WHITE PAPER

Ensuring Business Continuity with a Sustainable Risk Management Process

Table of contents

IT is the backbone of digital business. It must be protected against possible risks to ensure smooth operations. Risks are manifold, some arising from external threats (like viruses, aggressive hackers or data theft) and others from internal sources (such as inappropriate handling of passwords by employees, or poor license and contract management). Such IT security incidents can result in a partial or complete loss of data, the disclosure of sensitive or confidential data, or the manipulation of data. All of this can have a serious impact on business' ability to perform its tasks.

Due to the increasing pace of business change, risks are prone to modification as often as IT systems. IT risk management should not be a one-off project, but a continuous process targeting constantly changing IT risk and business environments, monitoring the risks and adjusting the risk management strategy accordingly.

With effective IT risk management processes in place, IT organizations are able to manage IT's integrity with regard to applications, projects, data, systems, and employees to ensure business continuity. An additional benefit of IT risk management is that it improves operational performance by helping understand IT operational risk so you can implement mitigation measures. Thus the number of incidents can be lowered, fostering greater business satisfaction. Another reason for wanting to establish a continuous IT risk management process is compliance—the consistent enforcement of and compliance with standards and regulations, such as SOX, Dodd-Frank and data protection laws.

IT risk management comprises the inventorization and prioritization of applications to identify possible risks, the assessment of the risks identified and, of course, their mitigation in order to reduce the overall threat to the enterprise.

Read on to find out more about Software AG's recommended approach to IT risk management and how it is supported by Alfabet for enterprise architecture, IT planning and portfolio management.

Inventorize applications

The objective of this phase is to prepare a detailed listing of all applications as preparation for setting the scope of the risk assessment. This phase also includes description of the interdependencies between the business, applications and the infrastructure in order to establish a comprehensive inventory that can be re-used for future assessments.

When creating the inventory, it is important to keep the actual need for risk assessment in mind to avoid an unnecessarily large scope. Decide on the reach of the assessment (for example, company-wide, region-wide, organizational or domain-wide) and whether to apply quantitative or qualitative criteria for choosing which applications belong in the inventory for risk assessment. A quantitative assessment calculates different risk factors to understand how these contribute to an overall risk value. A qualitative assessment is more descriptive but in most cases sufficient to identify risk areas that need attention.

Roles:

- IT Compliance Manager, CISO

Activities:

- Inventorize applications, services, technologies, business capabilities and their relationships to each other
- Define metrics and aggregation rules

Deliverables:

- Documented IT scope for risk assessment

Best-practice recommendations:

- Define ownership and responsibility for the application information
- Define roles for quality control and escalation of issues
- Document roles in the IT inventory for transparency and to anchor governance
- Use workflows and wizards to support automation of inventory management and ensure high quality data
- Integrate to primary sources as available

	Quantitative	Qualitative
Damage	• Define application support per organization/ process (or define application support via services provided) • Calculate potential damage based on historic incident figures for each support and estimate to fill gaps ⇨ More accurate and supports more differentiated mitigation strategies ⇨ High effort involved in inventorization and execution	• Define application support per process • Have process owner assess the damage probability based on historical failure rates ⇨ Less differentiated in assessment and mitigation ⇨ Quicker to inventorize and execute
Probability	• Define internal application architecture with relationship to deployments and devices • Calculate failure probalility based on historic failure information from various levels and available statistics ⇨ More accurate and supports mitigation at source ⇨ Makes accumulation and distribution effects transparent ⇨ High effort involved in inventorization and execution	• Define application support per process • Have process owner assess the damage probability based on historical failure rates ⇨ Less differentiated in assessment and mitigation ⇨ Quicker to inventorize and execute

Figure 1: Use either a quantitative or qualitative approach to decide which applications will be in the scope for the risk assessment.

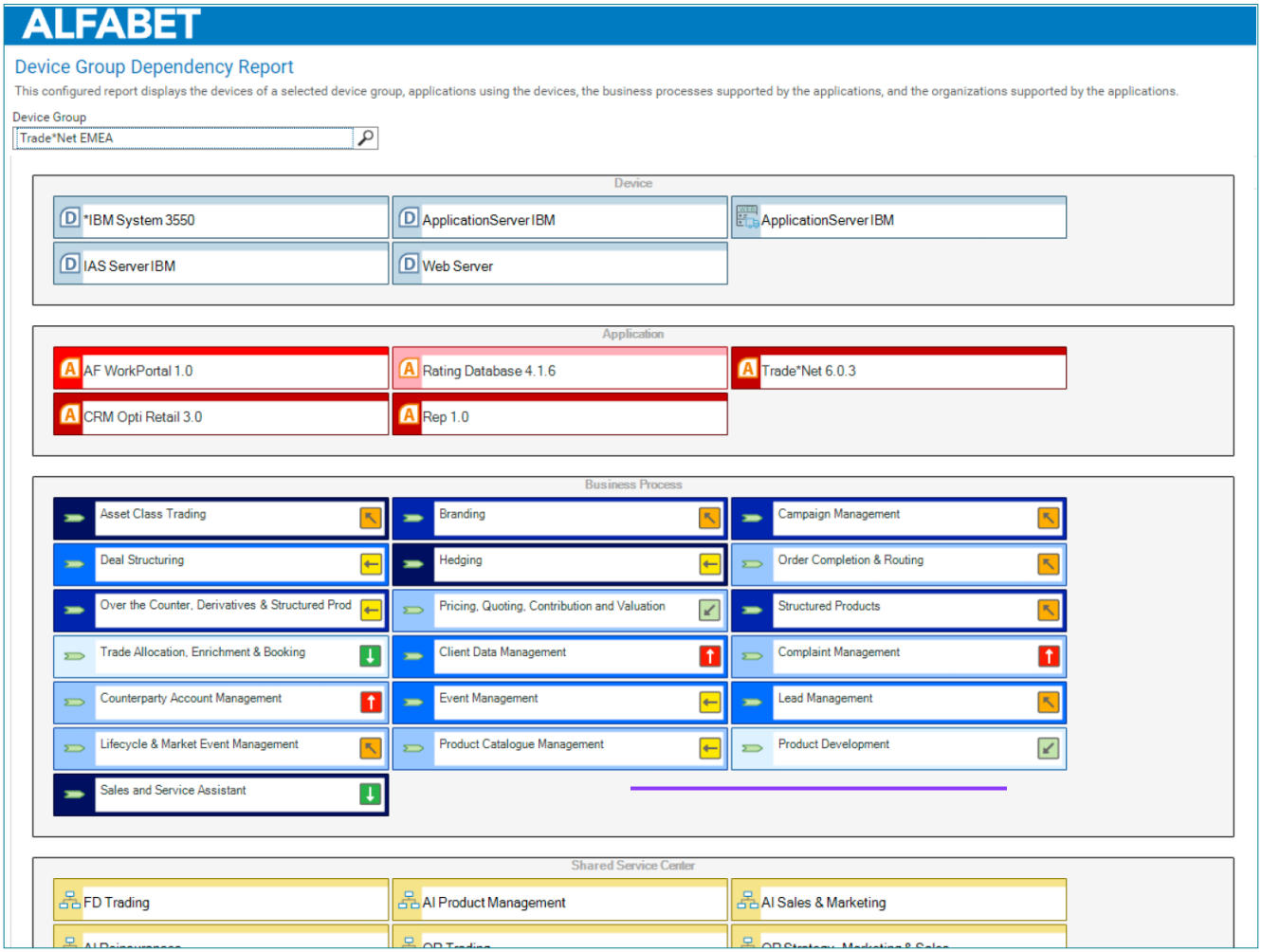

Figure 2: The ability to see the interdependencies of the architecture elements is critical for business continuity. In this view you see all of the devices, applications and business processes dependent on each other. The various colors and shades indicate risk of loss (blue) and incidence rate (red) with low indicated by a pale color and high indicated by a deep color. The icons indicate business criticality with the arrow up indicating high importance and down indicating low importance.

Prioritize applications

IT risk assessment is commonly carried out by multiple stakeholders and involves many objects—applications, processes, technologies, services—and a variety of risks that are to be assessed. Thus a clear focus should be set on only the relevant objects. This should be done in two phases. First, identify the most risk-relevant applications—those which are most important to protect—and make them first priority. These will be applications that support business-critical capabilities or are subject to compliance regulations. Second, perform a detailed risk and mitigation survey. The survey is to fine-tune the reasoning for an application being risk-relevant. This process and follow-up analyses can be automated by using workflows, calculation routines and reporting tools, thus making it less costly in terms of labor. The answers, for example, “major breach of law” for regulatory risk, can then be mapped to metrics reflecting the type of violation, such as confidentiality, integrity or availability. These metrics are then added up to provide a risk-relevance score for the applicationscope. Decide on the reach of the assessment (for example, company-wide, region-wide, organizational or domain-wide) and whether to apply quantitative or qualitative criteria for choosing which applications belong in the inventory for risk assessment. A quantitative assessment calculates different risk factors to understand how these contribute to an overall risk value. Aqualitative assessment is more descriptive but in most cases sufficient to identify risk areas that need attention.

Roles:

- IT Compliance Manager, CISO

Activities:

- Define questions and mappings to metrics
- Survey application owners
- Decide on prioritization

Deliverables:

- List of applications for risk assessment

Best-practice recommendations:

- Be pragmatic—pursue a qualitative approach directed at relevant stakeholders
- Use only a compact set of questions with simple answers
- Map the answers to numeric values for easier analysis

1. Data and Content	What is the classification of the data and content according to the predefined classification scheme?	1-public 2-internal 3-confidential 4-private confidential 5-strictly confidential 6-individual-related-public
2. Regulatory	To what extent are laws, regulations, norms or similar applicable? What are the consequences of non-observance?	1-no relevance 2-misdemeanor 3-minor offense 4-penalty 5-major breach of law
3. Contractual Relevance	Are there applicable contractual obligations with customers, suppliers or partners that may result in penalty payments?	1-none 2-up to 10% of contract volume 3-up to 30% of contract volume 4-up to 50% of contract volume 5-in excess of 50% of contract volume
4. Downtime	How long can the service be down without major impact?	1-no availability requirements 2-less than 1 week 3-less than 1 day 4-less than 4 hours 5-less than 1 hour
5. Financial Implications	What is the maximum total damage for the unit under the assumption of a worst case scenario (including penalty payments, opportunity costs and indemnities?)	1-not relevant 2-less than €500,000 3-less than €2.5 million 4-less than €10 million 5-more than €10 million 6-unknown

Figure 3: Here we see a sample survey of questions to ask for each application.

ALFABET

Application: EasiTrade Web v.2.1

Risk Relevance Questionnaire

		Question	Value	Protection Requirements (Risk Management)			
	1 2			1. Confidentiality	2. Integrity	3. Availability	4. Authenticity
1	▼	IT Operations Risk Management Evaluation					
2		1. Data and Content	social data	3.00	3.00	0.00	3.00
3		2. Regulatory	major breach of law	4.00	4.00	4.00	4.00
4		3. Contractual Relevance	up to 30% of contract volume	2.00	2.00	2.00	2.00
5		4. Downtime	less than 1 day	0.00	0.00	2.00	0.00
6		5. Financial Implications	less than 2.500.000$	2.00	2.00	2.00	2.00
7		6. PR Damage	problem with national or global press and authorities	4.00	4.00	4.00	4.00
8				15.00	15.00	14.00	15.00

Figure 4: Here we see a metrics scheme which gives a specific value to each answer depending on which type of protection requirement it would need.

Risk assessment

Assessing the risks to applications aims at understanding the risks an application is subject to and analyzing the relevant risk's damage potential in order to be able to suggest and evaluate possible mitigations.

Risk catalogs support consistent risk assessment by providing sample categories for risks and sample risks in these categories (for example, willful act > manipulation of data or data theft). In the course of the assessment, each risk is assessed as to its probability and damage potential. Inventorizing possible mitigations for the risks in the catalog supports the standardization of the mitigation strategy and reduces the effort in risk assessments. When assessing the risk for an application, it is important to document the relevant mitigation and to what extent the proposed mitigation will change the risk's probability and damage values in order to be able to identify the most effective mitigations.

Roles:

- IT Compliance Manager, CISO

Activities:

- Catalog risks
- Assess probability
- Assess potential damage
- Suggest mitigation and assess change to risk

Deliverables:

- Application risk portfolio

Best-practice recommendations:

- Use a risk catalog to standardize risks and their mitigations
- Use multiple-choice questions and simple answers for comparability, for example, risk: none, low, medium, high, very-high; damage: <$100 trillion, <$500 trillion, <$1 million, >$3 million

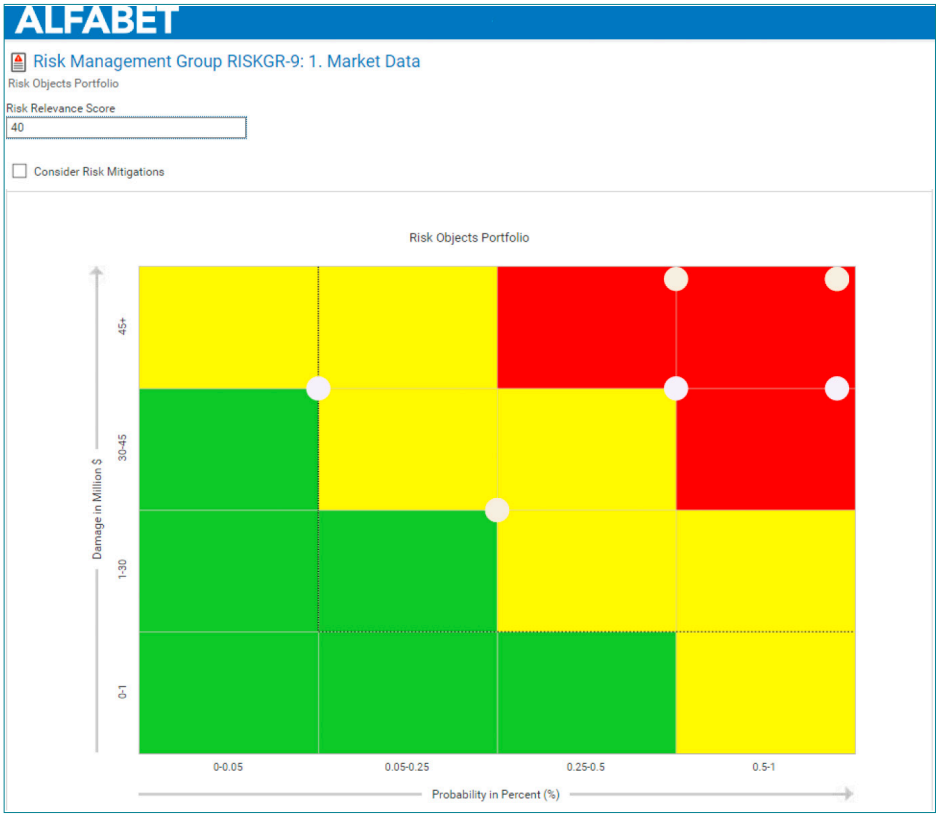

Figure 5: Once assessed, the risks can be shown in a portfolio according to damage potential and probability of occurrence.

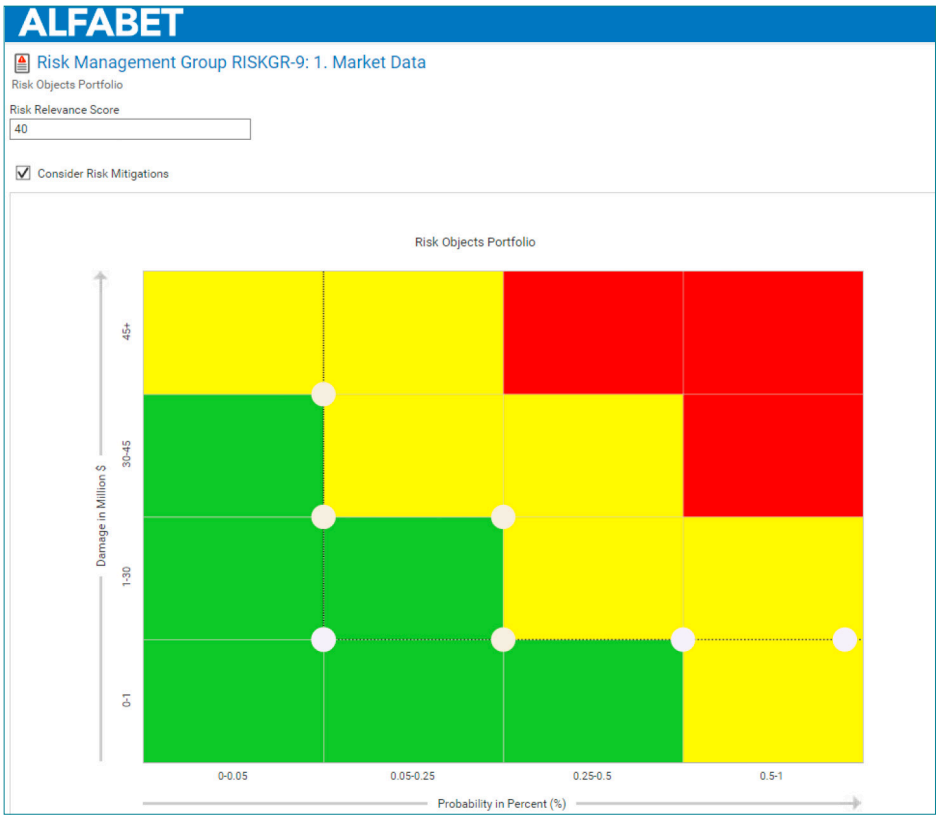

Figure 6: A filter on the portfolio shows mitigation effects to determine the best potential for reduction of risk. This and the previous chart provide a “before-and-after” risk portfolio.

Risk mitigation

Once identified and assessed, risks can be mitigated by initiating a project to support changes, or by implementing a control system in order to regularly check and ensure that all tasks are fulfilled appropriately.

Typically, internal control systems are a set of controls implemented to ensure that risk mitigations are performed according to plan. For example, if there is a risk of a system failure, a possible mitigation strategy is to provide a back-up instance of the system. Controls for this mitigation strategy could regularly check whether back-ups are made (for example, monthly), whether the restore procedure is documented (for example, yearly), and whether the restore procedure is tested (for example, bi-annually). Automating such control assessments delivers a substantial savings potential for the enterprise as it makes the process repeatable and also provides a basis for external and internal control audits, for example, as required by SOX. And finally, risk mitigation systematically reduces the extent of exposure to a risk and its probability.

Roles:

- IT Compliance Manager, CISO

Activities:

- Propose mitigation projects
- Propose controls

Deliverables:

- Reduced risk
- Documented controls

Best-practice recommendations:

- Formulate controls as questions
- Structure controls to address specific compliance topics
- Re-use controls to reduce effort

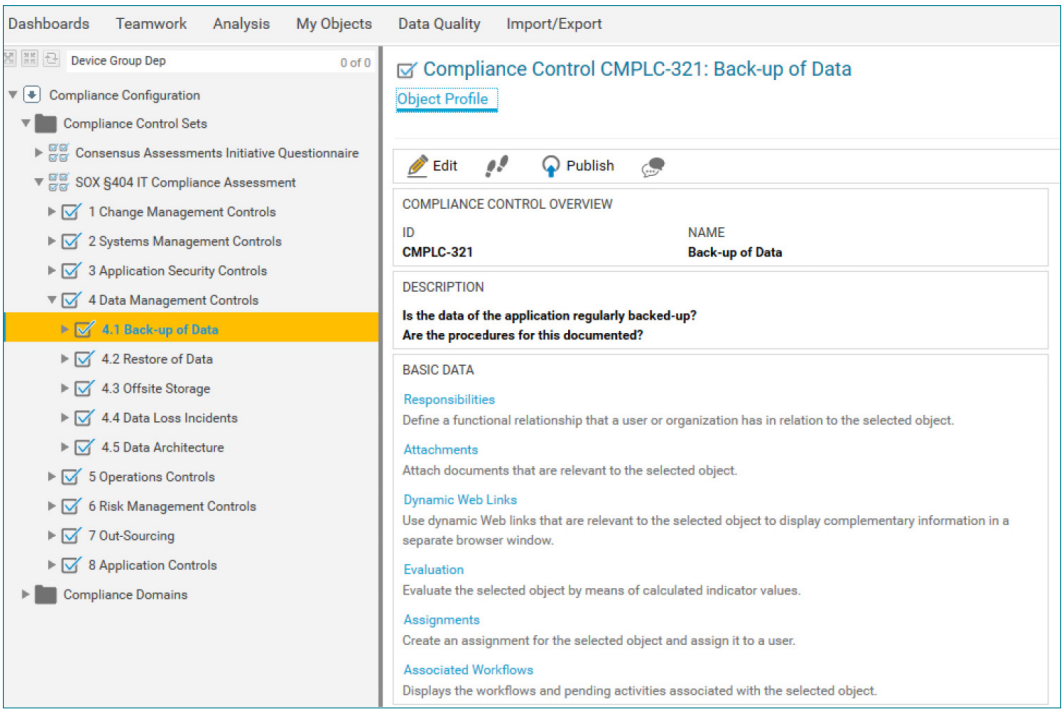

Figure 7: Here we see an example of a compliance control.

Efficient IT risk management with Alfabet

As IT tries to keep pace with the acceleration of the business environment, IT managers have to find that delicate balance between performance and risk. They need greater insight into their organization's risk exposure to be able to understand what IT systems carry risk, what the implications of the risk are, and what kind of mitigation measures are needed.

Every company in every industry will have some risk management process in place. But what they need to be asking themselves is: Are the processes and tools we are using really helping to identify all of the risks the company is facing? Because in IT risk management it's clear: What you don't know WILL hurt you. A risk management program needs to ensure that:

- ALL IT assets are being considered
- "Invisible" assets relating to risk-loaded assets are identified
- Risk surveys are executed time- and cost-efficiently
- Resources for assessing risks and mitigation efforts are only used on assets that are truly critical
- Mitigation plans are actionable, effective and published
- Decisions to accept certain risks are communicated to senior management
- Risk management processes are repeatable and sustainable

Alfabet puts a best-practice methodology into your hands that will improve your company's risk posture by identifying:

- Which projects and applications are risk-relevant
- What risks these projects and applications actually pose
- How risks can be effectively mitigated
- Which mitigations have not been implemented

Alfabet's proven technology platform enables you to:

- Capture the assets to be evaluated
- Understand the structure and relationships of the assets
- Employ collaboration technology to ensure timely survey participation
- Automatically translate survey results into risk-relevance values
- Create reports for easy understanding and communication of the risk portfolio
- Know when, where and how to start mitigation

Using Alfabet for a sustainable IT risk management program will reduce the chance of risk event loss and provide a basis for a cost-effective and sustainable risk management program.

Take the next step

Contact our experts today: **www.SoftwareAG.com/contact-alfabet**