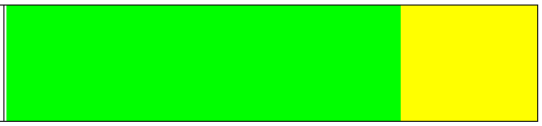
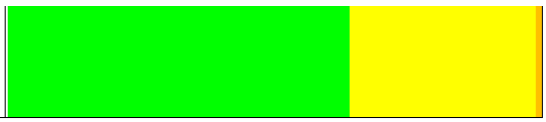
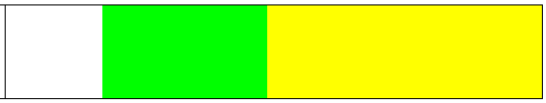
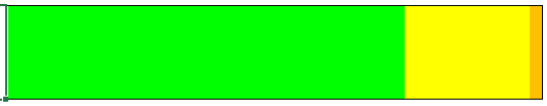
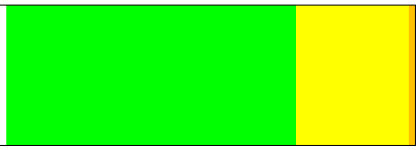
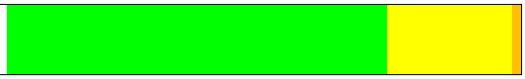
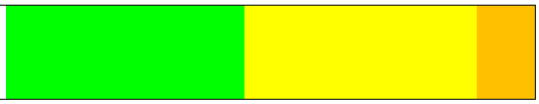
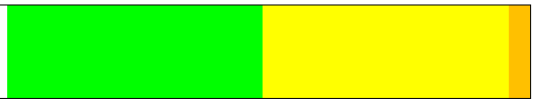
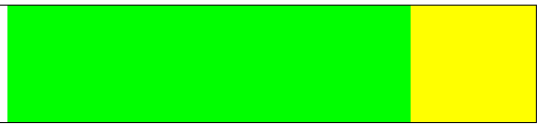
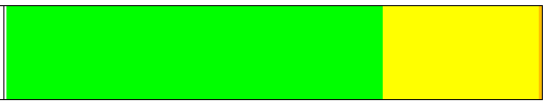
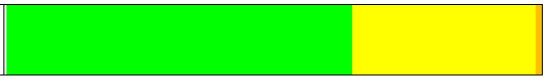
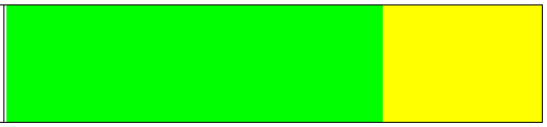
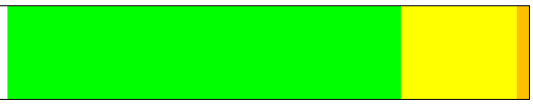
		Blank=N/A, green=low risk, yellow=intermediate risk, orange=high risk, red=very high risk	Trend
Governance	Reviews we conduct show that the ICT systems provide a good basis for, among other things, - management of the business, - control of customer engagement, and - internal reporting and reporting to authorities.		→
Governance	We have written policies in the area of ICT security, which are supported by written procedures. Policies and procedures are endorsed by management and subject to periodic review.		↘
Governance	We adhere to the principle of the three lines of defense, alternatively an internal model for risk management and control within the ICT area.		↘
Governance	We use recognized standards within ICT security.		→
Governance	We have policies that ensure that the ICT Risk Management Framework is a) reviewed annually and in in the event of serious incidents, and b) regularly audited by independent and qualified person		↘
Governance	We have no backlog when it comes correcting findings made during reviews of ICT activities.		↘
Governance	We have a well-established risk analysis process. Employees are familier with the process and actively and continously contribute to it.		↘
Governance	We collect information as a basis for assessing risk systematically and continously. The information can be analyses of anomalies and incidents, information from external sources, results of penetration testing, observations made by customers and employees.		→
Governance	ICT management annually reports the results of the risk assessment, including identified findings and recommended actions, to management.		↘
Governance	We maintain an inventory of mission critical ICT-equipment and software, including licenced software. Our configuration of technical equipment and software is adequately documented.		↘
Governance	We have a process for developing and improving a) the routines for ICT operations, and b) the control mechanisms to ensure compliance with the routines		↘
Governance	The ICT service agreements that support critical or important functions ensure the right to access, audit and supervision of matters relating to the outsourcing.		↘
Governance	We possess adequate and sufficient legal, technical and business expertise in the field of procurement and outsourcing.		↘
Governance	We follow up on our suppliers and the services that they supply with regard to service level (KPI), error correction and "lessons learned".		↘
Governance	We maintain a list showing which controls that are carried out by operation and development, risk and compliance, and internal audit (or other internal control set-ups), grouped into controls that contribute to integrity, confidentiality and availability of systems and data. Personnel responsible for the controls are listed.		↘
Governance	We conduct detailed risk assessments of our payment services operations. We have measures in place to protect payment service users from the risks identified, including fraud and the illegal use of sensitive data and personal information.		→
Governance	We maintain contact information for users of our service, and can quickly contact them if we suspect errors, or if we suspect fraud.		→
Governance	Employees have job descriptions. Job descriptions clearly define roles, responsibilities, and competency requirements.		↘
Governance	We have a employee security awareness program and employee security education program.		→

		Blank=N/A, green=low risk, yellow=intermediate risk, orange=high risk, red=very high risk	Trend
Integrity	We use controls to the extent possible that help ensure that our systems are not subject to unauthorized changes and that our services function as they should. Controls may include version control, code signing, work sharing ("four eyes principle"), checksums, sequence checks, etc.		↘
Integrity	We have controls that secure data in transit and at rest. The controls can be checksums, encryption, signing, access controls, and recovery routines (incremental backup).		→
Integrity	Logs are protected from modification and deletion. A time is associated with everything recorded in the log. All clocks used to record times are synchronized.		→
Integrity	We do not experience errors in applications and data that affect the integrity of the data (e.g. double entries, overwriting of customer data).		↘
Integrity	We collect information about operations, transactions and fraud, and use the information to make the services more secure and stable.		→
Integrity	We are continuously considering measures to protect the customer, such as 1) the ability to turn off features in the payment service (e.g. region blocking, internet blocking), 2) notification (SMS, email) when there are movements on the account or card, as well as in case of rejected access attempts, 3) continuous anti-fraud monitoring and 4) easy and good access to customer support.		→
Integrity	When developing new solutions, we consider the needs of all business areas to avoid challenges with "silo solutions", such as extensive program maintenance, complicated operations, and challenges with data synchronization.		→
Integrity	We do not allow employees on the business side or who work with reporting to develop their own applications (examples: Excel, MS Access, Python) that are used in our services or in our reporting to authorities.		→
Change management	We have good routines for change management and compliance with the routines.		↘
Change management	We have not made any changes where the current change procedures have not been followed.		↘
Change management	We have few changes that lead to unwanted incidents.		↘
Change management	The test systems are "production-like", meaning that test data (anonymized), applications, software, operating systems and hardware are the same in test as in production.		→
Change management	We make changes to the infrastructure ("non-functional" changes) when there is little customer activity, and can reverse the changes and roll back in a short time if necessary.		→
Change management	Før produksjonssetting utføres det sikkerhetstesting. Testingen gjøres av personer som ikke har vært involvert i utviklingen av tjenesten som testes.		↘
Change management	Before production deployment, security testing is performed. The testing is done by people who have not been involved in the development of the service being tested.		↘
Change management	The principle of division of labor is maintained throughout the change process, i.e. different people are responsible for development, testing, approval and production release.		↘
Change management	There is a low degree of complexity in the ICT systems. Clear areas of responsibility have been established that provide a good overview. Changes are handled in a way that ensures control and predictability, so that any consequences for other systems are assessed and addressed.		↘
Change management	Changes to ICT security controls (e.g. firewall rules) are approved by ICT Security before the change is implemented.		→
Change management	An increasing stream of new regulation increases the extent of changes in our systems.		↗

		Blank=N/A, green=low risk, yellow=intermediate risk, orange=high risk, red=very high risk	Trend
Operations	Over the past 12 months, we have conducted risk analysis, identified areas with a high risk of downtime (such as Single Point of Failure), and implemented measures to ensure continuous operation.		↘
Operations	We have an overview of the business processes and the ICT systems that support each business process. We assess the consequences for the business process (BIA) as a result of deviations or stops in the ICT systems. Based on the overview, we set targets for maximum time to restore normal operations (RTO) and maximum data loss (RPO).		↘
Operations	We regularly review plans, processes and procedures for continuity and recovery of ICT systems that support critical and important services.		↘
Operations	We apply recognized guidelines when using ICT service providers, such as the EBA Guidelines on outsourcing arrangements.		→
Operations	Our procedures for using ICT service providers define roles and responsibilities, as well as the competencies required to monitor and manage risks associated with the outsourced services.		↘
Operations	The collaboration routines and split of responsibilities between us and ICT service providers are detailed and precise.		↘
Operations	We keep the Register of Information (RoI) up to date (see (EU) 2024/2956) and have updated risk assessments of ICT service purchases. The second and third lines of defence have sufficient expertise and resources, and regularly follow up on the ICT service agreements and suppliers.		↘
Operations	The contracts with suppliers of ICT services that support critical or important functions regulate the support the supplier must provide in a situation where we want to change suppliers or switch to using our own systems.		↘
Operations	We have good measures in place to detect anomalies (abnormal load, abnormal use of ports/protocols, deviating response times, security incidents) in data traffic and take action before damage occurs.		↘
Operations	We have updated procedures for handling incidents, including cyber incidents. The procedures include rules for escalation and reporting.		↘
Operations	We test the ICT continuity and recovery plans for all systems annually, and in the event of significant changes to ICT systems that support critical or important functions		↘
Operations	We monitor "ticking bombs", i.e. components that gradually wear out, and values that gradually reach levels that require intervention, such as memory leaks, certificates that expire, electronic components that wear out, energy supplies that wear out (batteries, fuel for emergency power units), CPU utilization, RAM, disk.		↘
Operations	We have little "technical debt", which reduces risk when it comes to development and operations.		↘
Operations	We are experiencing less and less downtime in ICT systems that negatively affect business operations.		↘
Operations	Rights to administer systems and data ("admin rights") are granted where there is a business need.		↘
Operations	The interfaces that third parties use to access payment accounts are tested and approved in cooperation with the third parties. Errors that occur in the interfaces are fixed with the same priority as errors in our own solutions.		→
Operations	Interfaces used by third parties adhere to sequrity requirements set out in regulation.		→

		Blank=N/A, green=low risk, yellow=intermediate risk, orange=high risk, red=very high risk	Trend
Security	We have measures in place to protect ourselves against attacks (advanced persistence threat, trojans, ransomware, DDoS, email attacks). Examples of measures: Intrusion Detection and Intrusion Prevention, firewall, antivirus, web traffic control, email security, security updates, sandboxing.		→
Security	We have established a program for testing our digital resilience. For systems and applications that support critical or important functions, we test the digital resilience at least annually.		↘
Security	We perform vulnerability scanning of ICT systems that support critical and important functions on a weekly basis.		↘
Security	We check that security controls are appropriate and working as they should - annually for critical systems and at least every 3 years for non-critical systems.		→
Security	We have good procedures when it comes to security updates.		↘
Security	We have control over: - who has access to our data and systems (both internally and at suppliers) - what data and systems the user has access to - why the user has access rights - date for renewed assessment and identity verification of the user		↘
Security	Personnel have personal logon IDs. There are no "shared users".		→
Security	Logins that programmed processes make to systems and data are locked to the process so that personnel cannot use the login details to log in.		↘
Security	We have good access to ICT security expertise, including the expertise to set requirements for suppliers and follow up on delivery.		→
Security	We follow recognized standards that can contribute to the quality and security of the program code (for example, OWASP).		↘
Security	We are continually removing software that we no longer use, and software that is no longer supported by the vendor.		↘
Security	All remote access to our systems is done using VPN and two-factor authentication.		→
Data protection	We have good guidelines for classifying and protecting both structured (databases) and unstructured (Word, email, personal file areas) information.		↘
Data protection	We have good procedures for assigning, maintaining and controlling the rights that employees, suppliers, consultants and applications have in our systems.		→
Data protection	We log access to data and systems. If unauthorized access or attempted access occurs, an alert is sent and immediately followed up. We have controls that will notify if logging no longer works.		→
Data protection	We have divided the network into security zones based on a security rating of data and systems. The rating determines the level of physical and logical (access controls, encryption, etc.) security of data and functions in the zone. Zones for storing backup copies are included in the assessments.		↘
Data protection	We encrypt all data on portable devices.		→
Data protection	When terminating data storage agreements, the supplier must document that data has been irrevokably deleted.		→

		Blank=N/A, green=low risk, yellow=intermediate risk, orange=high risk, red=very high risk	Trend
ID theft	We have routines in place to stop a fraudster from hijacking a user-ID and use the ID in an unauthorized way,		→
ID-tyveri	We have routines in place to stop a fraudster from hijacking a customer-ID and use the ID in an unauthorized way,		↘
ID-tyveri	We require that the customer is subject to strong customer authentication in connection with e-commerce payments.		↗
ID-tyveri	We have good control over the provision, use and deletion of authentication tokens to customers.		→
ID-tyveri	We have controls in place that prevent "skimming" and "Card not present" fraud.		→
Internal fraud	Vi har gjort en detaljert risikovurdering og definert mislighetsscenarioer.		→
Internal fraud	We have defined a set of internal fraud scenarios that have a high likelihood of materializing.		↘
Internal fraud	To the extent possible, we impose dual control ("four eyes principle").		↘
Internal fraud	We monitor employee capital market transactions.		→
ICT supporting AML/CTF	Our ICT-systems present us with a composite picture of the customer, customer relationship and customer behaviour.		↘
ICT supporting AML/CTF	We have in place electronic monitoring of transactions and transaction patterns.		↘
ICT supporting AML/CTF	We have increasingly better precision when it comes to flagging suspicious behavior.		↘
ICT supporting AML/CTF	Transaksjonsovervåkingssystemet fanger opp alle mistenkelig betalingstransaksjoner.		↘
ICT supporting AML/CTF	The AML systems extensively use data from other systems.		↘
ICT supporting AML/CTF	With time, Our AML-systems gradually "learn" how to recognize suspicious money movements.		↘
ICT supporting AML/CTF	The sanction screening system has a high precision when it comes to recognizing listed persons and enterprises.		↘