

# Definitions

---

## Cybersecurity Definitions

- **Risk assessment:** a process of identifying potential risks, analysing their likelihood and potential impact, and implementing measures to mitigate those risks.
- **Risk position:** The level of risk that an organisation faces.
- **Risk matrix:** A tool used to assess and evaluate risks based on the likelihood and consequence of a risk event occurring.
- **Likelihood:** The probability of a risk event occurring.
- **Consequence:** The severity of the potential impact of a risk event.
- **Risk rating:** A measure of the overall risk posed by a scenario, calculated by multiplying the likelihood and consequence.
- **Inherent risk rating:** The risk rating of a scenario without any measures in place to reduce the risk.
- **Current risk rating:** The risk rating of a scenario with existing measures in place to reduce the risk.
- **Target risk rating:** The desired risk rating of a scenario with additional measures put in place to further reduce the risk.
- **Risk assessment report:** A report that summarises the risk assessment findings, the risk mitigation strategy, and any recommended measures for implementation.
- **Avoid risk:** completely eliminate or forego risk.
- **Treat risk:** reduce the likelihood or impact of risk.
- **Transfer risk:** assign or move the risk to a third party.
- **Accept risk:** acknowledge the risk and choose not to resolve, transfer or mitigate.