Policy

Security

ID: POL-0022
Revision nr.: 6
Revision date: 12-01-2024

Policy

Security

Aker BP takes a risk-based approach to how it conducts its business.
To manage risks appropriately, the company must also account for risks that originate when malicious actors intentionally try to harm its interests. We call these "security risks" including cyber risk.

The purpose of security is to protect Aker BP's material and immaterial assets from malicious actors and unintentional security incidents.

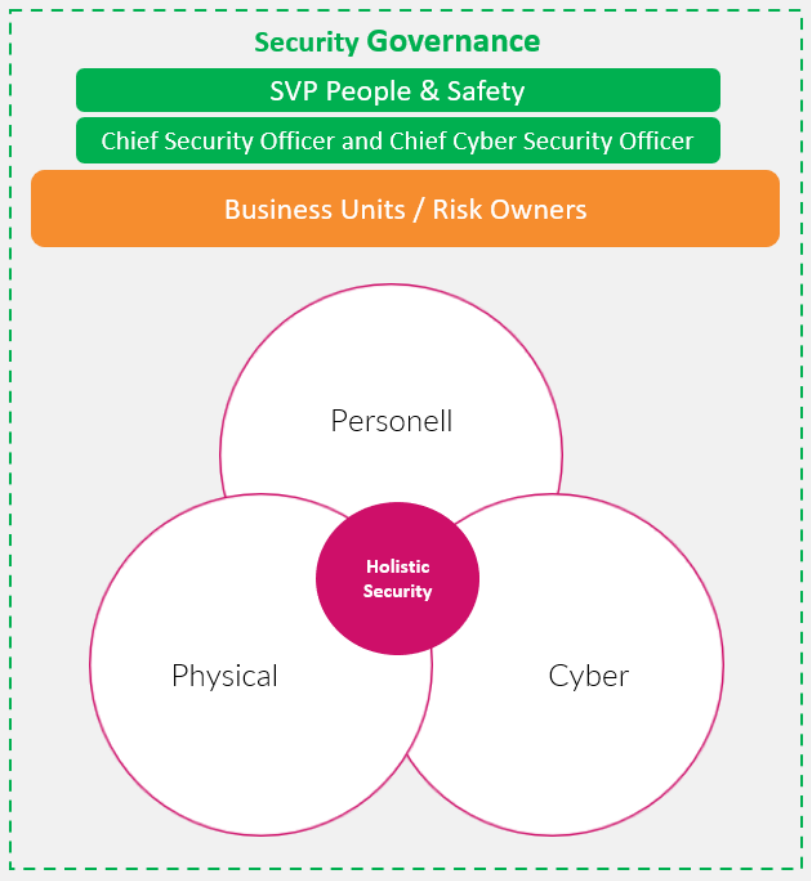
Audit and Risk Committee nominated on behalf of the board, oversee security with particular focus on cyber-security risk as part of their overall accountability towards risk governance and specific risks communicated through the Aker BP enterprise risk process.

The SVP People & Safety, on behalf of the administration (Executive Management Team), is the overarching subject matter accountable for Security in Aker BP. The Chief Security Officer (CSO) oversees Aker BP's holistic security and is responsible for governing Personnel and Physical security. The Chief Cyber Security Officer is responsible for governing Cyber security. The Chief Security Officer and the Chief Cyber Security Officer coordinate company-wide security risk management and governance.

Deciding and funding implementation of security barriers and security controls according to governance and risk, is the responsibility of each business unit according to financial authorization matrix.

Security risk shall be identified, monitored, analyzed, reported, and acted upon. Personnel, assets & facilities, information and digital systems shall be secured by adequate measures to control security risks within acceptable levels. This policy sets out principles designed to manage security risk that emerges from malicious actors' threat to Aker BP's material and immaterial assets and unintentional security incidents.

At any one time, Aker BP may face multiple threats, playing out on different attack surfaces (e.g., human manipulation, digital/cyberspace, physical assaults, psychological warfare, etc.). The company takes a holistic approach to security, meaning that mitigation and controlling security risk often require effort across multiple organizational entities and functions.



PRIN-0044 - Enable all employees to act securely

All personnel shall receive necessary training and education to act securely and follow the same security principles. Security background material shall be communicated in a clear and understandable fashion across the Company to ensure a fundamental awareness of relevant issues. A set of basic security rules applicable to all personnel shall continually reflect the Company's context and always be available in the Employee handbook. Personnel whose roles and responsibilities require additional competence and training shall be identified and provided with the necessary competence.

PRIN-0052 - Handle security risk in a uniform and systematic manner

Identification, monitoring, analysis, and management of security risk shall be handled through Aker BP's holistic security management system (SMS) framework and process coupled with the Risk & Barrier principles.

PRIN-0064 - Maintain an updated record of Aker BP material and immaterial assets

All material and immaterial assets shall continually be recorded. Asset value oversight enable effective cost/benefit prioritisation of defence against loss. Asset owner is responsible for ensuring an up-to-date value assessment.

PRIN-0066 - Maintain an updated record of threat actors

The threat landscape shall be continually monitored and analyzed to ensure our security controls and barriers (defenses) are relevant and appropriate. Threat actor profiles shall be recorded and kept updated. Insights from the threat library shall be used to estimate the likelihood Aker BP will face serious threats, and subsequently to assess overall security risk.

PRIN-0065 - Maintain an updated record of security controls/barriers and their weaknesses

All security barriers shall be documented in an approved system. The documentation shall include each barrier's status information to a level that makes it possible to evaluate its effect, limitations and/or weaknesses.

PRIN-0028 - Critical security incidents shall be prepared for, trained, and handled according to the emergency preparedness and response methodology

All critical security scenarios shall be prepared and trained for. If a security risk materializes it shall be handled through the emergency preparedness and response methodology (EPR). EPR is the risk/scenario-based framework it sets out training and handling of critical events and is designed to safeguard life, environment, assets, and reputation.

PRIN-0030 - Cyber risk from third parties shall not cause a significant risk towards Aker BP

Contracts and agreements shall include requirements ensuring cyber risk from third parties does not cause an unacceptable risk towards Aker BP. Third parties who digitally integrate or exchange data with Aker BP shall have security controls in place that are pre-approved prior operational use of the digital system or device in any part of Aker BP's digital infrastructure.

PRIN-0039 - Digital systems or components sending or receiving data on an Aker BP network shall be registered in an approved configuration management database and security monitored

Digital systems or components sending or receiving data on an Aker BP network shall be registered in an approved configuration management database and pre-approved prior operational use. System or component security shall be monitored. Approval is given from the owner of this principle and monitoring shall be done by the cyber security operations team.

PRIN-0002 - Cyber Security controls for digital systems

Security controls for all parts of the digital infrastructure shall be implemented according to company governance and requirements. This is required to ensure cyber security risk is managed, architecture principles are met and that the company ambition of end-to-end automation of processes is achieved.