Risk management

Solar's risk management is based on Enterprise Risk Management (ERM) and the Board of Directors' rules of procedure, which place the responsibility for risk management with the Executive Board.

The Executive Board is responsible for ensuring that the necessary policies and procedures are in place, that efficient risk management systems have been established for all relevant areas and are improved continuously.

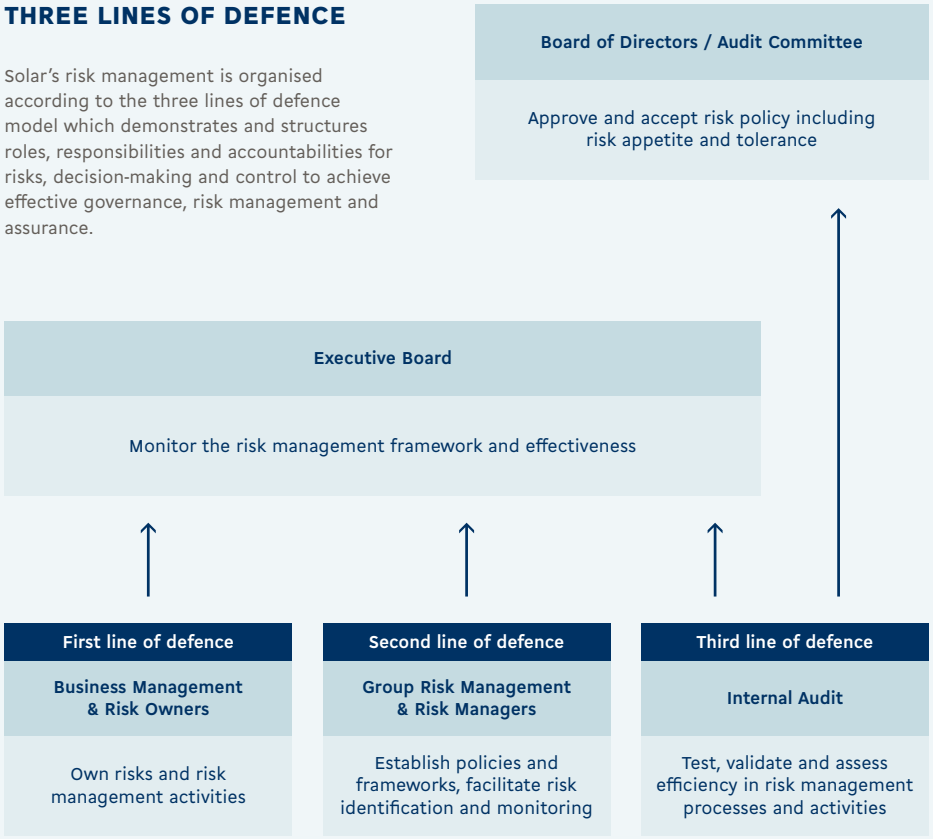
The overall purpose of the risk management initiative is to support the running of a robust business that is able to react quickly and flexibly when conditions change.

Solar's risk management efforts cover almost all Solar companies in Denmark, Norway, Sweden, the Netherlands, Poland and MAG45. The process supports national management teams in taking a structured approach towards risk management, with regular risk self-assessments anchored in the annual cycle. The data is consolidated at group level, and the findings are presented to the Board of Directors for approval.

The individual risk owners are responsible for mitigating risks to a level within Solar's risk appetite and tolerance. Throughout the year, Solar's Group Risk Management and local risk managers actively monitor the progress of this mitigation to ensure that risks are at an acceptable level.

THREE LINES OF DEFENCE

Solar's risk management is organised according to the three lines of defence model which demonstrates and structures roles, responsibilities and accountabilities for risks, decision-making and control to achieve effective governance, risk management and assurance.



Risk management

RISK DEFINITION

The focus of Solar's risk management is to identify and assess operational risks and operational aspects of strategic risks throughout the Solar Group. Solar defines these risks as events or developments that could significantly reduce Solar's ability to:

1) Meet profit expectations,
2) Execute the strategy, and/or
3) Maintain a licence to operate.

Solar works with the concepts of gross risk (inherent risk) and net risk (residual risk).

The gross risk effect is defined as the product of the impact and the probability of the risk materialising without any change in current risk mitigation.

The net risk effect is defined as the risk level when considering current as well as planned mitigation activities regarding both impact and probability.

RISK APPETITE AND TOLERANCE

Solar's risk appetite and risk tolerance articulate the extent to which Solar is willing to accept risks in five overarching categories: Governance, Strategy and Planning, Operations/Infrastructure, Compliance and Reporting.

Accordingly, the risk appetite outlines Solar's strategic outlook towards risk and defines the degree to which Solar is risk-seeking or risk-avoiding, while the risk tolerance, as an indicative parameter, outlines the level of net risk that Solar is willing to accept for a given measure of reward.

Risk appetite and risk tolerance are set by the Board of Directors and are reviewed annually.

RISK SELF-ASSESSMENT

Solar evaluates the effect of a risk based on a product of the probability of the risk materialising and the gross impact if the risk does materialise. In detail, the probability of the risk is defined as the expected frequency with which the risk may occur, while the impact is divided into three dimensions:

1) Effect on earnings
2) Reputational damage
3) Compliance (licence to operate)

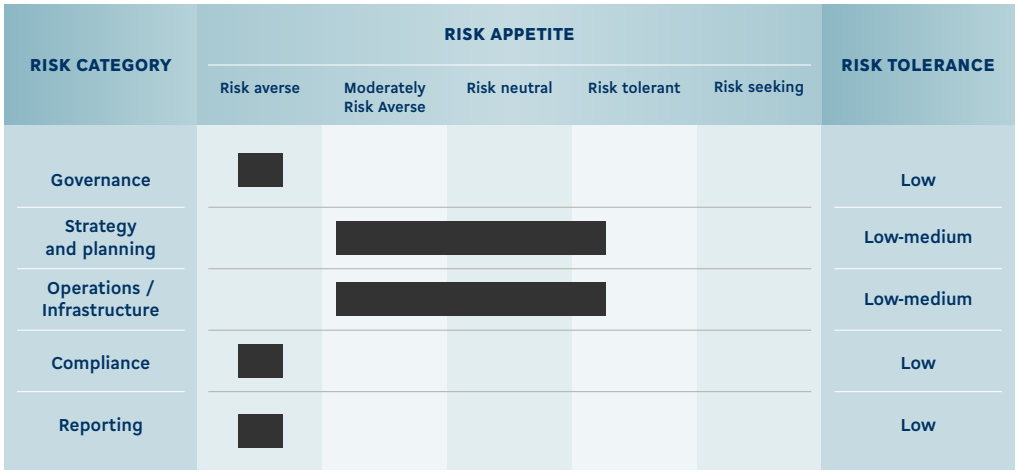
RISK HANDLING

The purpose of identifying and then handling risk is at all times to bring it to an acceptable level, which is in line with risk appetite and tolerance. In Solar, we work with four different risk treatment strategies when handling risks.

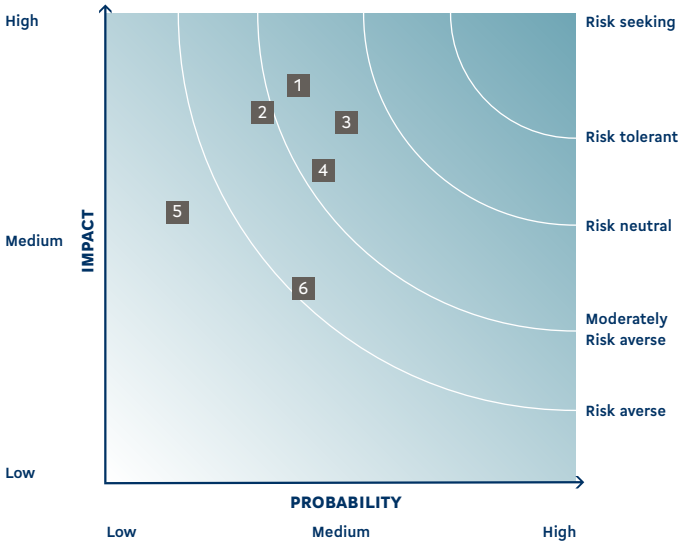
- Avoid – seeking to eliminate uncertainty by changing circumstances.
- Transfer – seeking to transfer ownership and/or liability of the risk to a third party.
- Accept – recognising residual risks and devising responses to monitor and control these.
- Mitigate – seeking to minimise risk exposure to below acceptable threshold.

The above strategies provide a number of formal responses to identified risks to help risk owners manage these.

RISK APPETITE AND TOLERANCE PER RISK CATEGORY



SOLAR RISK MAP 2018



Solar's top risks are mapped out in terms of probability and impact in the risk map. The overall risk picture is relatively stable compared to the previous year.

1 Cyber risk
2 IT interruption
3 Change management
4 Central warehouse breakdown
5 General Data Protection Regulation
6 Webshop upgrade

EXPOSURE TO POTENTIAL TOP RISKS AND MITIGATION

RISK	1. Cyber risk	2. IT interruption	3. Change management	4. Central warehouse breakdown	5. General Data Protection Regulation	6. Webshop upgrade
SCENARIO	Risk of exposure to IT breakdown and/or data breach due to cyberattack.	Generic risk of business interruption due to unforeseen events affecting IT operations.	Risk of failure to execute the sourcing and services strategy at a sufficient pace as a result of inappropriate mindset and/or a lack of competences.	Generic risk of unforeseen system and equipment's interruption or events such as fire, power outage, flooding or other natural or manmade disasters.	Risk of not meeting the requirements of the General Data Protection Regulation (GDPR) at an acceptable level. Although the regulation came into force in May 2018, it requires strong governance and continuous monitoring.	Risk of failure to harvest expected benefits from the implementation and development of the new e-business platform.
IMPACT	Business interruptions in the shape of data breaches, intellectual property theft and regulatory consequences as well as loss of reputation are among the consequences of cyberattack incidents, ultimately leading to financial losses. Despite the impact severity, the probability of the worst case scenario is assessed as relatively low.	Potential interruptions in the IT solutions area may result in financial losses and/or lead to reputational damage. Despite the impact severity, the probability of the worst case scenario is assessed as relatively low.	Currently, the assumed impact of this risk would be low revenue and profits from services sales. Further interruptions or delays in the area of strategy execution may lead to loss of competitiveness, a decrease in quality and customer trust as well as a loss of internal competence. All these factors will lead to a failure to meet profit estimates and, therefore, can influence Solar's position on the market.	Unwanted events may potentially lead to partial or complete warehouse breakdown. Accordingly, materialisation of this risk can result in financial losses as well as loss of reputation.	GDPR non-compliance may lead to severe financial and/or reputational consequences.	Failure to meet customer expectations, and/or failure to transfer customers from the current platform to the new one may affect the benefits assumed by Solar, and ultimately lead to the loss of competitiveness and decrease in profitability.
MITIGATION	Solar continuously strives to communicate appropriate internal information about security policies to uphold organisational awareness. Monitoring policies and procedures are in place for the main networks and systems. By ensuring new security tools or upgrading the existing ones, Solar continues to reduce vulnerabilities and monitors the network in search of unusual behaviours. Furthermore, external studies are performed regularly to assess the maturity level of Solar's cyber-resilience.	IT area is continuously monitored and evaluated. To lower the probability of the risk materialising, business-critical applications are mirrored at two central data centres in order to enable the business to run if one of these centres experiences downtime. Project teams improved through anchoring risk management in the project plans and defining relevant mitigating activities.	Solar's Executive Board continues to communicate how the main focus areas correspond with strategy execution and expected benefits. A series of initiatives were carried out to ensure clear priorities regarding daily business, adequate organisational structure and expected competences.	To reduce the probability of the risk materialising, Solar aimed to ensure the optimal warehouse management system. Experiences from successful implementation in one of the central warehouses were considered in planning and preparation for the next implementations. Additionally, external audits are conducted, the warehouse equipment's state is monitored regularly, and Group IT controls the overall performance. Several procedures are in place in case of a potential central warehouse breakdown.	Necessary precautions were taken in order to ensure organisational readiness before 25 May 2018. Solar ensured an adequate governance model for handling the risk in order to maintain customers' and investors' trust in the Solar brand. Increased efforts in the communications area have been initiated and will be continued in order to increase organisational awareness of the GDPR requirements.	Solar's mitigation efforts include recovery planning, product data enrichment, transparency in communication and testing. Further to feedback obtained from test customers, priorities were set and relevant actions were taken. Solar decided to onboard customers to the new platform in part to ensure the best possible customer experience. Until reaching full readiness for transferring customers from one webshop to another, two platforms will be in operation.