Exposure to potential risks and mitigation

IT breakdown

Scenario
Solar's activities rely heavily on IT solutions, and thus are exposed to interruptions.

Impact
This can result in financial losses as well as loss of reputation.

Mitigation
Most of the IT hardware is located at our two central IT data centres. To lower the probability of the risk materialising, all business-critical applications are mirrored at these data centres to safeguard IT operations, meaning that our business can continue to run even if one centre has downtime.

Several procedures are in place in case of a potential IT breakdown, including contingency plans with clear tasks and responsibilities. These contingency plans are updated regularly to decrease the impact should the risk materialise.

Our IT security board reviews IT security continuously and the IT area is meticulously and constantly monitored.

To mitigate IT risks, Solar continuously improves IT security governance and IT processes and procedures.

Central warehouse breakdown

Scenario
Solar's activities are heavily dependent on a fully functioning supply chain. Consequently, Solar's business is exposed to breakdowns from unforeseen events such as fires, power outages, flooding or other natural or manmade disasters that could potentially lead to partial or complete warehouse breakdowns.

Impact
Accordingly, materialisation of this risk can result in financial losses as well as loss of reputation.

Mitigation
To reduce the probability of the risk materialising, external audits are conducted regularly, while performance and software are monitored continuously by Group IT.

Several procedures are in place in case of a potential central warehouse breakdown, including contingency plans with clear tasks and responsibilities. These contingency plans are updated regularly to decrease the impact should the risk materialise.

Digitalisation / IT implementation

Scenario
Risk of increased exposure to business interruptions while working with digitalisation/implementation of new IT systems.

Impact
Solar is aware of potential risks of updating essential platforms which could affect the ability to conduct business. Thus, the implementation of new IT systems is considered a significant risk should unforeseen events or issues appear, which can potentially result in the loss of revenue.

Mitigation
Solar Group anchors risk management thoroughly in project plans with mitigations comprising among other things fallback scenarios, involvement of external experts and IT recovery plans.

Change management / strategy implementation

Scenario
Risk of failure to execute the sourcing and services strategy at a sufficient pace as a result of inappropriate mindset and/or lack of competencies.

Impact
Currently, the impact of this risk is low revenue and profits from services sales. In the long term, this situation will challenge Solar's strategic direction and ability to run a successful business.

Mitigation
To drive the execution of the sourcing and services strategy, a series of initiatives is executed including follow up tools, training, and organisational investments. Extensive communication on the advantages of the business transformation will bear a vital part of mitigating the risk.

Contract management

Scenario
Risk of entering into contracts with terms and conditions (e.g. liabilities and warranties) that exceed Solar's risk appetite.

Impact
The consequence of not complying with these contracts could be significant sanctions that are not proportional to the delivery and responsibility of Solar and exceed the commitment that the local subsidiary is willing to accept.

Mitigation
Contracts have been reviewed, and standard contracts for suppliers and customers adjusted according to the recommendations of a legal advisor. Escalation plans have also been reviewed, and clear guidelines on authority to sign contracts have been prepared. Focus will remain on these tasks and a new and improved standard contract for suppliers is under preparation.

To further mitigate the risk, Solar will introduce activities with the purpose of raising risk awareness within the organisation to always ensure the correct balance between risk and reward.

Cyber risk

Scenario
Worldwide, the speed and variety of cyber security events and crimes continue to intensify. Therefore, Solar must increasingly focus on protecting its critical operations, intellectual property and brands from cyber threats.

Impact
The potential impact of cyber risks is multi-faceted. 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 cyber incidents, ultimately leading to financial losses.

Mitigation
Solar works with a governance structure and strives to continuously communicate appropriate internal information about i.e. security policies to uphold organisational awareness. Monitoring policies and procedures are in place for the main networks and systems. Furthermore, external studies are performed regularly to assess the maturity level of Solar's overall cyber and information security management and to provide recommendations in order to ensure that we constantly improve in order to mitigate the changing cyber risk.

Financial risks

Financial risks are described in the notes of the consolidated accounts.

Control

Internal control is described in the statutory report on corporate governance available at:
www.solar.eu/investor/corporate-governance.