# APPENDIX 2: BASIS FOR THE RISK MATRIX

Finanstilsynet's assessment of the main vulnerabilities in the financial sector, classified according to probability and the seriousness of the consequences for individual institutions, is discussed in this attachment. Based on observations and assessments in Chapters 3 to 7 and in section 8.1, the assessments below form the basis for the risk matrix in chart 8.1 in chapter 8.

The following definitions are used:

**Vulnerability:** Weakness in technical infrastructure, functions and processes that may result in undesirable incidents.

**Threat:** Factor with the potential to cause an undesirable incident.

**Risk:** Expressed as the combination of the probability of an incident and its consequences. Inadequate internal processes or systems or failure thereof, human error or external actors may increase the probability of an incident occurring, as well as its consequences.

**Consequence:** Results of an undesirable incident.

**Risk assessment:** Identification, analysis and evaluation of risk. A risk assessment lays the foundation for an institution's risk-mitigating measures and the priority given to them.

### Governance model and internal control

Finanstilsynet assesses the overall risk associated with vulnerabilities in the institution's governance model and internal control as medium. The probability of the three lines of defence not revealing serious weaknesses in the institution's internal control through their activities is assessed as medium and the consequences as moderate. This is based on the following assessments:

- The probability of failure to comply with laws and regulations not being detected as a result of inadequate supervision by an institution's operational management is assessed as medium and the consequences as serious.
- The probability of important requirements in governing documents not being implemented and operationalised, including controls, is assessed as medium and the consequences as moderate.
- The probability of the risk management function not having adequate ICT expertise to fulfil its second line functions in the ICT area is assessed as medium and the consequences as moderate.
- The probability of the compliance function not detecting serious weaknesses in operational units' control is assessed as medium and the consequences as moderate.
- The probability of the institution's board and executive management not possessing information that confirms or disproves compliance with internal and external requirements is assessed as medium and the consequences as moderate.
- The probability of the institution's board and executive management not contributing to ensuring that IT investments support the institution's strategy and needs, and not having the necessary understanding of the risk picture in the ICT area to ensure stable and secure ICT operations is assessed as medium and the consequences as moderate.
- The probability of unclear roles in the institution's first and second lines of defence leading to serious weaknesses in the surveillance and control of the institution's governance is assessed as medium and the consequences as limited to moderate.
- The probability of serious vulnerabilities not being detected as a result of deficient risk management between operational units and the risk management function in the second line of defence is assessed as low to medium and the consequences as moderate.
- The probability of serious weaknesses in internal control not being detected by the internal audit as a result of inadequate competencies and understanding of risk on the part of the institution's internal audit is assessed as low and the consequences as moderate.

- The probability of serious organisational challenges as a result of weak change management is assessed as medium and the consequences as moderate.

### Skills and skills management

At present, Finanstilsynet assesses the overall risk associated with vulnerabilities in connection with skills and skills management as medium. The probability of adverse incidents occurring or not being adequately managed as a consequence of a lack of skills in Norway is assessed as medium and the consequences as limited to moderate. This is based on the following assessments:

- The probability of the board and the executive management not maintaining a sufficient overview of employee skills and current and future needs as a result of inadequate skills management is assessed as low to medium and the consequences as limited to moderate.
- The probability of inadequate skills management in institutions resulting in the loss of and/or an inadequate supply of the skills necessary for sound operations is assessed as medium and the consequences as moderate.
- The probability of inadequate security expertise in institutions resulting in significant operational risks is assessed as medium and the consequences as moderate to serious.
- The probability of business disruptions and unavailable services as a result of insufficient skills is assessed as low and the consequences as moderate to serious.
- The probability of breaches of information security as a result of inadequate access to security skills is assessed as low to medium and the consequences as moderate.
- The probability of institutions' inadequate competence in services developed and operated by service providers resulting in breaches of laws and regulations is assessed as low to medium and the consequences as limited.
- The probability of increased dependence on foreign service providers as a result of lack of resources and rising needs in Norway is assessed as low to medium and the consequences as moderate.
- The probability of inadequate understanding of the risks attending the use of cloud services resulting in adverse incidents is assessed as medium and the consequences as moderate.
- The probability of inadequate competence in new technology, such as RPA, AI and blockchain, resulting in failure to identify significant operational risks when using such technology is assessed as medium and the consequences as limited to moderate.

### Vendor management

Finanstilsynet assesses the overall risk associated with vulnerabilities in vendor management as medium to high. The probability of adverse incidents is assessed as medium to high and the consequences as moderate. This is based on the following assessments:

- The probability of major irregularities in the service provider's internal control not being discovered by the institution is assessed as medium to high and the consequences as moderate to serious.
- The probability of security breaches occurring as a result of inadequate supervision and commitment to the security requirements by the service provider is assessed as medium to high and the consequences as moderate.
- The probability of an unacceptably long restoration time in the case of serious business disruptions due to unclear roles and responsibilities in the cooperation with the service provider and between service providers is assessed as medium and the consequences as serious.
- The probability of service unavailability as a result of inadequate monitoring of service quality is assessed as low and the consequences as moderate.
- The probability of undesirable dependence on service providers as a result of inadequate regulations (for example exit rules) in the agreement is assessed as low to medium and the consequences as moderate.

- The probability of undesirable dependence on service providers as a result of inadequate expertise on the part of the institution concerning the outsourced services is assessed as medium to high and the consequences as limited to moderate.
- The probability of inadequate (regular) risk assessments failing to detect weak sustainability on the part of service providers as a consequence of a difficult liquidity situation (bankruptcy risk), a challenging resource situation or other factors that may threaten the service provider's ability to deliver, is assessed as low and the consequences as moderate.
- The probability of serious weaknesses in a service provider's internal control not being detected through the work of a service provider's chosen auditor on an independent audit report is assessed as medium and the consequences as moderate.
- The probability of inadequate quality assurance of services acquired from different service providers and subcontractors as a result of deficient follow-up, lack of competence and failure by the service provider and subcontractors to acknowledge and comply with the institution's requirements, is assessed as medium to high and the consequences as moderate.

### Cybercrime

Finanstilsynet assesses the overall risk associated with vulnerabilities and threats causing damage as a consequence of cybercrime as high. The overall grade has not changed in this year's report, but Finanstilsynet considers the risk to be somewhat higher than in 2021 as a result of increased criminal activity, especially aimed at the institutions' customers. The probability of adverse incidents is assessed as high and the consequences as serious. This is based on the following assessments:

- The probability of serious weaknesses in an institution's defences not being uncovered as a result of non-existent or deficient security testing is assessed as medium to high and the consequences as serious.
- The probability of an institution having serious faults in its security configuration of critical systems as a result of failure to classify its systems is assessed as medium and the consequences as serious.
- The probability of an institution having serious faults in its security configuration of cloud services is assessed as medium and the consequences as serious.
- The probability of institutions being hit by a ransom virus with loss of critical business data as a result of malware (encryption) is assessed as medium and the consequences as critical.
- The probability of an institution not detecting criminals who have established a digital foothold inside the network before damage is averted is assessed as medium and the consequences as critical.
- The probability of criminals succeeding in exploiting vulnerabilities in networks and applications before being discovered (security patch applied) is assessed as medium and the consequences as serious.
- The probability of serious security flaws not being patched in time as a consequence of inadequate security updates (patch management), including at service providers and subcontractors, is assessed as medium and the consequences as serious.
- The probability of weaknesses in defences as a consequence of the institution not being in control of the vulnerability management of software and hardware and the associated configuration is assessed as medium and the consequences as serious.
- The probability of new applications or changes in existing applications being released into production with serious security flaws, also at service providers and subcontractors, is assessed as medium and the consequences as serious.
- The probability of third-party applications integrated by a third party in or between the institution's systems and its customers resulting in adverse security incidents is assessed as medium to high and the consequences as moderate to serious.
- The probability of employees or service provider personnel representing a significant vulnerability as a result of negligence and inadequate competence in secure use of the institution's systems is assessed as low to medium and the consequences as serious.

- The probability of criminals or foreign intelligence services attempting to recruit employees or service provider personnel to gain access to information about vulnerabilities in the digital infrastructure or other information about the institution, or of the institution's employees or service provider personnel being used involuntarily, through threats, as an instrument for a cyberattack, is assessed as medium and the consequences as serious.
- The probability of employees being used involuntarily, through social engineering, as a medium for a cyberattack is assessed as high and the consequences as serious.
- The probability of the institution's customers being used involuntarily, through social engineering, as a medium for criminals' financial gain is assessed as high and the consequences as moderate.
- The probability of the institution's customers being used voluntarily, through social engineering, as a medium for criminals' financial gain is assessed as medium and the consequences as moderate.
- The probability of disloyal employees exploiting vulnerabilities in the system for financial gain is assessed as low to medium and the consequences as limited.
- The probability of disloyal employees in the institution or personnel at service providers' development units planting malicious code in critical business applications is assessed as low and the consequences as moderate.
- The probability of employees or service provider personnel helping criminals to channel criminal transactions through an institution's systems is assessed as medium and the consequences as serious.
- The probability of personal data, including information about an institution's employees and service provider personnel who have roles that may be of interest to and exploited by criminals, falling into the hands of criminals is assessed as medium to high and the consequences as serious.
- The probability of institutions using methods of communication that are also used by criminals in their attempts at social engineering is assessed as medium and the consequences as limited to moderate.
- The probability of weaknesses in the establishment and use of security mechanisms creating new attack surfaces that will be used by criminals is assessed as medium and the consequences as moderate.

### Information leaks

Finanstilsynet assesses the overall risk associated with vulnerabilities and threats causing damage as a consequence of information leaks as medium to high. Finanstilsynet observes that the institutions have improved their efforts to prevent information leaks and are actively working on this to safeguard their values. The probability of adverse incidents is assessed as medium to high and the consequences as moderate. This is based on the following assessments:

- The probability of classified documentation being sent from the institution in an unauthorised manner as a result of lack of classification and control is assessed as medium to high and the consequences as moderate.
- The probability of confidential information going astray as a result of failure to control outgoing emails is assessed as medium and the consequences as moderate.
- The probability of confidential information going astray as a result of failure to control the use of USB storage media is assessed as medium and the consequences as moderate.
- The probability of confidential information going astray as a result of failure to control service provider personnel is assessed as medium to high and the consequences as moderate.
- The probability of confidential information that may be used to harm the institution intentionally or unintentionally being sent to or shared with external parties in an unauthorised manner is assessed as medium to high and the consequences as moderate.
- The probability of employees or service provider personnel operating as insiders and handing over or sending confidential information, such as lists of email addresses and login information, to criminals, is assessed as medium and the consequences as moderate.

- The probability of confidential information going astray as a result of lack of control or errors made when submitting information to customers is assessed as medium and the consequences as moderate.
- The probability of confidential information going astray as a result of use of portable equipment outside the office network is assessed as medium to high and the consequences as moderate.

### ICT operations

Finanstilsynet assesses the overall risk associated with vulnerabilities in ICT operations as medium. Finanstilsynet considers the risk to be somewhat reduced compared with 2021 as a result of the improved availability of payment services and other customer services. The probability of adverse incidents is assessed as medium and the consequences as moderate to serious. This is based on the following assessments:

- The probability of unstable and / or unavailable services as a result of increased integration among different service providers is assessed as medium and the consequences as moderate.
- The probability of operational problems as a result of errors in shared infrastructure is assessed as medium and the consequences as serious.
- The probability of operational problems as a result of inadequate competence and a lack of comprehensive understanding and overview of the institution's architecture and digital business processes is assessed as medium and the consequences as moderate to serious.
- The probability of impaired data quality as a consequence of complex integration among service providers is assessed as low and the consequences as moderate.
- The probability of operational problems as a result of inadequate change management (hardware, applications, databases, operating systems etc.) is assessed as medium and the consequences as moderate to serious.
- The probability of the agreed time for correcting critical errors not being adhered to as a result of the complexity of the system portfolio, entailing integration between new and old systems, is assessed as low to medium and the consequences as moderate to serious.
- The probability of monitoring of the IT environment not uncovering operational irregularities (for example expired certificates, databases, memory leaks and electronic components) is assessed as medium and the consequences as moderate to serious.
- The probability of operational problems as a result of inadequate follow-up of technical debt is assessed as low to medium and the consequences as moderate.
- The probability of the test system not being sufficiently similar to the production system is assessed as medium to high and the consequences as moderate to serious.

### Emergency preparedness and crisis management

Finanstilsynet assesses the overall risk associated with vulnerabilities in emergency preparedness and crisis management as medium to high. The probability of adverse incidents resulting in the activation of disaster recovery systems for critical business processes is assessed as very low to low and the consequences as serious to critical if the system does not function as intended. This is based on the following assessments:

- The probability of the institution's disaster recovery system not being established in accordance with its needs as a consequence of the absence of or inadequate business impact analyses and requirements is assessed as medium to high and the consequences as critical if the system has to be activated.
- The probability of institutions not being adequately prepared to respond to a serious situation as a result of deficient training and exercises is assessed as medium and the consequences as critical.
- The probability of the crisis management of an institution and its service provider being inadequately coordinated in the event of a serious incident is assessed as medium and the consequences as critical.

- The probability of institutions failing to handle a serious incident effectively as a consequence of unclear roles and responsibilities internally and between the institution and the service provider is assessed as low to medium and the consequences as serious.
- The probability of the disaster recovery system not functioning as intended owing to deficiencies in the technical set-up and infrastructure and testing of the system, as well as in the evaluation of the tests, is assessed as low to medium and the consequences as critical.
- The probability of inadequate updates, including security updates, of the disaster recovery system is assessed as medium and the consequences as serious.
- The probability of an institution affected by a serious digital attack not being capable of handling the situation effectively as a consequence of the lack of a contingency plan to handle cyber attacks and inadequate training and exercises is assessed as medium and the consequences as critical.

### Geopolitical factors

Finanstilsynet assesses the risk associated with vulnerabilities in relation to foreign operators that deliver critical ICT services to Norwegian institutions as medium to high. There were major changes in geopolitical factors in 2022 due to the war in Ukraine. The institutions have informed Finanstilsynet that the war has changed the threat picture from a cybersecurity perspective, although no increase has been reported in the number of incidents. The probability of adverse incidents when foreign service providers are cut off from delivering their services is assessed as low and the consequences as serious. This is based on the following assessments:

- The probability of an institution's disaster recovery personnel being able to maintain secure and stable operations in situations where foreign service providers are unavailable, is assessed as low and the consequences as serious.
- The probability of an institution's disaster recovery personnel not being able to maintain secure and stable operations in the event of serious ICT incidents where foreign service providers are unavailable, is assessed as low to medium and the consequences as serious.
- The probability of a breakdown in communication with foreign operators, whereby the foreign provider will be cut off from performing critical ICT services, is assessed as low and the consequences as serious.
- The probability of institutions being affected by geopolitical factors related to ICT operations is assessed as low to medium and the consequences as serious.

### Change management

Finanstilsynet assesses the overall risk associated with vulnerabilities in connection with change management as medium. The probability of adverse incidents is assessed as medium and the consequences as moderate. This is based on the following assessments:

- The probability of service unavailability as a result of non-functional changes (changes in the configuration of operating components) is assessed as medium and the consequences as moderate.
- The probability of weaknesses in change management procedures (including inadequate testing) is assessed as medium to high and the consequences as moderate.
- The probability of failure to establish adequate controls for identifying functional and non-functional changes that have been released into production without monitoring the change process, so-called unauthorised changes, is assessed as medium and the consequences as moderate to serious.
- The probability of functional changes (software) introducing vulnerabilities into institutions' defences is assessed as medium and the consequences as moderate.
- The probability of a high rate of change due to new business functionality and regulatory requirements resulting in solutions being put into production without the necessary quality assurance is assessed as medium and the consequences as moderate.

### Access management

Finanstilsynet assesses the overall risk associated with vulnerabilities in access management as medium to high. The overall grade has not changed in this year's report, but Finanstilsynet considers the risk to be somewhat higher than in 2021 as a result of reported incidents and completed inspections. The probability of adverse incidents is assessed as medium to high and the consequences as moderate. This is based on the following assessments:

- The probability of employees with extended access rights performing illegal actions is assessed as low to medium and the consequences as moderate.
- The probability of service provider personnel with extended access rights performing illegal actions is assessed as medium and the consequences as serious.
- The probability of employees or service provider personnel having access rights without the institution's executive management being aware of it is assessed as medium to high and the consequences as moderate.
- The probability of employees or service provider personnel having extended access rights without the institution's executive management being aware of it is assessed as medium to high and the consequences as moderate to serious.
- The probability of confidential information going astray as a result of inadequate access management and control of employees' accesses is assessed as medium to high and the consequences as moderate.
- The probability of confidential and/or classified information going astray as a result of a service provider's security breaches is assessed as medium to high and the consequences as moderate.
- The probability of service provider personnel, or a service provider's subcontractor's personnel, breaking rules while performing operating tasks is assessed as medium to high and the consequences as serious.

### Data quality

Finanstilsynet assesses the overall risk associated with vulnerabilities in connection with data quality as medium. The probability of adverse incidents is assessed as medium and the consequences as moderate. This is based on the following assessments:

- The probability of decisions being based on the wrong premises is assessed as medium and the consequences as moderate.
- The probability of the AML system not intercepting all payment transactions is assessed as medium to high and the consequences as moderate.