

TU DELFT INFORMATION SECURITY

Author: Jérôme Zijderveld, Chief Information Security Officer:
Version: 1.0
Date: Oct. 19, 2023
Classification: Public

TU Delft

Information Security

TU Delft's success increasingly depends on state-of-the-art technologies and digital information. Research and education are becoming increasingly "data driven" and massive quantities of real-life data are being collected and processed in real time. At the same time, ongoing digitalisation will usher in new information security risks.

Protecting the university and its people against growing threats and mitigating and managing new risks due to increasing dependencies places high demands on TU Delft's resilience. This will require the university to ratchet up its efforts at an organisational, process and technological level, but also calls for greater awareness and alertness among staff, students and guests connected to TU Delft.



This document describes TU Delft's approach to information security. This paper focuses on three matters:

1. Strategy: Vision and governance guiding the implementation of information security at TU Delft.

2. Themes: TU Delft's central information security themes.

3. Resilience: the precautions TU Delft has taken to prevent, identify and minimise any damage in the event of a successful cyber attack.

Strategy

Importance of information security

Digitised information processing is part of the foundation on which TU Delft aims to achieve its ambitions. Digital learning methods, exchange of large amounts of data and online collaboration inside and outside the lecture hall has become part and parcel of the daily work of staff and students. Security of information is therefore essential to continue achieving our education, research and valorisation ambitions and to protect our crown jewels.

Ambition

TU Delft's ambition is to pursue a structurally high level of information security and resilience. At the same time, we respect TU Delft's primary interests and stay committed to the TU Delft's strategic principles of accessibility (borderless education) and openness (open science).

Governance

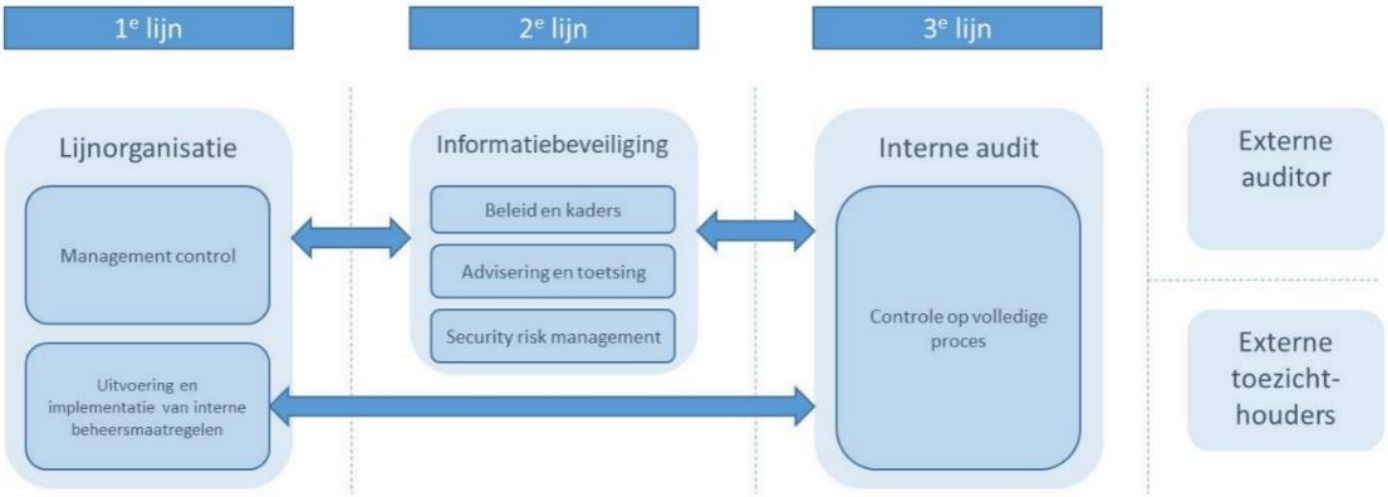
Plan-Do-Check-Act

The PDCA cycle provides an ongoing understanding of risks, security levels and weaknesses. The cycle describes the work we do every day to improve information security today and tomorrow.

Three lines of defence

In the university's information security governance, the information security function is closely intertwined with the executive organisation and with the internal audit function, as shown in the figure below.

The actors in this model provide quality control of the entire information security process and are responsible for its execution. Risk ownership, including ownership of information security risks, belongs to the first line.



Themes

TU Delft has identified several core themes to guide its information security efforts. This list is not exhaustive, but reflects the focus of TU Delft's information security function.

Leadership & governance

To make more emphatic use of the trailblazing role of the board and management within TU Delft (management buy-in) and to bolster execution (ability to execute).

Awareness & training

Activities generally focus on knowledge and behaviour of all end users and in particular users with elevated privileges.

Security operations & monitoring

Current capabilities have proven to be insufficient in the face of growing cyber threats, with detection of real and potential attacks and incidents becoming more common.

IT risk management

A risk-based approach to link threats to key information assets and identify the impact of information security risks on the organisation and primary processes.

Identity & access management

Thanks to periodic checks, inflow, throughflow and outflow processes, and the elevated privilege process, the right people have the right access to TU Delft data. Implementing advanced self-service, automation and flexibilisation in IAM processes enhances control and allows for better monitoring of user identities and rights.

Crisis management & resilience

The ability to respond appropriately in a security crisis and enhance the knowledge, skill and experience of the experts involved.

Public standards frameworks and legislation

Information security at TU Delft has been harmonised with the model information security policy outlined in the SURF Framework of Standards for Information Security in Higher education, which is based on the Maturity Model Information Security published by NBA-LIO and NOREA. As the collaborative organisation for Dutch education and research, SURF is committed to increasing the quality of education and research through IT innovation.

The tactical Baseline Information Security TU Delft (BIT) outlines the concrete components that make up the strategic information security policy. The BIT consists of a set of organisational, process, technical and human-centred security measures, based on the NEN-ISO/IEC27001:2017 and NEN-ISO/IEC27002:2017 standards (Code for Information Security).

Internal and external audit

One of the guiding principles for information security at TU Delft is a demonstrably established and auditable information security process.

The regular and risk-based internal audits reflect the current state of information security and are supplemented by an annual, external audit. TU Delft uses the recommendations arising from these audits to improve its information security.

Resilience

The steps taken by TU Delft to increase resilience can be divided into three categories: prevent, identify and respond.

Prevent

TU Delft has made considerable strides with regard to preventive measures for people, processes and technology. Examples include increasing employee awareness of cyber attacks, the standard use of Multifactor Authentication to add an extra layer of security to systems with sensitive information, and applying encryption to both managed devices and between sender and receiver.

Identify

TU Delft has taken several measures to help it identify cyber attacks, such as a 24/7 SOC, vulnerability scans and new roles in the security organisation to ensure that attackers can be identified more quickly.

Respond

TU Delft is renowned for its openness. To safeguard the university's open identity, rapid, strong response processes were put in place to limit damage and promote quick recovery in the event of an attack.

Examples of these response processes are the 24/7 standby shifts of the Security Incident Response Team (SIRT) and the Computer Emergency Response Team (CERT) to resolve incidents as quickly as possible and repel attacks, the regular (tabletop) drills to practice responding to playbook-based cyber attacks and OZON, the nationwide cyber crisis exercise.

Business Continuity Management

Business Continuity Management is becoming an increasingly important topic at Dutch universities and beyond. The purpose of Business Continuity Management at TU Delft is to provide the organisation with a structural backbone to help it prepare for major incidents and/or disruptions.

Information security precautions have been taken to minimise the impact of cyber attacks or major IT disruptions on the university's primary processes and to return to business as usual as quickly as possible.These precautions can be split into two categories:

Preparing for disruptions

These precautions focus on reducing - or eliminating - the chance of a disruption and its ramifications. Examples include:

- Internal & external backups
- Data replication
- Dual emergency power supply
- Capacity tracking
- Configuration Management Database
- Vulnerability and Patch Management
- Antivirus software and spam filters
- Redundant design of systems and networks.

Resilience during disruptions

These precautions focus on controlling and ending disruptions as quickly as possible. Examples include:

- The SIRT and CERT
- The organisation-wide crisis organisation
- Conducting business impact and risk assessments
- Applying appropriate security measures through data classification
- Anticipating potential threats based on a threat map
- Baseline Information Security at TU Delft
- Hybrid working capacity