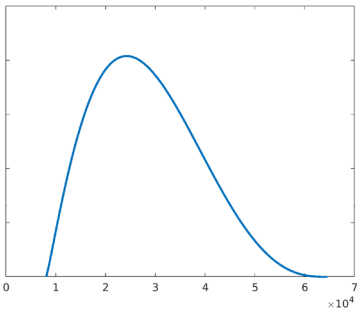
During day-to-day operational tasks, backups must be occasionally restored, but there is no systematic testing in place. Usually, the backup restoration just works fine, but from time to time there are severe issues related to backup integrity.



Estimation:
PERT distribution
Internal rate: € 95 per hour incl. overhead.
Min. effort to restore backups: 30 minutes per server.
Likely: 90 minutes per server.
Max: 4 hours per server.
Number of servers: 210
Lower = € 95 x 210 x 0.5 = € 9,975
Likely = € 95 x 210 x 1.5 = € 29,925
Upper = € 95 x 210 x 4 = € 79,800

(1.2.3) Cost of system verification

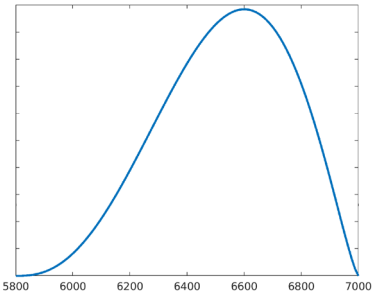
Before (major changes of) business systems are promoted to the production environment, thorough testing is conducted. Thus, test cases already exist.



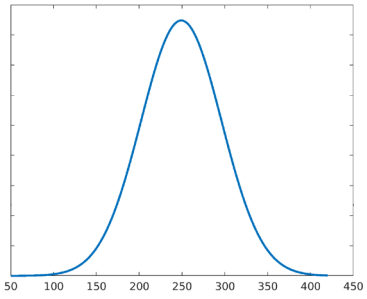
Estimation:
PERT distribution
Internal rate: € 95 per hour incl. overhead.
Min. effort to test: 1 hour per business system.
Likely: 3 hours per business system.
Max: 8 hours per business system.
Number of business systems: 85
Lower = € 95 x 85 x 1 = € 8,075
Likely = € 95 x 85 x 3 = € 24,225
Upper = € 95 x 85 x 4 = € 32,300

(2.2.1) Loss of revenues

The company's online shop is hosted on the web servers in the DMZ. The attack is committed on "Black Friday" which starts the most important sales week for the company, causing a significant loss of revenue. Sales figures from the past years show that there was a growing trend from 5800 orders 3 years ago to 6800 orders last year.



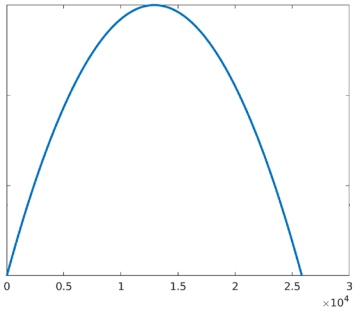
Estimation for the number of "lost" orders:
PERT distribution
Min. orders: 5,800
Likely: 6,600
Max: 7,000



Estimation per order:
Normal distribution
mean = € 249
standard deviation = € 47

(2.3.1) Incurred labour costs during disruption of internal operation

The company could force all employees who are not assigned to incident resolution tasks to take mandatory vacation. In this case, the incurred labour costs during disruption of internal operation is significantly reduced.

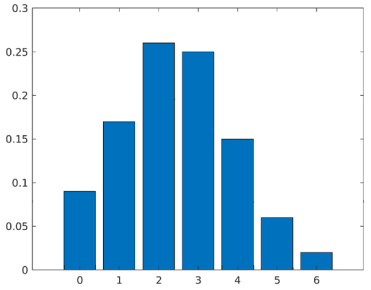


Estimation:
Modified PERT distribution (λ = 1, i.e. high uncertainty)
Internal rate: € 95 per hour incl. overhead.
Min.: 0 unproductive hours per employee
Likely: 4 hours
Max: 8 hours
Number of employees: 34
Lower = € 95 x 34 x 0 = € 0
Likely = € 95 x 34 x 4 = € 12,920
Upper = € 95 x 34 x 8 = € 25,840

(3.3.2) Violation of contractual obligations / compensatory damages

In addition to its own online shop, the organisation hosts 3rd party online shops and provides them in a "software as a service (SaaS)" manner. At the time of the incident, they have seven customers and the respective service level agreements (SLA) require a 98.5 % uptime (availability) per year on a 24/7 basis. In order to avoid a service level breach and the associated liability to pay damages, the maximum allowed unplanned downtime (for the entire year) of the service is approximately 5 days 11 hours 30 minutes. The SLA states that for each additional full 24 hours of downtime, the organisation has to pay € 1,000 per customer. (In order to keep this demonstration simple, it is assumed that there was no unplanned downtime prior to this incident.)

Based on the estimations for "system installation", "system configuration", "backup restoration", and "system verification" provided above, an analysis shows the following distribution for the throughput time of incident response tasks.



Discrete distribution:
9 % chance to compensate 0 days downtime: 0 x € 7,000 = € 0,000
17 % chance to compensate 1 day downtime: 1 x € 7,000 = € 7,000
26 % chance to compensate 2 days downtime: 2 x € 7,000 = € 14,000
25 % chance to compensate 3 days downtime: 3 x € 7,000 = € 21,000
15 % chance to compensate 4 days downtime: 4 x € 7,000 = € 28,000
6 % chance to compensate 5 days downtime: 5 x € 7,000 = € 35,000
2 % chance to compensate 6 days downtime: 6 x € 7,000 = € 42,000

Step 2.2.3: Monte Carlo Simulation and Aggregation

The overall aggregated financial impact of the hypothetical risk scenario is computed according to the following pseudocode:

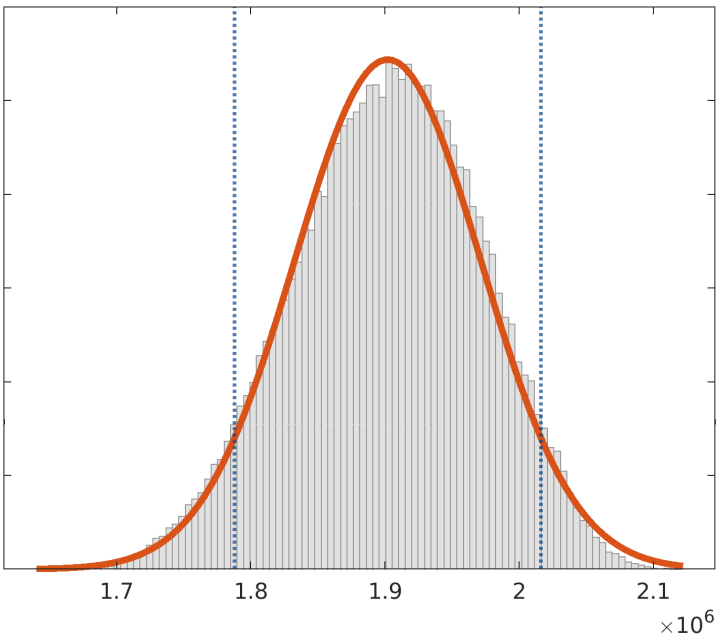
```
For experiment = 1 to 100,000

  impactFactor1 = DrawRandomSampleFromDistribution(estimatedDist1);
  impactFactor2 = DrawRandomSampleFromDistribution(estimatedDist2);
  ...
  impactFactorN = DrawRandomSampleFromDistribution(estimatedDistN);

 overallImpact[experiment] = impactFactor1 + impactFactor2 + ... + impactFactorN;

end for
```

The simulation is repeated 100,000 times resulting in 100,000 impact results. MATLAB is used to create a histogram with 100 bins (by utilising the standard `histogram` command; grey area in the visualisation below). Then a Gaussian distribution is fitted to the histogram (by utilising the standard `histfit` command; red graph in the visualisation below).



The fitted Gaussian distribution has the following characteristics:

Mean = € 1,901,959.83 Standard deviation = € 69,320.86

The boundaries of the 90 % confidence interval (CI) are the 5th percentile ("p5") and the 95th percentile ("p95"):

p5 = € 1,787,937.16 p95 = € 2,015,982.50

Note that the precision of the 90 % CI may mislead people into believing that there is more rigour in the risk assessment process than actually exists. Therefore, the final outcome is rounded to

p5 = € 1,750,000 p95 = € 2,050,000

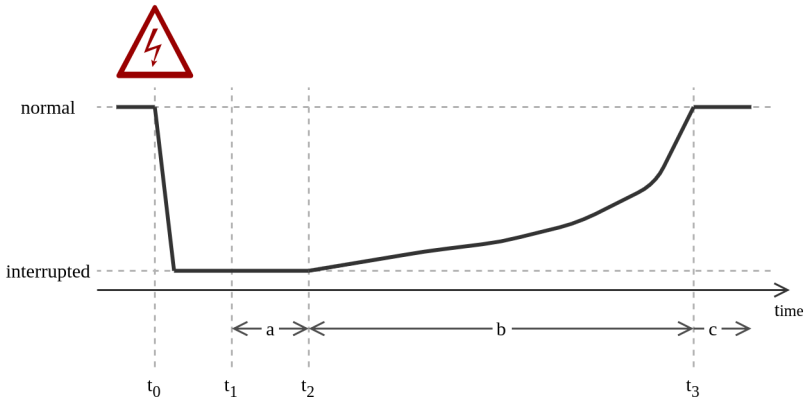
indicating that with 90 % probability this confidence interval covers the true financial impact of the assessed risk scenario.

Step 2.2.4: Determine Factor Importance

Sampling-based approaches to sensitivity analysis are well-researched, effective and widely used. Regression analysis was used to determine each factor's influence on the overall financial impact. The result shows that the factors "(2.2.1) Loss of Revenues" and "(1.2.2.1.2) Labour Cost of Configuration" are the major "impact drivers". There are two options now: (a) challenge the estimations provided for these two factors to assure that the assessment is plausible or (b) if it is assured that the assessment is plausible, search for potential risk mitigation or risk transfer options which particularly focus on one (or both) of these factors. For the sake of simplicity, the decision is to continue with option (b).

Step 4: Define a Potential Risk Mitigation or Risk Transfer Option

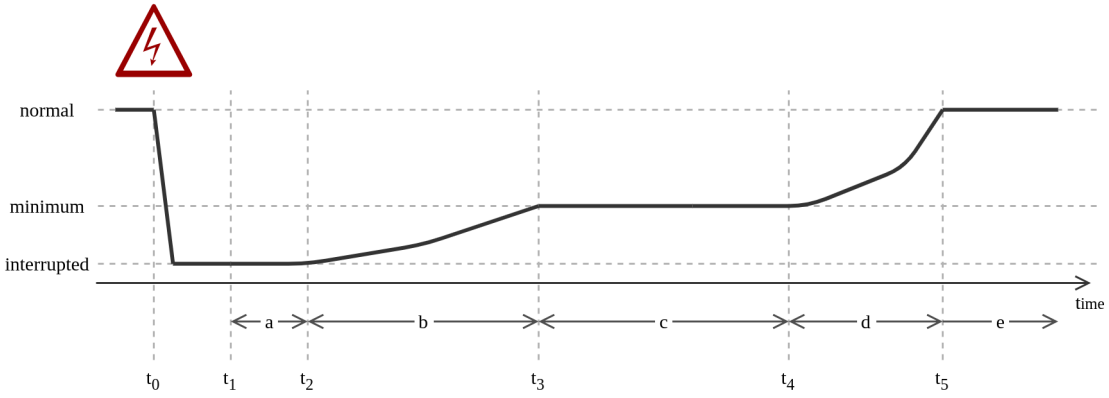
The overall financial risk impact determined in steps 2.2.1 to 2.2.3 above are based on the assumption that there is a complete interruption until *all* systems are recovered and operate at normal level again (i.e. the time period from t_0 to t_3 in Exhibit 8), because there is no continuity plan in place that ensures that critical business information systems are recovered with a higher priority than less critical systems.



a = investigate | b = recover to normal operations level | c = operate at normal level

Single-phased recovery.

However, there is a strong correlation between the duration needed to complete the incident response tasks and the loss of revenues. One potential mitigation option is illustrated in Exhibit 9: The idea is to create a prioritised list of critical systems that shall be recovered first in order to limit the adverse business impact. After these critical systems are recovered, a minimum operation level is achieved (starting with t_3). While operating at this minimum level, the other (less critical) systems can be recovered.



a = investigate | b = recover to minimum operations level | c = operate at minimum level | d = recover to normal operations level
e = operate at normal level

Multi-phased recovery.

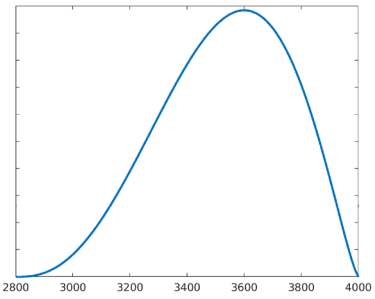
Step 5.2: Conduct a Hypothetical Financial Impact Assessment

This step examines the degree to which the implementation of the risk mitigation measure described in Step 4 would decrease the risk for the organisation. Note that it is not reasonable to assume that the overall incident response costs will decrease, because sooner or later all systems have to be recovered. Only the task sequence is optimised to reduce the loss of revenues. Furthermore, the sensitivity analysis shows that compensatory damages to be paid because of service level breaches are negligible, therefore those systems are not classified as critical.

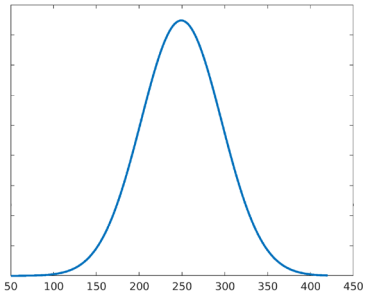
All estimations remain unchanged - except the following:

(2.2.1) Loss of revenues - mitigated

The company's online shop is hosted on the web servers in the DMZ. The attack is committed on "Black Friday" which starts the most important sales week for the company, causing a significant loss of revenue. Sales figures from the past years show that there was a growing trend from 5800 orders 3 years ago to 6800 orders last year.



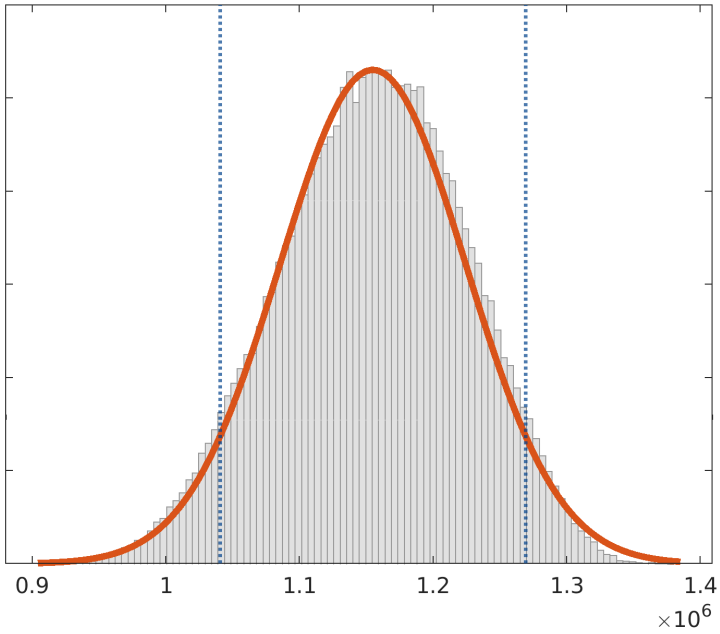
Updated estimation for the number of "lost" orders (due to the prioritised recovery of critical business information systems):
PERT distribution
Min. orders: 2,800 (was 5,800)
Likely: 3,600 (was 6,600)
Max: 4,000 (was 7,000)



Estimation per order (unchanged):
Normal distribution
mean = € 249
standard deviation = € 47

Step 5.2: Conduct a Hypothetical Financial Impact Assessment

Again, the Monte Carlo simulation is repeated 100,000 times resulting in 100,000 impact results which are used to create a histogram with 100 bins (grey area in the visualisation below). A Gaussian distribution is fitted to the histogram (red graph in the visualisation below).



The fitted Gaussian distribution has the following characteristics:

Mean = € 1,154,817.35 Standard deviation = € 69,484.03

The boundaries of the 90 % confidence interval (CI) are the 5th percentile ("p5") and the 95th percentile ("p95"):

p5 = € 1,040,526.29 p95 = € 1,269,108.40

Again, the precision of the 90 % CI may mislead people into believing that there is more rigour in the risk assessment process than actually exists. Therefore, the final outcome is rounded to

p5 = € 1,000,000 p95 = € 1,300,000

indicating that with 90 % probability this confidence interval covers the true financial impact of the assessed risk scenario.

Comparing this CI with the initial CI it can be seen, that the p95 decreased by € 750,000 (from € 2,050,000 to € 1,300,000).

Step 7: Conduct a Cost/Benefit Analysis

After combining the risk impact with the (unchanged) probability assessment, the difference between the current risk and the residual risk can be computed and compared with the actual cost of implementing this mitigation measure. Other risk mitigation or risk transfer options can be assessed in the same way.

The proposed financial risk impact assessment method should help both the risk practitioner to identify which impact factors require treatment and therefore to assess adequate treatment options and risk owners to take (hopefully better) informed decisions.

BRIEFING FINISHED, PLEASE START YOUR EVALUATION

At this point you should be familiar with the proposed financial risk impact assessment method. If you have any open questions related to the proposed method, please do not hesitate to contact Mr. Gernot Kielhauser via e-mail (gernot.kielhauser@edu.donau-uni.ac.at) in order to discuss and clarify your questions. Otherwise, if you come to the conclusion that the information provided in this brochure is sufficient to allow you to evaluate the proposed method based on your expertise, please go to SurveyMonkey (the link to the survey is provided in the email you received) and fill in the survey questions.

Thank you very much for supporting my study.