Cybersecurity @ RWE

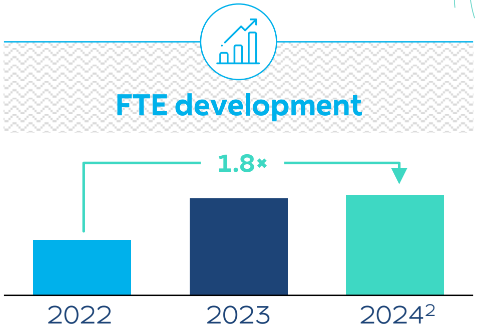
Disclaimer

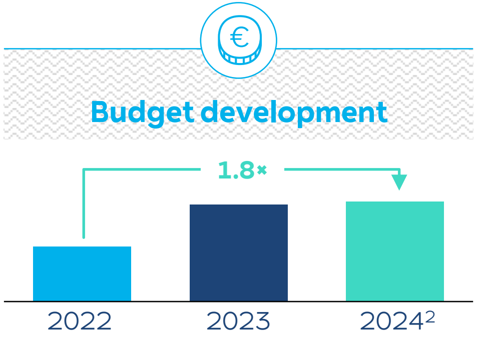
This document contains forward-looking statements. These statements are based on the current views, expectations, assumptions and information of the management, and are based on information currently available to the management. Forward-looking statements shall not be construed as a promise for the materialisation of future results and developments and involve known and unknown risks and uncertainties. Actual results, performance or events may differ materially from those described in such statements due to, among other things, changes in the general economic and competitive environment, risks associated with capital markets, currency exchange rate fluctuations, changes in international and national laws and regulations, in particular with respect to tax laws and regulations, affecting the Company, and other factors. Neither the Company nor any of its affiliates assumes any obligations to update any forward-looking statements.

Cybersecurity – Roles and Responsibilities

Increasing commitment and resources for Cybersecurity tasks

Roles	Responsibilities
CISO (Chief Information Security Officer)	• Coordinates cybersecurity within the RWE Group • Responsible for the groupwide strategy, regulations, targets, initiatives and processes for cybersecurity • Reports, regularly and, if necessary, on an ad hoc basis directly to the entire Executive Board of RWE AG on the cyber security situation within the RWE Group
BISO (Business Information Security Officer)	• Supports the CISO in the coordination and monitoring of the ISMS[1] in the respective Group company • Central contact for all cybersecurity requirements of the respective Group company
Governance & Risk	• Carry out compliance assessments and advise the business units and IT • Involved in the processes of exception handling and shall carry out regular reviews of the exceptions granted • Develops, evaluates and maintains the cybersecurity rules and regulations and any additional requirements • Monitors compliance by means of reporting and is responsible for cybersecurity risk management
Identity Governance & Architecture	• Responsible for development and maintenance of IT security architecture and design • Maintenance and development of identity- and access management
Cybersecurity Operations	• Coordinate and investigate major cybersecurity incidents incl. conducting forensic investigations • Collects, analyses and reports on the current threat situation (threat intelligence) • Implementation and operation of IT security measures, tools, technologies operational processes and SOC[3] management

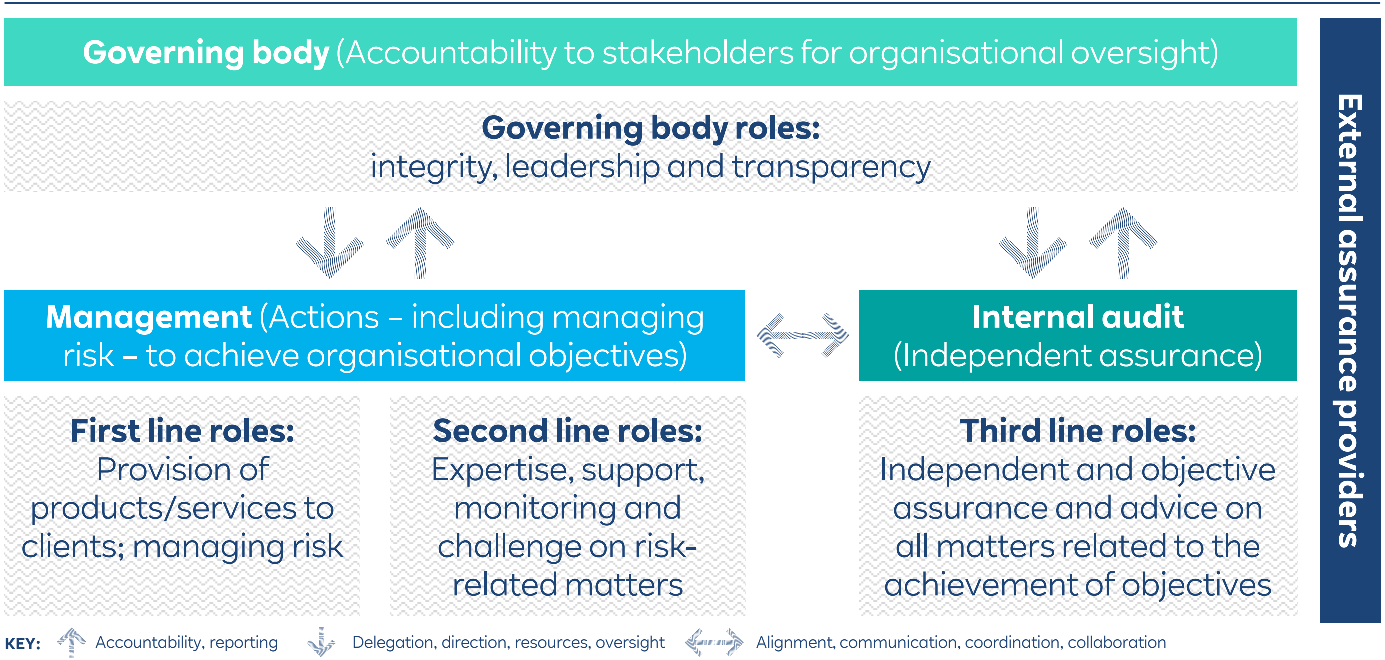

FTE development


Budget development

[1] Information Security Management System [2] Expected [3] Security Operations Center

Cybersecurity inside the IIA’s Three Lines of Defence Model @RWE

The IIA’s Three Lines Model



Governing body (Accountability to stakeholders for organisational oversight)

Governing body roles: integrity, leadership and transparency

Management (Actions – including managing risk – to achieve organisational objectives)

Internal audit (Independent assurance)

First line roles: Provision of products/services to clients; managing risk

Second line roles: Expertise, support, monitoring and challenge on risk-related matters

Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives

External assurance providers

KEY: ↑ Accountability, reporting ↓ Delegation, direction, resources, oversight ↔ Alignment, communication, coordination, collaboration

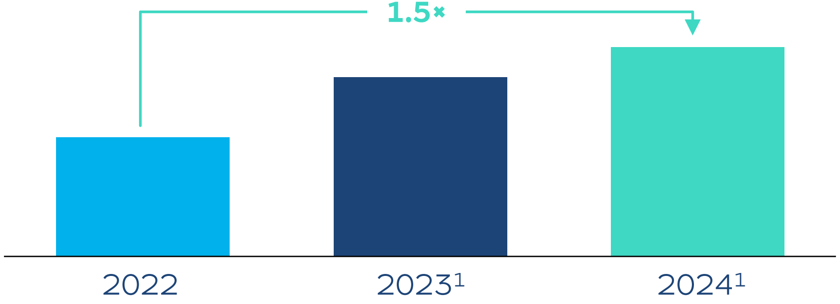
Cybersecurity part of second line role

Defines standards and methodology (e.g., provides directives, frameworks, tools, technologies and supports to enable the management of risks in first instance), controls and monitors first line roles

Continuous improvement @ Cybersecurity

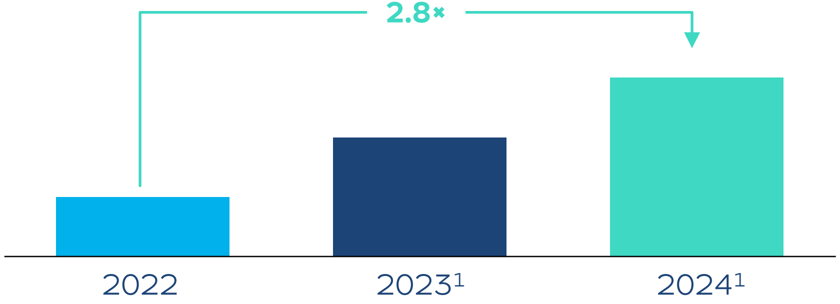
Business involved through Cybersecurity awareness trainings and assessments

Awareness user level



- Obligatory cybersecurity web-based trainings
- Additional risk-based approach of targeted and user specific trainings (e.g. admin trainings, gamification approach)
- Live hacking demonstrations
- Intranet articles on cybersecurity awareness topics are published
- Regular test-phishing mails and easy reporting implemented

Conducted cyber assessments



- Carry out compliance assessments and advise the business units and IT in determining criticality assessments, risk analyses, risk treatment planning and supplier assessments
- Processes of exception handling and carry out regular reviews of the exceptions granted

[1] Expected

Cybersecurity – Goals

A modern Enterprise-wide Cybersecurity is needed to protect RWE’s assets and interests

Goals

Detect cyber-attacks and anomalous activities that impact the organisation

Protect critical infrastructure for energy supply

Improving system resilience in a connected world

Identify actions needed to manage cybersecurity risk to the organisation

Ensure availability, integrity and confidentiality of sensitive information

Cybersecurity – Challenges

A modern Enterprise-wide Cybersecurity is needed to protect RWE's assets and interests

Challenges

- Changing threat situation
- Supply Chain attacks
- Rising regulatory requirements
- Fundamental changes of the energy system
- Increase of cyber-attacks worldwide