part of eex group

Technical and Organisational Measures Due Diligence Questionnaire Catalogue

IT Strategy & Governance
14.06.2024

Ref. 1.0.5

Table of Contents

1. Disclaimer

While reasonable care has been taken in the preparation of this publication to provide details that are accurate and not misleading at the time of publication neither European Energy Exchange AG, hereinafter also as EEX, nor any other of DBAG's affiliates or their respective servants and agents (a) make any representations or warranties regarding the information contained herein, whether express or implied, including without limitation any implied warranty of merchantability or fitness for a particular purpose or any warranty with respect to the accuracy, correctness, quality, completeness or timeliness of such information, and (b) shall be responsible or liable for any third party's use of any information contained herein under any circumstances, including, without limitation, in connection with actual trading or otherwise or for any errors or omissions contained in this publication.

This document is published for information purposes only and shall not constitute investment advice respectively does not constitute an offer, solicitation or recommendation to acquire or dispose of any investment or to engage in any other transaction. This publication is not intended for solicitation purposes but only for use as general information. All descriptions and examples contained in this publication are for illustrative purposes only.

2. Scope and purpose

The following document outlines the specific technical and organizational control requirements by European Energy Exchange AG and its major service provider European Commodity Clearing AG and Deutsche Börse AG regarding Information Security and Data Protection, in order to assist our customers with their due diligence requirements concerning European Energy Exchange AG's business, services and practices. Within Deutsche Boerse Group (DBG), we have established common Information Security Framework and a common Data Protection Framework, implementing EEX requirements, with the express purpose of ensuring a consistent and standardised level of regulation that can be effectively utilised across the entirety of the group and across employed service providers. European Energy Exchange AG's Information Security Management System is fully aligned with the ISO27001 standard.

3. Corporate Introduction

3.1 The European Energy Exchange (EEX)

Is a leading energy exchange which builds secure, successful and sustainable commodity markets worldwide – together with its customers. As part of EEX Group, a group of companies serving international commodity markets. It offers contracts on power, natural gas, emission allowances, and freight and agricultural products. EEX also provides registry services as well as auctions for Guarantees of Origin.
More Information (www.eex.com)

3.2 What is the difference between EEX as an Exchange and EEX AG?

Both at a national and at an international level, the European Energy Exchange is one of the trading platforms which are subject to the most comprehensive supervision. At a national level, the supervisory mechanisms are based on a structure which is unique in Europe: while the company operating the exchange operates as a joint stock company under private law, the exchange as such, is an institution under public law which is subject to the German Exchange Act. As a result, EEX is subject to the same strict quality and supervision criteria as any other conventional securities exchange in Germany.
As a joint stock corporation under private law, EEX AG is permitted to operate the EEX exchange and, as a result, it has the right (and is also obliged) to operate the exchange. In this context, EEX AG provides the exchange with the financial, human and material resources required to carry out and further develop the exchange operations.

4. Overview of processes and controls

4.1 Governance / ISMS

There is an Information Security Management System (ISMS), based on legislative statutory, regulatory and contractual requirements as well as best practice international standards (ISO 27001), risk posture and threat landscape. The ISMS is maintained and regularly improved.

An Information Security Framework aligned with the ISO 27001 Standard is documented, approved, established, and maintained to manage risk and to continually improve information security. The core of the framework is comprised of a charter, policies, standards, and supported by guidelines, processes and procedures. Management and independent reviews of Information Security, including external audits by national and international authorities (e.g., Saxon State Ministry of Economic Affairs, Labour and Transport, Federal Office for Information Security (BSI)) and internal audits, are periodically conducted to ensure suitability, adequacy, and compliance with the requirements.

Information Security and Cyber Resilience Strategies have been designed and are continuously verified and enhanced. All information security responsibilities are defined, allocated and communicated. A security governance mandate/charter is documented and approved by the Executive Boards.
Chief information Security Officers (CISO) of EEX and of other DBG entities are appointed to fulfil the responsibilities outlined in the Information Security Framework.

Principal responsibility for overseeing data protection compliance resides with the Data Protection Officer (DPO), whose duties are detailed in Article 39 of the GDPR. DBG has introduced a Data Protection Management system based on GDPR requirements, adheres to the principle of data protection (privacy) by design and default Art. 25 GDPR and has an order and contract control in place. Data Protection Officer (DPO) of EEX and of other DBG entities are appointed to fulfil the responsibilities outlined in the Data Protection Framework.

The main goals for Information Security and Data Protection are to ensure Confidentiality, Integrity, Availability and Authenticity of data in accordance with Article 32 of GDPR.

An Information Security Report is presented to Senior Management and Executive Board of EEX on a quarterly basis. Additional standard reports are generated on a monthly basis.

4.2 Asset Management

4.2.1 Asset Inventory

An IT asset inventory has been established and is reviewed at least once per year or after significant changes, to make the vulnerability management process effective. The inventory contains information about asset ownership and further asset relevant/identifying attributes.

A software inventory including licenses status enables periodic software compliance verification.

Software installation must follow a change management process for regular and emergency software deliveries.
A record of processing activities according to Art. 30, 5 GDPR is in place to reflect personal data processing.

4.2.2 Information Classification

There is a defined process how Information Owners must classify information types and how the criticality is inherited to other assets like business applications or servers. The criticality must be documented in the asset inventory and is used to perform regular risk assessments on a risk-based approach.

4.2.3 Removable media management

Removable media are only used if there is a business need. Procedures and authorization levels for the management of removable media are documented. In principle, private data storage devices are prohibited on business premises, case-specific exceptions are only approved on request.
Data Leakage Prevention measures are in place to protect against unauthorized extraction of sensitive information:

- All hardware ports of the user equipment that can be used for connection of removable media are blocked and will only be enabled if there is a business need.
- In exceptional cases, only encrypted mobile data storage devices are used.

4.2.4 Disposal of media

Procedures are in place to identify the information items that might require secure disposal.
Data storage devices are disposed of in accordance with data protection requirements and destroyed by a vetted disposal firm.
Secure asset erasure procedures are followed to ensure proper data destruction prior to disposal.
Certificates of the secure destruction of media are obtained.

4.3 Risk Management

An Information Security Risk Management framework has been defined and integrated with the Information Security Management System.
Risk Assessments of information assets must be performed regularly and after significant changes, following a defined process. The results from the risk assessments are reviewed by the risk management team to ensure that gaps, potential threats, and vulnerabilities are adequately identified and assessed.
Information Security Risk Management methodology is periodically reviewed, improved and updated if necessary. All applied methodologies, processes, activities and major decisions regarding the management of information security risks are documented.
In order to facilitate the monitoring and reporting of risks a central Risk Register is maintained.

There are an Individual Data Processing policy and associated standard in place which define requirements for the use and replacement of IDPs / local applications to limit the risk of individual data processing. Via the implemented IDP process and tools, IDPs are identified and registered in a central IDP inventory, documented, and annually reviewed.
DBG's risk appetite framework constitutes the tools and concepts that are used to manage risks. The aim is to be able to monitor risks continuously and thereby manage risks according to the risk appetite. The aim of DBG's risk management framework is to set adequate and comprehensive risk management standards to ensure the sustainability of DBG's operations. An OpRisk management framework is in place which covers identification, measurement, monitoring and reporting of operational risks. Risk Owners are defined to manage and mitigate OpRisk within their assigned area of responsibility. The OpRisk capital is quantified, and the results reported on the Group and Legal Entities levels. In this context scenario analyses are carried out at least annually for all OpRisk scenarios. After final approval of the scenarios by the Risk Owner, Risk Management includes those into the economic capital model for DBG to sufficiently cover the residual risk exposure.

4.4 Exception Handling

For certain processes there are exception handling processes defined which support the conscious and adequate management of deviations from standard procedures. They are no replacement of the risk management process but are rather used for standard day-to-day operational activities (e.g., firewall rules, vulnerability management, URL access, etc.) where individual risk treatments would lead to inadequate and unproportional management overhead. The exception processes define under which specific circumstances deviations from standard processes and rules are only allowed and how they have to be documented and approved. Only if the defined criteria are met and the necessary steps are followed, exceptions will be granted to the requestor.

4.5 Secure development lifecycle

A secure software development process has been designed and must be applied:

- Development, test, and production environments are segregated
- Security testing must be conducted as part of the testing cycle in the Software Development Lifecycle (SDLC).
- There is a process for security code reviews which must be performed before major releases. In addition, a service is available to identify secrets in the source code and there are tracking capabilities to monitor the remediation of identified code vulnerabilities.

Sensitive data is protected:

- In principle, sensitive data must not be used for testing.
- In case sensitive/personal data must be used for system testing, approval by the information owner is required before production data is copied to a test environment, and an explanation must be provided. In those cases, these test environments must be secured with the same protection level as the production environment where the data is coming from. Access to these test environments must be strictly restricted and the data must be deleted immediately after the test has been finished. Sensitive data must be pseudonymized/ anonymized, randomized or deleted in development and test environments.

- Alignment with the Data Privacy Officer (DPO) is required in cases when usage of sensitive personal data is needed for testing purposes.
- Source code must only be housed in official, approved, and managed source code repositories to enable proper security oversight and controls (e.g., versioning control).
- For access to the individual code repositories in the DBG-approved central source code management system the need-to-know principle must be applied.
- Security documentation for each internally developed application must be created and is regularly reviewed based on the application`s criticality.

4.6 Access Control

4.6.1 Logical Access Control

User access management

For assets which require an authorization concept, the roles and user rights must be transparently declared and documented. The implementation of need-to-know and need-to-do principles are compulsory for authorization procedures and must be considered in the regular recertification process.

Where shared accounts are used, an Account Owner must be assigned so that traceability of actions to one individual is ensured.

For accesses where Multi-Factor Authentication (MFA) is required, only standard DBG approved solutions must be used as verification factors.

There is a central process to onboard users to the central Identity and Access management (IAM) solution which offers standardized onboarding, offboarding and user recertification capabilities. Through risk assessment process, it is verified if users are onboarded to the central IAM solution.

To reduce the risk of errors and fraud, it must be described in the authorization concept how Segregation of Duties (SoD) is achieved/implemented.

For authentication of users, applications and services should make use of the central Identity Provider (IdP) solution and federation concepts to prevent the use of additional password management systems and procedures as well as leverage proper authorization mechanisms. In risk assessments, it is verified if the central IdP is used or whether there are alternative authentication solutions used that potentially pose a risk to the service and organization.

Role owners / Line managers must ensure that Access recertification of user accounts takes place on a regular basis. The central Identity and Access Management team is supporting the regular recertification by providing recertification workflows via the central IAM tool.

Locked accounts to be released must follow DBG approved identity verification process.

Privileged Access Management (PAM)

Dedicated User accounts must be created corresponding to User Identities and used for privileged access.

Privileged access must be recertified regularly.

The use of privileged access is time-limited based on its criticality level.

Any interactive use of privileged accounts must be recorded by the central Privileged Access Management (PAM) tool.

Using the central PAM tool, Privileged Access sessions are monitored and recorded. Corresponding access logs which are sent to the central SIEM are analysed with regards to unauthorized privileged accesses, if any. In case unauthorized privileged access is detected, a defined escalation procedure is triggered.

System and applications access controls
Access to systems and applications must only be granted after prior login with Multi-factor Authentication (MFA), wherever applicable. Authentication information must be only validated on the target systems and not on client devices for gaining access to applications/services.
Access to data processing systems and workstations must be logged.
All default system or application accounts have to be removed, disabled, or have their default passwords changed.
There is an established onboarding process to transfer logs on real-time to the central Security Information and Event Management (SIEM) system to detect unauthorized access and investigate security incidents, if needed.
Screens of user devices are automatically locked after a defined inactivity time, requiring a password to gain access again. Interactive user sessions with applications / services must be timed out as well after a defined inactivity period. User's session validity should be reduced for critical applications/services.

Password management policy
Initial temporary passwords must be changed by the user immediately during first login.
Requirements and measures for password security are defined in the security standards. They contain requirements with regards to password complexity, password length, password history, account lockout, etc. which are aligned with industry best practices.
Provisions are in place if passwords or token devices are lost or forgotten.
Password reset or recovery process must follow DBG's established process.
Only authorized individuals and components can trigger the password reset process.
Passwords must never be displayed in cleartext during user authentication and must not be stored in systems in plaintext format, but in hashed format. Error messages in case of failed log-on must not provide any sensitive information to the user.
Account lockout occurs in case of repeated failed attempts, and owner of the account as well as corresponding supervisor must get notified.

4.6.2 Physical Access Control

Following controls are applied to control physical access:

- Business premises and buildings are monitored 24 hours a day, seven days a week by security staff.
- Opening of doors is technically monitored.
- Inspection patrols are carried out risk-based, where applicable.
- There are service contracts for technical surveillance systems.
- Adequate functional monitoring of surveillance systems, tamper detection and physical surveillance of access panels/cabling, critical bridge rooms, etc. is regularly performed.
- Identity checks are carried out by security staff.

- Access is only granted to authorized persons after checking and verifying identity.
- Offices are secured by a controlled key arrangement.
- The reception is staffed where applicable during core hours and receives visitors.
- Emergency exits are secured against improper use.
- Maintenance and repair staff are supervised.
- There are documented alerting and response mechanisms where appropriate environmental control thresholds have been breached.

Furthermore, there are additional controls for security zones:

- The data centre is segregated from office premises with strictly restricted access and surveillance.
    - Data centre sites are autonomous regarding site infrastructure, such as power, cooling and network connection
    - In buildings holding assets for multiple organizations, additional physical access security measures are applied
    - DBG data centres are regularly audited by independent third-party according to data centre audit standards
- Authorized persons are determined with respect to security areas.
- Access to security areas is traceable.
- Access rights to secure areas are regularly reviewed, updated and revoked when necessary.

4.7 Cryptography

4.7.1 General cryptographic requirement

Confidentiality, integrity and authenticity of data must be ensured by using cryptographic procedures aligned with industry standards and state-of-the-art. Details about adequate protocols, algorithms, procedures are defined in the Cryptography Guideline which has to be followed.

4.7.2 Data at rest

Data stored within DBG's internal infrastructures classified as "critical" or "major" with respect to confidentiality and/or integrity and/or authenticity or where the visible label of the data is "strictly confidential" or "confidential" must be protected by cryptographic measures.
Personalized security credentials must be stored in protected form (i.e., encrypted or hashed).
Personal data should be stored pseudonymized if possible, e.g., transfers personal data processed in such a manner that the personal data can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group, without the use of additional information (this is held exclusively and kept separately by the DBG entity in an EU Member State, as well as the algorithm or repository that enables re-identification).
Backups are protected according to its information classification.

4.7.3 Data in transit.

Communications leaving DBG's internal networks are protected by using a secure version of a standardized transport layer protocol.
A Virtual Private Network (VPN) solution is used for remote access which uses only DBG-approved cipher suits.

4.7.4 Key management

Keys must be generated and stored in a controlled and protected environment.
Access to key-encrypting keys (e.g., the key used by a certificate authority) is protected using the multiple-eyes principle.
Access to systems storing key material is limited to authorized people.
Critical keys like important key-encrypting keys or master keys are generally stored in a Hardware Security Module (HSM). Hardware storing key material is tamper-proof and certified according to industry standards.
Countermeasures are defined for potential incidents with regards to the management and use of keys, e.g., key compromise.
Clear guidelines are in place for critical key restoration, and it is ensured that only authorized personnel can access the data.
European entity is in control over keys chosen to protect personal data subject to the GDPR.

4.8 Human resources

4.8.1 Background checks

Pre-employment background checks are carried out on all candidates based on applicable employment law, such as criminal records and sanctions list checks.
Procedures for background checks are developed and documented considering laws and regulations and are annually reviewed.
Collected data is securely stored. There are defined rules and processes for employees start working for or leaving the company and for those changing their position within the company. Depending on the respective case defined onboarding, offboarding or recertification/review processes are triggered.

4.8.2 Terms and conditions of employment

Confidentiality or non-disclosure agreements specifically mentioning data privacy / information security responsibilities must be signed prior to being given access to EEX and/or DBG's information systems, facilities and information assets.
Information security requirements relevant for changes of employment are defined.
A documented and approved Disciplinary Process is in place in case of violations.
All DBG company assets must be returned upon termination of the employment, contract or agreement.

4.8.3 Information security awareness, education, and training

A comprehensive information security awareness and training program is established to ensure that personnel understand their responsibilities regarding Information Security.
All staff is required to complete the Information Security training upon hire, and at least annually thereafter.
The awareness and training program is updated at least annually.

Compliance with Information Security training requirements is monitored, and records are stored.
Additional training programs or awareness initiatives for specific aspects of Information Security are defined (e.g., risk assessments, information classification / labelling, phishing campaigns).

4.9 Network and infrastructure management

4.9.1 Network management and services

Network segmentation and segregation of network communication between applications, services and endpoint devices is defined and must be implemented. In this context the wireless network, leased lines to customers and internet facing systems are due their exposure clearly separated from the internal production zone.
Interfaces must be specified in the security documentation of relevant assets and are reviewed in regular risk assessments.
Only approved and authenticated devices can access the internal network. Access to networks and network services is logged and regularly evaluated for anomalies.

Unauthorized access from the internet is prevented by:

- Use of stateful firewalls at the perimeter.
- Web-application firewalls in front of public-facing web applications.
- All firewall rules are recertified at least annually.
- Firewall and router configurations are tamper resistant.

Distributed denial-of-service (DDoS) filtering capabilities are in place.
Anti-malware protection is installed/active in endpoints processing DBG data.
Anti-malware protection includes:

- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are deployed to analyse network traffic between network zones to identify attacks or misuse.
- Host-based IDS (HIDS) must be deployed on internet-facing servers to ensure higher protection for such exposed systems
- Proxies with web-filtering and malware protection capabilities.
- Regular update of malware signatures from vendor’s site and automatic deployment.
- Anti-malware solution installed on servers and email gateways scans all transferred files.

There is a separate network infrastructure for visitors.

4.9.2 Information transfer

Electronic communication is only performed with DBG authorized instant messaging services and by using DBG company E-mail accounts.
Transfer of DBG information to storage provided by third parties / Cloud infrastructure is allowed only for authorized and approved third party service providers. There is proxy filtering which blocks communication to internet websites and applications which are classified as inappropriate or malicious.
Corporate e-mails are always sent encrypted, either via a secure TLS session or via message encryption (if receiving gateway is not enforcing a TLS session).

4.9.3 Cloud Security

In DBG's standards and guidelines cloud security specific requirements are defined which are derived from best practices like the Cloud Control Matrix (CCM) or the Security Guidance of the Cloud Security Alliance. Resiliency must be ensured on every layer, i.e. on the meta structure/management plane, application, data and infrastructure layer.
The same or equivalent hardening requirements for the security of on-premises networks are applied for virtual networks in the cloud.
There are defined requirements for segregating networks to achieve isolation in the shared environment of a cloud service. Fulfilment of these requirements is verified within risk assessments on a regular basis.
Appropriate oversight of the use of cloud services is provided by the appointment of Chief Cloud Officers.

4.10 Mobile devices and teleworking

A standard specifying requirements for mobile devices' security is maintained.
All DBG mobile devices are configured to prevent data leakage:

- The device is automatically locked after a period of inactivity
- USB ports are disabled for mass storage media
- Access to the device is denied after several unsuccessful attempts
- Remote wiping of container-based solutions is possible.

The storage container of mobile devices, systems or data carriers is fully encrypted using DBG approved cryptographic measures to preserve their confidentiality. Company laptops/tablets run on supported operating systems and are kept up to date with all relevant security patches.
Where privately owned mobile devices (Bring-Your-Own-Device) are approved to process and store data, appropriate controls are implemented that ensure a separation of private and business usage supported by a software to protect business data on the private device.
Company laptops used for teleworking and remote access automatically establish a Virtual Private Network (VPN) connection to the corporate network. When no VPN connection is established, connectivity to DBG network is prohibited.
Two-factor-authentication is always in place for teleworking activities.
Split-tunnelling is prevented by ensuring that all VPN-Clients network traffic for remote access is routed to the VPN.
All mobile devices, systems and data carriers are disposed, destroyed or storages adequately deleted after end of use in accordance with applicable industry standards.

4.11 Data protection

Processes are established to meet the obligations established in the General Data Protection Regulation EU 2016/679 ('GDPR') and applicable national data protection laws and binding guidance of European and domestic data protection authorities. A repository for data processing activities (RoPA - Record of Processing Activities) at Deutsche Börse Group level is set up for compliance with article 5, 30 of GDPR – including responsibility for activities in the company.

Commissioned data processing as defined in article 28 of the GDPR is not allowed without a contractual basis and the principal's dedicated instruction including technical and organisational measures to ensure security of personal data by processors. Instructions should be compatible with the standards as mentioned in this document.
Contractual, technical and organisational safeguards are in place for data stored, processed, or accessible outside the European Union in accordance with articles 44 subseq. of GDPR if required.
The Standard Contractual Clauses of the European Commission are selected as preferred option. Additionally, transfer impact assessments are conducted to assess effective protection of personal data in third countries and supplementary measures are taken if deemed necessary.
Data Protection risk triggers are considered, and Data Protection Impact Assessment (DPIA) is performed for higher sensitive personal data processing if applicable.
European Energy Exchange AG and DBG must maintain records relating to services provided to the customer for the period required by law.
All processing activities including processing of personal data need to have a deletion concept in place to delete personal data when no longer needed for retention or other legal reasons (deletion concept).
Full cooperation regarding the return, deletion or erasure of all customer's confidential data or destruction of data carriers is guaranteed.
All activities processing personal data are defined with principle of data protection by design and by default (Art. 25) including principles such as data minimisation, data portability, data subject rights and processes for ensuring data accuracy as appropriate.

Group Data Protection Management system requires reporting of potential personal data breaches and complaints to the DPO plus subsequent reporting to the data protection authority in case of a risk to the affected individuals.

4.12 Data Leakage Prevention

A Data Leakage Prevention standard in place:

- Standard software images with anti-malware protection and deactivated administrator rights for users are installed in all DB workstation devices. USB ports are disabled for mass storage media.
- Conversations containing information that is categorized as internal or higher in public places or over insecure communication channels, open offices and meeting places are prohibited.
- Reports are in place for outbound E-mail, to control and monitor transmission of confidential data.

4.13 Change management

New systems and devices shall be configured with current security updates/patches and considered in a regular process which scans infrastructure assets for compliance with security baselines. Configuration attributes of all major information systems are stored in a centrally managed configuration management tool.

There is a standard change control process in place where changes are documented, approved by management, and communicated before they are initiated. It is guided by policies, procedures and controls.
Criteria for prioritizing and classifying the changes are defined.
Changes to operational systems and applications must be tested in a testing/development environment prior to being applied to operational systems. Changes to network architecture are as well subject to evaluation in a testing environment.
A process for emergency changes is defined. A Change Advisory Board must approve critical changes in regular operations and emergency changes to IT systems and applications.
Updates and patches are handled as part of the change management process.

4.14 Vulnerability management

Vulnerability detection measures are in place to ensure that vulnerabilities are identified in a timely manner.
Information about recently published vulnerabilities and emerging cyber threats is incorporated in the vulnerability management process.
In order to technically identify vulnerabilities, there are regular vulnerability scans performed. Depending on the asset type there might be network based vulnerability scans or authenticated vulnerability scans or a combination of both. Detected vulnerabilities are reported in the vulnerability management tool for proper tracking and remediation.
Vulnerability remediation activities are planned and prioritized according to consistent severity scores by asset owners and support groups.

4.15 Technical compliance reviews

Requirements for regular technical compliance reviews are defined in the Information Security Framework. There is a defined guideline which specifies how independent penetration tests can be requested and performed.
Penetration testing is conducted as defined in respective security standards and guidelines:

- Regularly on internet facing infrastructure and internet facing IT applications.
- Regularly according to criticality on critical internal IT applications and components.
- Regularly on wireless access points.

In addition, there is an onboarding process for configuration compliance scanning. Essential software components (e.g., operating systems, databases, webserver, etc.) must be configured according to defined security baselines. Via configuration compliance scanning deviations from those security baselines are detected, reported to the vulnerability management tool and need to be remediated by asset owners and support groups, respectively.
All potential vulnerabilities identified in vulnerability scans, penetration tests, configuration compliance scans, and security code reviews are reported to the asset owners and support groups respectively to commence remediation.

4.16 Logging and monitoring

There is a central process to onboard logfiles to the central Security Information and Event Management (SIEM) solution. By having relevant logs in the central SIEM, correlation rules can be applied, security-relevant events monitored in near-time and security incidents detected by defined use cases.
During risk assessments it is validated if relevant applications / systems are onboarded to the central SIEM. In case deviations are detected, a risk is documented in the risk register and the risk management process is followed.
In the security standards it is defined which data (e.g., authorization changes) must be logged and forwarded to the SIEM. There are mechanisms in place that prevent logs from unauthorized access and manipulation.
There are dedicated teams in Group Security Department, which are responsible for central use case lifecycle management, SIEM configuration and event policy definition, security orchestration and automation, threat landscape definition and monitoring, behavioural analysis as well as development and integration of AI functionalities across the security tool landscape.
Furthermore, a Security Operations Centre (SOC) is centrally performing security monitoring, incident detection, incident ticketing and vulnerability monitoring 24x7. A Cyber Emergency Response Team (CERT) is handling alerts (e.g., phishing attempts) which are reported to them.

4.17 Security Incident Management

4.17.1 Incident Response

Information Security events causing a breach of confidentiality, integrity, availability or authenticity are treated as security incidents.
In the event of an Information Security Incident, EEX will immediately take all appropriate measures to prevent loss or damage to customer information, disruption to the services provided, and damage or disruption to the information assets associated with the provision of services.
Documented and approved guidelines, processes, procedures and communication plans are prepared to ensure the prompt and consistent management of information security incidents:
An organized approach with defined steps has been adopted.

- Once the IS incident has been successfully dealt with, it is formally closed and archived
- Experience gained from responding to an incident is channelled into the further design and improvement of processes, during a lessons-learned phase.

There is a central Cyber Emergency Response Team (CERT) responsible of dealing with information security incidents.
Incident response playbooks for handling various IS incident scenarios are continuously developed to ensure efficient and effective response. Tabletop exercises are carried out and documented.
Every activity related to the handling of IS incidents and forensic investigations is logged and documented

4.17.2 Reporting Information Security events

Relevant reporting channels are defined, and responsibilities established to be able to respond to an incident, if necessary. Appropriate communication channels are provided for employees to notify the CERT team of IS events.
The existence of an IS incident or any relevant details will be communicated to affected and relevant parties (internal and external people or organizations) on a need-to-know basis.
Incidents impacting personal data are notified to the Data Protection Officer.
Relevant authorities are notified of relevant IS incidents in due time to satisfy regulatory requirements in the applicable jurisdictions.

4.18 Collection of evidence and root cause analysis

Procedures are applied for the identification, collection, acquisition and preservation of information that is susceptible of serving as evidence as soon as possible after the occurrence, to determine the extent of the compromise and identify its root cause.
Logs supporting information security incident investigations are securely stored in the SIEM solution. In case of forensic investigations further artefacts are kept in an inventory for an appropriate amount of time. Sound chains of custody are maintained.
Staff handling digital evidence is provided with adequate training.
There are defined requirements regarding the usage of an external vendor for the outsourcing of a forensic investigation.

4.19 Business Continuity Management and IT Disaster Recovery

To mitigate the availability risk of time-critical processes, a holistic and comprehensive Business Continuity Management (BCM) system is in place, integrated into DBG's and EEX's overall risk management framework. Business Continuity and Disaster Recovery plans, developed under supervision of a dedicated Continuity Management Function (2nd Line of defence) describe the approach for continuity.
The BCM system includes a dedicated IT Service Continuity Management (ITSCM) framework, as well as general guidelines for the design and implementation of Incident & Crisis Management processes, as far as relevant for business continuity.
Business Continuity Plans (BCPs) are a collection of information, guidelines and procedures which are compiled, developed, and maintained by the relevant organisational units for use in the event of a business disruption, an incident, emergency, or a crisis to maintain the continuity of critical operations.

IT Disaster Recovery Plans (IT-DRPs) are established by the respective asset responsible (if applicable: based on information provided by respectively involved 3rd party IT service providers) to document the IT related infrastructure and business application recovery, restoration and continuity to respond to IT disruptions that significantly impact Information and Communication Technology.
The overall impact of services, processes and resources unavailability is assessed via a Business Impact Analysis (BIA) that must be performed annually.
Recovery Time Objectives (RTOs) for organisational units and technology assets are derived from the annually conducted BIA.

There are plausibility checks as part of the risk assessments whether the implemented measures are adequate with regards to the defined RTO. In case deviations are identified, a risk is documented in the risk register and followed up according to the risk management process.
BCPs and IT-DRPs must be regularly tested (at least annually) to ensure their effectiveness:

- BCM and IT-DR tests results may trigger ad-hoc review of the Business Continuity Plan if weaknesses are identified during the execution.
- On a yearly basis or after major changes the test program must be reviewed and updated taking results of conducted tests into consideration.

Any identified deficits must be documented, and corrective actions and improvements planned and implemented by the respective owner. Further, BCM integrates with corporate Purchasing, Outsourcing, Material Change, Information Security, and Operational Risk (OpRisk) Management frameworks to ensure business continuity measures are pro-actively considered and implemented.

4.20 Data backup and recovery

Appropriate backup and redundancy measures must be implemented and documented to fulfil the availability requirements. Data / software backup and recovery arrangements are included in the design and operations of systems. Recovery Point Objectives (RPO) need to be documented in the security documentation for the relevant assets and aligned with the requirements of time-critical organizational units documented within the BIA.
The implementation of following requirements is reviewed as part of regular risk assessments of the relevant asset types.

- Backup facilities must be provided.
- Controls implemented on the main site must be extended to the backup site.
- Necessary hardware and software must be available, ready for use and in order to recover the original data by backup equipment.
- Completely redundant systems must ensure processing availability.
- An Uninterruptible Power Supply (UPS) with enough capacity must be installed.
- Redundancy of critical connections must be ensured.
- Data backup is protected against unauthorized access.
- The back-up copies are stored separately from the original data.
- Data will be deleted only after predefined data retention times.
- Approved backup solutions meeting data classification requirements are used.
- Controlled and regular backup of files, databases and applications must be ensured; as well as backup of the configuration of used cryptographic measures to ensure they can be quickly re-established.
- Tests of data backups must be regularly carried out and results are documented.

4.21 Supplier Security

Contracts with suppliers who have access to information assets of EEX and DBG or their customers include effective and enforceable confidentiality provisions containing Information Security requirements, which must be accepted before any information may be exchanged.

Weaknesses regarding the management and security of confidential, personal, or otherwise sensitive data or information on the part of the supplier are considered as reason for contract termination or legal prosecution.
A supplier security process is in place and covers the following topics:

- An up-to-date register of direct subcontractors or service providers is maintained.
- Subcontractors are required to assist notifying data breaches.
- Agreements with suppliers include requirements to address the Information Security risks associated with information and communications technology services and products within their supply chain. These risks are reflected in the risk assessment process and included in the Risk Register.
- Compliance with EEX and DBG's information security control framework is validated prior to granting access to direct subcontractors or service providers with access to DBG data.
- Comprehensive monitoring and review instruments measuring adherence to information security requirements are in place.
- The contracts specify responsibilities of the supplier for conducting background and qualification checks of supplier's employees.
- Agreements include provisions related to the secure transfer of business information.

4.22 Regular testing, assessment and evaluation

DBG has a process in place for regular testing, assessment and evaluation of its technical and organisational measures in place leading to an iterative improvement of taken measures to keep the implementation of measures as state of the art and in accordance with new legal and technological developments.
All measures taken are subject to regular internal subject-matter expert, control function and external control function audits.

5. Glossary

Business Continuity Management (BCM)	Organizational unit responsible for establishing efficient emergency and crisis management for systematic preparation for coping with loss events, so that important business processes are not or only temporarily interrupted even in critical situations and in emergency situations. BCM is also responsible to align with respective units and to develop measures to prevent such events.
Business Impact Analysis (BIA)	Process of evaluation and valuation of the potential negative effects to the business processes as a result of a disaster, accident or emergency.
Distributed Denial of Service (DDoS)	A technique that uses numerous hosts to perform an attack to disturb the availability of services.
Cyber Emergency Response Team (CERT)	A cyber emergency response team is an expert group of persons that handle information security incidents.
Data Protection Officer (DPO)	Person responsible for ensuring compliance with data protection within an organization. The person can be an employee of the organization or an external data protection officer and must not be in conflict or at risk of self-regulation.
General Data Protection Regulation (GDPR)	It is a regulation which was drafted and passed by the European Union (EU) and which defines data privacy and protection requirements that have to be fulfilled when collecting/processing data of people in the EU.
Hardware Security Module (HSM)	Hardware security devices which provide a specific level of tamper-resistance. This device is often used to securely generate, apply and protect sensitive cryptographic keys.
Identity and Access Management (IAM)	Identification, implementation, and maintenance of access rights to corporate assets (including applications) via central Identity and Access Management and regular recertification.
Individual Data Processing (IDP)	Form of data processing, for which end users as users of an IT system, or application, define and execute a work activity. IDP includes changes to data and content, processing of data used as input for other operational processes, management board and supervisory board reporting and external reporting. This is achieved by employing individually defined functionalities on the basis of standard software, typically office desktop applications, at the employees work desk and under individual responsibility of the employee, i.e., independent of the standard processes for Regular Applications (e.g., for development, testing, approval and implementation) and tailored to the individual needs of the employee or department.
Intrusion Detection System (IDS)	Device or software application that monitors a network for malicious activity or policy violation.
Information Owner	The Information owner is responsible for ensuring that the information for which he/she is responsible is provided with the necessary and appropriate protective measures. Furthermore, the information owner assumes the risks arising from the use or misuse of the information for which he/she is

	responsible. At DBG, the Information Owner is generally a member of the Management Board of the LE or AG.
Information Security Management System (ISMS)	An information security management system (ISMS) includes all of the policies, procedures, documents, records, plans, guidelines, agreements, contracts, processes, practices, methods, activities, roles, responsibilities, relationships, tools, techniques, technologies, resources, and structures that organizations use to protect and preserve information, to manage and control information security risks, and to achieve business objectives. An ISMS is part of an organization's larger management system.
LE Chief Information Security Officer (LE CISO)	A legal entity chief information security officer is responsible for implementing the security strategy and security framework in the respective legal entity to ensure adequate protection of people and physical assets. The LE CISOs work in close collaboration with the CISO of DBAG to ensure a high level of compliance and security.
Risk Register	In the information security context, central Information Security risk inventory, where all risks, e.g., resulting from the plan to implement new functionalities with information security impact, are maintained and tracked. Risk entry in the Risk Register is part of the Risk Assessment process; the follow-up is part of the Risk Register process which is out of scope in this document.
RPO	Point in time to which data must be recovered after a disruption has occurred.
RTO	Period of time by when minimum levels of IT services and/or products and the supporting systems, applications, or functions must be recovered after a disruption.
Secure Development Lifecycle (SDLC)	Defined process which needs to be followed when developing code for applications/services.
Security Information and Event Management (SIEM)	Security information and event management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis of security events, as well as a wide variety of other event and contextual data sources.
Transport Layer Security (TLS)	Hybrid encryption protocol for secure data transmission over the Internet (deprecated predecessor: Secure Sockets Layer, SSL).
Uninterruptible Power Supply (UPS)	Device which provides emergency power in case there are failures of the power supply (e.g., disturbances of the power grid or certain power connections).
Virtual Private Network (VPN)	Gateways that are used to establish a secure cryptographic channel between communication partners. Furthermore, VPN is used for secure connection of remote users to a company's internal network.