Funded by the European Union

secureu
DIGITAL EDUCATION TOOLS FOR SECURITY RISK MANAGEMENT

HOW SECURITY RISK MANAGEMENT CAN CONTRIBUTE TO ACHIEVING RESILIENCE WITHIN ORGANIZATIONS

Lambert Bambach / Avans University of Applied Science, the Netherlands / 2024

Abstract

The management of a maritime company realizes that organizational resilience incorporating Business Continuity Management requires more than a reliance on procedures to recover assets. What if they can't be recovered within reasonable timeframes, or at all? The management wants to gain insight in the steps that are necessary to enable organizational resilience in a progressive way. Building the capacity for agility, adaptation, learning, and regeneration to ensure that the organization is able to deal with more complex and severe events (such as a pandemic, climate change, or cyber-attacks) and be fit for the future.

Link to ISO 31000

Improvement, integration, leadership and commitment, design, human and cultural factors, continual improvement, customized, inclusive, communication & consulting, risk identification and risk analysis.

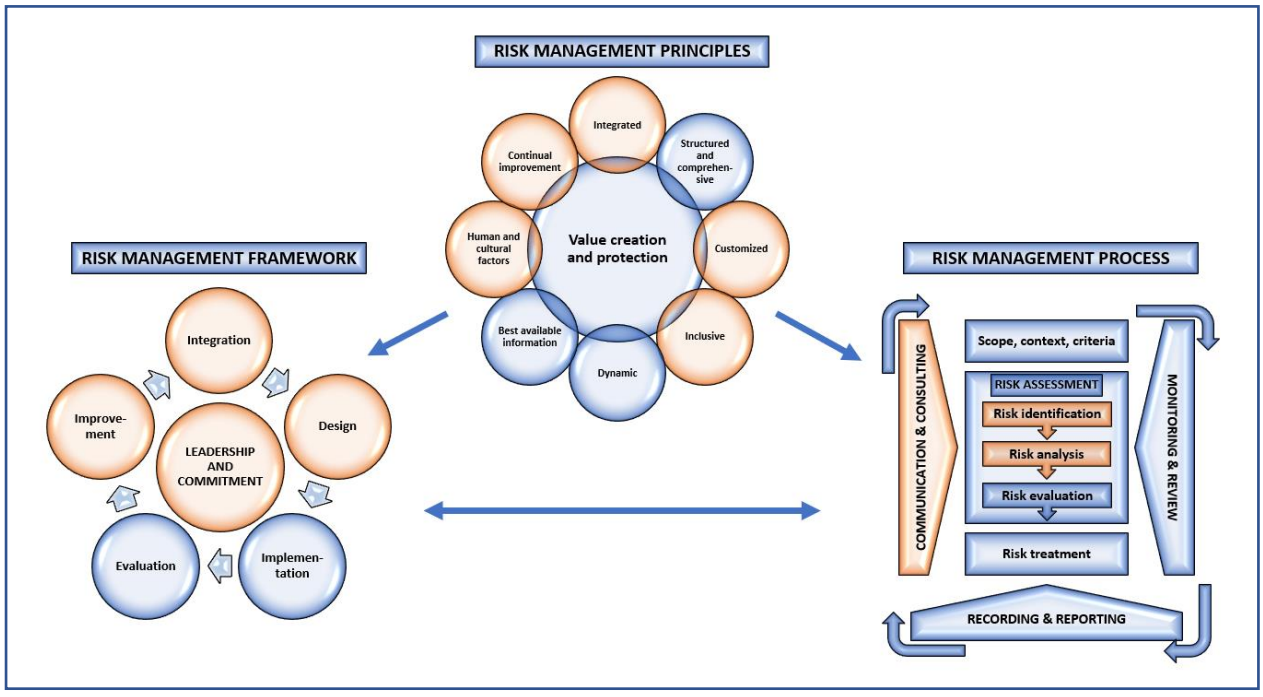

Figure 1. Risk management framework, Risk management principles and Risk management process according to ISO 31000:2018

1. Introduction

A Dutch maritime contracting company that specializes in dredging, land reclamation, and constructing man-made islands experiences that relying on a reactive strategy is not enough on its own to meet the potential scale and pace of change imposed by sudden shocks and future challenges. The management realizes that organizational resilience incorporating Business Continuity Management requires more than a reliance on procedures to recover assets. And what if they can't be recovered within reasonable timeframes, or at all?

2. Case

The management expects that a next crisis might be very different from the COVID-19 pandemic, and another government bailout may not be forthcoming. Therefore, companies must take more responsibility for their resilience and must invest in future resilience.

The management have asked you to look into the steps that are necessary to enable organizational resilience in a progressive way. Building the capacity for agility, adaptation, learning, and regeneration to ensure that the organization is able to deal with more complex and severe events (such as a pandemic, climate change, or cyber-attacks) and is fitter for the future.

3. Best practices

3.1 Goal of the organization

The organization aims for maritime ingenuity for a sustainable and secure future.

3.2 Risk Assessment

The organization identifies risks and translates them into effective and practical solutions. The organization identifies threats and risks in the field of Security Risk Management that directly influence their primary process, as well as trends in threats that arise from geo-political tensions, such as climate change, that can indirectly affect their primary processes. The organization continuously supports the operation in assessing whether the organizational security baseline is still sufficient or not and whether it needs to be adjusted, as well as in the further development of security measures to support resilience for the organization.

3.3 Steps that help to enable resilience within the organization

In the further development of security measures to support resilience the following steps should be taken into account to enable organizational resilience in a progressive way.

3.3.1 Discuss future failure

Resilient organizations accept that their design, plans and operations, are fallible – they ask what if? They also anticipate and make less complacent assumptions about future issues – they ask what next? With this mindset one allows people to speak up who might remain silent for fear of being labelled a pessimist or being punished for speaking up with a dissenting view. It helps dampen excessive optimism about security of the operation, when one assumes the incident has already occurred instead of pretending it might happen. Moreover, it helps people to overcome blind spots – it forces people to see things from different perspectives, especially when you have sufficient cognitive diversity in the room.

3.3.2 Consider connected impacts

No organization is resilient unless the system is resilient. The five capitals model can be used to allow organizations to examine five connected impacts (Table 1) for every severe but plausible scenario. The model can also help organizations examine their connected resilience and consider what needs to be done to maximize the value of the five capitals, manage 'trade-offs, and avoid weakening them, to minimize any key impacts. In many organizations, these impacts are labelled people, reputational/regulatory, operational, environment and financial. Although the model can help to examine the connected resilience it is a mistake to assume that specific issues in one of the capitals will have a corresponding impact in others. Specifically, reputational impacts can be unpredictable.

Five capitals	Key impacts
Human capital (e.g. skills, capabilities, experience, know-how, tacit knowledge)	People impact (e.g. harm, wellbeing, health absenteeism, turnover)
Social capital (e.g. networks, norms, values and understandings that facilitate cooperations, collaboration and community)	Reputation/regulatory impact (e.g. reputation, confidence, trust, complaints, customer loyalty, regulatory fines, contractual penalties, market integrity)
Built capital (e.g. building, water processing, manufacturing and processing plants, energy, transportation, communications infrastructure, technology)	Operational impact (e.g. machine downtime, system outages, capacity utilization, on-time delivery, yield, data loss)
Natural capital (e.g. materials, soil, air, water, plants and animals)	Environmental impact (e.g. biodiversity loss, pollution, deforestation)
Financial capital (e.g. cash, assets, credit, and other forms of funding that build wealth)	Financial impact (e.g. profitability, liquidity, cash flow, solvency, valuation)

Table 1. Five Capitals Model

3.3.3 Understand Essential Outcomes (EOs)

Often resilience is thought of as the absence of disruptions (or as an acceptable level of risk). In this perspective, resilience is defined as a state, where as few things as possible go wrong. Crucially, this view does not explain why Essential Outcomes (EOs) almost always go right. An alternative to the conventional approach of trying to make *'as few things as possible go wrong'* is to try to make *'as many things as possible go right'*.

To gain the insights for the organization to do this, a visual representation of an EO can be produced by journey mapping and resilience (service) blueprinting involving diverse contributions from a multi-disciplinary team. The benefits of (service) blueprinting are shown below (Table 2).

The benefits of service blueprinting
▪ Forming a stable, shared understanding of an essential outcome
▪ Assembling the contributing factors into a coherent causal diagram
▪ Examining single points of failure/lack of alternative paths, crucial interfaces, critical steps (points of no return), and 'risk important' actions
▪ Exploring how factors are interconnected across borders and boundaries
▪ Incorporating different worldviews and data from diverse sources
▪ Producing a rich, visual picture to share with colleagues
▪ Highlighting problems areas that should be addressed to prevent incidents from occurring in the future

Table 2. The benefits of service blueprinting

3.3.4 Define a resilience threshold based on the impact tolerance approach

Organizations can define their own resilience thresholds, which ultimately entails quantifying how a disruption could impact the organization, different customer groups, and the wider sector and

system. To enable organizational resilience in a progressive way organizations should adopt the impact tolerance approach instead of the traditional risk-based approach. Below (Table 3) the impact tolerance approach is compared to the traditional risk management approach.

Traditional risk-based approach	Impact threshold approach
Primarily internal – impact on the organization's objectives	Primarily external – impact to an external stakeholder and broader system
Focus on named risk types	Focus on essential outcomes
Appetite for and classification of risks: minor, moderate, high or severe	Thresholds of what is tolerable/acceptable
Likelihood of the risk occurring	Assumes that risk has occurred
Defines effects and actions or interventions which would reduce the inherent exposure	Defines effects and actions or interventions which would reduce the inherent exposure and factors in recoverability
Often uses words such as 'significant', 'substantial', 'some', 'extensive', 'damage', that are open to interpretation and cannot be quantified	Provides essential outcome measures
Updated and reviewed periodically (quarterly, annually)	Ongoing monitoring and review of the essential outcome. In some organizations, this involves feeding in live information to anticipate and prevent disruptions

Table 3. The impact tolerance approach vs the traditional risk management approach

3.3.5 Balance strategic choices

When thresholds are identified for the EOs it is possible to examine each EO and make choices and changes to enhance resilience based on the four resilience intervention choices and four outcomes of resilience – 4Rs: readiness, responsiveness, recovery and regeneration. The choices include (Table 4):

Intervention choices and outcomes of resilience	
Controls to increase *readiness*	e.g. safeguards, add new plans or procedures, add codes of conduct, ensure compliance, find an fix errors, increase supervision/oversight/audit
Flexibility to increase *responsiveness*	e.g. add redundancy, add diversity, create flexibility (by design) empower people by giving them the freedom and discretion to act, develop teamwork and communication
Optimization to improve *recovery*	e.g. clarify existing roles and responsibilities, improve existing processes, reduce cost, improve monitoring, fix gaps in knowledge and skills
Innovation to increase *regeneration*	e.g. create safe spaces for experimentation, encourage informal networking , developing new capabilities, resources and ways of working, design thinking workshops

Table 4. Intervention choices and outcomes of resilience

3.3.6 Stress test thresholds

Organizations are tested every day by issues like near misses and incidents, which are learning opportunities. Resilient organizations review their successes and failures, assess them systematically, and record the lessons in a form that employees find open and accessible.

Incidents not only cause harm, service loss, or emergency but also generate surprise and shock. These incidents can create a mismatch between people's way of thinking (e.g. what is safe, secure, acceptable, ethical, tolerable, standard?) and their environment. Therefore, recovering from an extreme event requires a "full cultural readjustment … of beliefs, norms and precautions, making them compatible with the new understanding of the world". This can be supported by adaptive leadership from management, using design thinking in multidisciplinary teams. With many incidents, organizational learning often stops with the publication of 'lessons learned', overlooking 'lessons applied'. Without making changes in the way that work is done, only the potential for improvement exists.

3.4 Standards

There are various standards and norms for strengthening an organization's resilience. The five standards named below are the most common to be adopted by organizations to strengthen their resilience. It is important to note that the implementation of these standards should be tailored to the specific context and needs of each organization.

ISO 22301: This is the international standard for business continuity management. It provides a framework for planning, setting up, implementing, monitoring, assessing, maintaining, and continuously improving a documented system to prepare for, respond to, and recover from disruptive events as they occur.

ISO 27001: This is the international standard for information security management. It helps organizations manage the security of their information assets, such as financial information, intellectual property, employee data, or information entrusted by third parties.

ISO 31000: This is the international standard for risk management. It provides principles and guidelines for effective risk management in any organization, regardless of size, activity, or sector.

ISO 22316: This is the international standard for organizational resilience. It provides guidance on how to improve an organization's resilience by increasing its ability to respond to, and adapt to, changes and disruptions.

ISO 22320: This is the international standard for emergency management. It provides incident response guidance, including aspects of planning, setting up, leading, coordinating, executing, ending, and evaluating an incident.

3.5. Contribution by Security Risk Management to support the steps that help to enable resilience within the organization

Security Risk Management can support the steps to enable resilience within the organization by helping to create a mindset that building resilience cannot be assumed to be a one-time effort. Resilience is a moving target, ever-changing in response to the changing requirements of the context in which the organization works and the changing conditions it faces concerning its EOs. In supporting the mindset towards resilience, Security Risk Management can apply the 6 steps below and the questions that go with it (Table 5).

Therefore an answer to the management in this case can be to follow the steps below, which are necessary to enable organizational resilience in a progressive way. Following these steps can help in building the capacity for agility, adaptation, learning, and regeneration to ensure that the organization is able to deal with more complex and severe events (such as a pandemic, climate change, or cyber-attacks) and is fitter for the future.

Discuss for failure to avoid complacency and instill 'future thinking'. Ask what if? Ask what next? Encourage your people to speak up.	**Consider the connections** between the 'five capitals' to understand the potential impact of disruption on stakeholders, organization and on wider society .	**Understand what is important** to stakeholders and to society, the 'essential outcomes' (EOs). that require a high degree of resilience.	**Set impact thresholds** for EOs to determine tolerable limits that should not be breached, considering the impact on all five capitals.	**Make strategic choices** about resilience interventions by balancing control, agility, efficiency and innovation.	**Conduct stress testing** to determine whether you are able to remain within the impact thresholds irrespective of the threat.
What assumptions do people in the organization hold about failure?	What contribution will the enhanced resilience of the organization make to the overall resilience of your sector, community and society?	How is the EO delivered?	What would constitute an intolerable impact to the EO?	How progressive or defensive is the mindset in the organization?	How will the EOs be achieved during stress or disruption?
Do people openly discuss future failure, potential issues and mistakes?	How might the action or inaction of the organization impact the five capitals now and in the future (natural, human, social, built and financial?)	What might prevent the delivery or recovery of the EO?	How would disruption to an EO impact different customer groups, the organization, and the wider sector system?	How flexible or consistent is the design in the organization towards resilience?	What assurance do you have that alternative means and contingencies will enable you to meet EOs within impact tolerance under severe but plausible scenarios?
How are people tasked with spotting challenges, changes or potential disruptors on the horizon?		Could the EO be delivered by alternate means?		How do you balance tensions and leverage a 'both/and' mindset?	How will you test future opportunities and the choices you should (or should not) make today? How might those choices limit your options some years down the line?
Which future trends might provide new opportunities for the organization? What advantages could you develop?		Do we have sufficient flexibility to deliver the EO even in severe or extreme scenarios?		What further investment is required to maintain EOs within acceptable tolerance thresholds?	

Table 5. Steps that help to enable resilience within the organization

References

Adaptive leadership: Stress-Test Your Strategy: The 7 Questions to Ask (hbr.org) / Accessed 11072024

Design thinking: Design thinking, explained | MIT Sloan / Accessed 11072024

ISO 22301: ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements / Accessed 11072024

ISO 22316: ISO 22316 Security and Resilience | BSI Middle East and Africa (bsigroup.com) / Accessed 11072024

ISO 22320: ISO 22320:2018 - Security and resilience — Emergency management — Guidelines for incident management / Accessed 11072024

ISO 27001: What is ISO 27001? A detailed and straightforward guide (advisera.com) / Accessed 11072024

ISO 31000: ISO - ISO 31000 — Risk management / Accessed 11072024

Journey mapping: Journey mapping 101: What it is and why it's important | Valtech / Accessed 11072024

Lessons learned: Triple Loop Learning - NPC (thinknpc.org) / Accessed 11072024

(Service) blueprinting: Service Blueprints: Definition (nngroup.com) / Accessed 11072024

Stress test: Stress-Test Your Strategy: The 7 Questions to Ask (hbr.org) / Accessed 11072024

The five capitals model: The Five Capitals - a framework for sustainability | Forum for the Future / Accessed: 11072024

Why Organizations Need to Measure Resilience: https://www.rmmagazine.com/articles/article/2024/07/09/why-organizations-need-to-measure-resilience / Accessed: 11072024