Overview of Internal Controls

Bloomberg

2025/2026

Disclaimer

This Overview of Internal Controls includes confidential information from Bloomberg. By accepting this document, you agree that, without the express written consent of Bloomberg, you will not disclose to any person outside your firm the fact that this document has been provided to you or the contents herein. Please note that the information provided in this document is for informational purposes only, is subject to change, and is being provided by Bloomberg without any representation or warranty, express or implied, as to the accuracy or completeness of such information. At all times, Bloomberg shall retain sole control over the maintenance and operation of the policies and procedures detailed herein. Provision of applicable services is subject to agreement to the terms and conditions of a definitive, final contract. In the event of any inconsistency between this information and the terms of a final contract, the terms of the final contract shall govern.

Table of Contents

Overview of Internal Controls

1. Introduction 4
2. Document Ownership 5
3. Organization and Governance 6
4. Enterprise Risk Management (ERM) 7
5. Bloomberg Policies, Standards and Procedures 9
6. Vendor Management 11
7. Asset Management 13
8. Human Resource Management 14
9. Physical and Environmental Security 15
10. Incident Management 17
11. Access Control 18
12. Business Continuity 20
13. Disaster Recovery 22
14. Information Security 24

1. Introduction

As a leading global provider of data, news, and analytics, Bloomberg is committed to ensuring and maintaining the protection of our infrastructure and the data contained within. Advances in technology have enhanced and improved the way the world conducts business. Bloomberg recognizes that these advances bring both benefits and challenges in maintaining the security, confidentiality, integrity, and availability of information.

The purpose of this document is to provide an overview of Bloomberg's information security program and other internal security controls that are currently implemented to help ensure the confidentiality, integrity, and availability of the products and services we offer. The security controls may be administrative, physical, logical, or technical in nature, and operate to ensure that adequate coverage exists to protect our systems and data. Bloomberg's management has established a process to guide the development, maintenance, and monitoring of the internal controls environment.

This Overview of Internal Controls document is a living document and will continue to be enhanced based on changes in the operating environment. This will aid Bloomberg in keeping pace with new and evolving threats, risks, and solutions in the marketplace today.

2. Document Ownership

This document was prepared by the Chief Risk Office at Bloomberg. For questions and clarifications, please contact brco@bloomberg.net.

3. Organization and Governance

3.1 Overview

Leadership of Bloomberg is comprised of various groups and committees; a selection is below:

3.1.1 Board of Directors

The Board has deep experience in finance, technology, media, philanthropy and government, and oversee the company's operations, finances, and legal & compliance obligations and advise how to operate effectively in relation to Bloomberg's business strategy.

3.1.2 Management Committee

Bloomberg's Management Committee helps oversee corporate strategy and operations. Business leaders consult and update Management Committee members on strategy and related topics on a regular and ad hoc basis. The Management Committee provides strategic direction to ensure alignment with business objectives, supports resource allocation, and raises relevant topics with the Board of Directors. The Management Committee is composed of eight members: the company Founder (Michael R. Bloomberg), Co-Founder, Chair Emeritus, Chief Executive Officer, President, Chief Financial Officer (CFO), Chief Legal Officer and the CEO of Bloomberg Philanthropies.

3.1.3 Chief Risk Office (CRO)

The Chief Risk Office works closely with the Management Committee and the organization as a whole to provide oversight and management support around information security at Bloomberg. The CRO is led by the Chief Risk Officer, who has a reporting line to the Management Committee and the Audit, Risk and Compliance Committee. The Chief Risk Officer is responsible for the management of multiple teams including Enterprise Risk Management (ERM), Risk Strategy and Operations, Vendor Risk Management, Data Governance and Risk and Compliance Shared Services.

3.1.4 Chief Information Security Office (CISO)

The Chief Information Security Office is ultimately responsible and accountable for the design and implementation of the information security program. The CISO is led by the Chief Information Security Officer, who reports directly to the Chief Legal Officer. The information security program sets the strategic direction for the implementation of appropriate security measures across Bloomberg. The CISO is responsible for identifying risks and defining adequate levels of information security controls based on the risks. These teams also provide guidance on the implementation of security controls across the organization. The CISO works closely with several departments, such as HR, Legal/Compliance, Engineering, and Technical Operations on implementation activities. In some cases, the CISO is also responsible for the implementation of the controls.

3.1.5 Internal Audit

The Chief Audit Executive responsible for managing the Internal Audit's function reports functionally to the Audit, Risk, and Compliance Committee (ARCC) and the ARCC reviews and approves the organizational structure of the Internal Audit function. The ARCC reviews and approves, on an annual basis, Internal Audit's mandate, Internal Audit Plan, Internal Audit budget and staffing. The ARCC ensures that the Internal Audit function is independent and objective. The ARCC reviews the results of Internal Audit projects and reviews the updates provided by the Internal Audit function on management's progress in remediating and in actioning management's response.

4. Enterprise Risk Management (ERM)

Bloomberg recognizes risk-taking as a fundamental characteristic of the company's culture. Bloomberg has implemented a risk management program across the organization that is aligned to business objectives and industry best practices. Risk Management is embedded in day-to-day business. The Enterprise Risk Management (ERM) team is responsible and accountable for the design, implementation, and monitoring of the risk management program. The ERM team is a function separate from the business, part of the second line of defense that reports directly to the Chief Risk Officer. The ERM team develops central policies and procedures to identify, assess, and manage risks and related controls and issues. The key objectives governing the program are:

- to set the standards to enable risk management across the organization;
- to enable tools, workflows and training to support risk management; and
- to monitor and report on risk information for decision making.

4.1 Risk Management Processes

The ERM team develops the central framework and processes for risk management. Using a risk-based approach, the ERM team engages with the various lines of business and relevant control groups embedded in business areas to assess the likelihood and impact of risk events, as well as assess the efficacy of relevant controls to help ensure risk levels remain within acceptable levels. Factors such as changes in the business environment, new or updated regulations, and new products and services are considered when identifying areas and topics for risk assessment. The key risk assessment processes are:

4.1.1 Risk Identification

The ERM team works with the various lines of business to support the identification of potential events that, if they were to occur, could potentially trigger a material business impact. The risk identification process considers a wide range of threats (e.g., cyber threats, malicious insiders, natural disasters, pandemics, business changes, etc.) including the potential impact on people, processes, and information systems, and the likelihood of a risk event materializing at Bloomberg.

4.1.2 Risk Measurement

As a part of the risk measurement stage, mitigating controls are identified. The ERM team and the relevant line of business evaluate and monitor controls for effectiveness in mitigating the identified risks. A standard risk rating criteria is leveraged to uniformly assess the residual risk that remains.

4.1.3 Risk Response

Risk responses are documented by the line of business managers and have an associated owner, due date, and clearly identified remediation activities. The ERM team provides oversight to ensure that appropriate response strategies are implemented.

4.1.4 Risk and Control Monitoring

The scope and frequency of monitoring activities depend on the specific risk's risk rating and effectiveness of internal controls of the line of business unit and company. The line of business managers and risk owners may work with the ERM team to implement escalation triggers for further review. The RATO (Risk Assurance and Testing oversight) team periodically tests controls to ensure operational effectiveness.

4.1.5 Risk Reporting

The ERM team reports on risk exposures and associated mitigation plans and periodically reports on status to senior management and the Risk Steering Committee.

4.1.6 Risk Training

The ERM team provides centralized training on risk management to drive awareness and adoption of centralized risk management policies and procedures.

4.1.7 Risk Management Technology

Bloomberg has implemented an Enterprise Governance, Risk, and Compliance (EGRC) platform to support risk management across the company. The EGRC platform enables the ERM team to maintain a central repository of risk-related efforts, collaborate on risk assessments, and report on the status of risk activities.

5. Bloomberg Policies, Standards and Procedures

Bloomberg has developed a policy framework that creates a uniform structure for the implementation of policies, standards, and procedures (collectively, "policy documents"). These policy documents take into account industry standards, such as the Control Objectives for Information and Related Technology (COBIT) and National Institute of Standards and Technology (NIST) frameworks. Operational policy domains within this framework include:

- Business Continuity
- Contingent Worker Policy Guide
- Corporate Records Retention
- Data Center, Cloud Service, and Node Sites
- Disaster Recovery
- Data Management
- Enterprise Risk Management
- Global Resource and Information Core Guide ("Core Guide")
- Incident Management
- Information Security
- Personal Data Privacy
- Personnel Management
- Physical Security
- Policy Framework
- Software Development Lifecycle
- Vendor Management

5.1 Policy Governance

Approval committees comprised of key leaders across Bloomberg, including from CRO, Legal, and HR, have been established to oversee the creation and approval of Bloomberg policy documents. A single Policy Owner is identified for each policy. Policy Owners are responsible for reviewing their policy documents, including obtaining input from internal subject matter experts from relevant departments identified by the Policy Owner.

5.2 Policy Life Cycle Management

5.2.1 Policy Document Maintenance and Periodic Reviews

The Policy Owner is responsible for performing periodic reviews of their policy documents and updating them when necessary. Considerations taken into account during this mandatory periodic review include whether:

- the purpose and goal of the policy documents are still being met; and
- the policy documents are up-to-date and consistent with the company's strategic plan, legal requirements, and other related policies, standards, and procedures.

Policy documents may also be updated outside of their typical review schedule to account for changes in Bloomberg's products and services, the external environment in which they operate, and any emerging risks or threats. The triggers for out-of-cycle updates include:

- changes to the external operating environment;
- changes to government policy, legislation, or regulation;
- review of the strategic direction of the company;
- new initiatives within or across management areas; and/or
- need for consistency across areas of client service delivery.

5.2.2 New Policies

New policies may be created to address anticipated needs or in response to an existing need not addressed by a current policy. The CRO regularly assesses the activities and responsibilities of the company, monitors the external environment, and reviews recommendations from Bloomberg personnel in order to identify the need for additional policies.

5.3 Policy Compliance

All Bloomberg employees are required to review the company's policy documents and acknowledge them at least annually. Various company policy documents are also covered during semi-annual training programs. Many of the acknowledgements include the responsibility for maintaining the confidentiality and security of the information employees are granted access to, and that employees must take due care to protect the technology equipment issued to them. Individuals found to have violated policy documents may be subject to disciplinary action, consistent with the severity of the incident, and to the extent permissible by law.

6. Vendor Management

Bloomberg utilizes third-party vendors to provide various products and services to Bloomberg. Vendors may include any person or company that:

- Licenses and/or supplies systems, services, or technology for use by Bloomberg employees, contractors, temporary staff, and/or Bloomberg's clients;
- Performs functions on Bloomberg's behalf for those products or services Bloomberg chooses not to conduct internally or Bloomberg does not originate (e.g., outsourcing);
- Provides goods or manufactures proprietary Bloomberg products (e.g., B-Units, keyboards); or
- Handles Data, regardless of remuneration, excluding where such Data is shared as part of a client relationship. Data handling activities include storage, labeling, processing, transmission, disposal of, or access to Data Sets.

A Vendor Management policy has been developed to define the operating framework for the company to engage with vendors.

6.1 Vendor Risk Management Governance

A dedicated Vendor Risk Management (VRM) team resides within the Chief Risk Office and is primarily responsible for assisting departments with the identification, assessment, mitigation, and continuous monitoring of risks inherent in working with vendors and other third parties. The VRM team provides oversight and management support for the vendor management program and is responsible for implementing adequate controls, drafting procedures, and auditing for compliance. The VRM team is also responsible for documenting, tracking, and escalating vendor-related issues identified as part of risk assessments, and working with vendors and business units on risk mitigations.

6.2 Vendor Risk Assessment Process

6.2.1 Engagement Inherent Risk Assessment

In this initial phase, the VRM team gathers commercial vendor engagement-related information, including engagement scope, data to be accessed / collected / processed and / or stored, business sponsor, technologies involved, and engagement criticality. Based on the information gathered during this phase, the VRM team determines the level of due diligence required for the engagement.

6.2.2. Due Diligence and Risk Based Vendor Selection

At this phase, according to engagement inherent risk level, VRM requires the vendor to complete due diligence questionnaires and provide supporting documentation such as SOC 2 Type 2 reports, ISO 27001/27002 certifications, and policies, standards, and procedures. VRM reviews this documentation to assess the vendor's controls and practices related to information security, privacy, business continuity, third-party risk management, among others. Additionally, VRM may conduct vendor onsite visits and assessments. Concerns or issues with the engagement are documented within a risk register and shared with the relevant business and Risk Management. VRM works with vendors and business stakeholders to mitigate identified risks through remediation, escalation, and risk acceptance from Bloomberg leadership, or by not proceeding with the engagement.

6.2.3. Contract Terms

During the contracting phase, Bloomberg ensures appropriate contractual terms, including information security, privacy, and business resiliency requirements are in place.

6.2.4. Ongoing Vendor Oversight and Vendor Engagement Periodic Re-Assessment

Additionally, VRM conducts periodic re-assessments of:

- vendor engagements' inherent risks; and
- vendors' control environments and practices.

High-risk vendors are monitored during the lifetime of the relationship for cybersecurity events. Additionally, VRM periodically conducts reassessments of vendor engagement inherent risks, and vendors' control environments and practices. Further, VRM monitors critical vendors for risks in areas other than cyber, including financial, ESG, geo-political, sanctions / restrictions, and natural disasters.

6.2.5. Renewal and Termination of Vendor Relationships

Vendor contracts are renewed or terminated based on the business need as well as the performance of the vendor. Bloomberg maintains a process to remove facilities and systems access provided to vendor personnel upon termination of the engagement and to confirm that Bloomberg's data are recovered or destroyed per contractual requirements, when applicable.

7. Asset Management

Bloomberg has an asset management program in place to manage the life cycle of physical and electronic assets. The program covers the following types of assets:

- Hardware – All Bloomberg hardware assets (internal or external) are tracked using a hardware inventory system. Bar Codes are placed on all assets, which include both a material and serial number.
- Software – Bloomberg collects information about third party software (including Open Source Software and commercial products) and appropriate due diligence is performed before approval to use within the infrastructure. All approval requests are ticketed. Personnel must not install nor distribute any unauthorized assets. Purchased software assets also have financial management elements tracked such as licensing, support requirements and end-of-support timeframes.

7.1 Asset Classification

Bloomberg has a defined process to classify assets. Assets are assigned to specific lines of business. Roles to manage inventory systems are reviewed periodically.

7.2. Asset Management Processes

Each line of business owns its respective assets and is responsible for limiting access based on corporate standards. Robust chain of custody controls are in place for equipment within our facilities.

7.2.1 Asset Disposal

Upon return to a Bloomberg warehouse, Bloomberg sanitizes all physical assets that contain storage media. In instances where the data is not completely sanitized, the physical assets are destroyed at the appropriate location.

8. Human Resource Management

Bloomberg's Human Resources department has implemented policies and procedures to reduce the risk of theft, fraud, and misuse of information or facilities by personnel. Key processes include:

8.1 Hiring Practices

To reduce operational risk, newly hired employees, subject to applicable laws, undergo a background check prior to commencing employment with Bloomberg. The background checks cover, at a minimum, and again subject to applicable laws, the following:

- Global sanctions check
- Education
- Employment history (employers and dates of employment)
- Criminal Check

Additional checks may be performed for certain roles as necessary.

8.2 New Hires

All new hires are required to sign a Confidentiality Agreement as well as an acknowledgment of the contents of Bloomberg's Global Resource and Information Core Guide, which includes the following:

- General Standards of Conduct and Ethical Behavior
- Policies setting forth acceptable use

8.3 Termination Processes

HR is responsible for triggering the termination of system and network access on the same day through communication with appropriate administration teams. HR also reminds employees, during the separation process, of their obligations and responsibilities under the confidentiality agreement.

8.4 Security Awareness Training

Bloomberg has in place an enterprise-wide targeted training program reinforcing Bloomberg's policies and procedures. The objectives of the training program, overseen by Human Resources, are to:

- Explain the proper rules of behavior;
- Communicate company policies and procedures on a wide range of topics;
- Detail each individual's accountability for following company policies and procedures; and
- Test each individual's understanding of their role in maintaining the highest ethical standards.

Bloomberg employees go through appropriate training at least annually. Department managers, in collaboration with Human Resources, may also develop and administer ongoing training as necessary. While the training highlights employees' responsibilities and obligations, employees are expected to also exercise good judgment in the performance of their roles, understand Bloomberg's policies and procedures, report questionable behavior, and ask questions. Bloomberg institutes mandatory training for all employees, conveying best practices, corporate policy, and responsibilities concerning information security.

9. Physical and Environmental Security

Bloomberg is committed to maintaining physical security through the application of appropriate protection measures at all Bloomberg sites. Each Bloomberg site is assigned a tier level based on business criticality. Physical security measures are designed and maintained based on the assigned tier level of each location and an assessment of location risks for the specific site. These measures are implemented with the goal of:

- Protecting the life and safety of Bloomberg personnel, clients, visitors, and the general public at Bloomberg facilities;
- Protecting Bloomberg assets, both physical and digital;
- Preventing business disruption;
- Safeguarding against hazards;
- Maintaining the confidentiality, availability, and integrity of information; and
- Preventing crime.

Bloomberg locations maintain physical security measures in order to protect people, property, and assets through the judicious placement of barriers and other devices to deter and delay the entry of intrusions – including human, vehicle, and/or electronic threats. The security measures are applied based on the level of the perceived environmental and physical risks through the use of multiple layers of concentric protection. The Global Head of Security Operations is responsible for oversight and management support for physical security.

Key physical security controls include:

9.1 Layer 1 – Physical Security Perimeter

All Bloomberg locations (including data centers) are protected by appropriate security perimeters, including physically secure walls, controlled access points, alarms and security personnel. Security conducts a risk assessment to define the security perimeters (e.g., boundaries requiring security measures to protect assets from unauthorized access) and the location and strength of each of the perimeters.

9.2 Layer 2 – Physical Security of Office Areas

Bloomberg employs a variety of physical security controls throughout our global offices. Physical entry measures taken at Bloomberg's office areas include:

- Access points (e.g., delivery and loading areas and other points where unauthorized persons may enter the premises) are controlled. Logs are maintained for all access.
- Entrance areas are protected by appropriate electronic access control systems to limit access to authorized persons. Access to areas where information is processed or stored is controlled and restricted to authorized personnel only.
- Personnel are required to wear visible Bloomberg-issued identification at all times. Visitors are required to provide a government-issued ID. Visitors are given paper access badges upon proof of identity that identifies them as non-employees and must badge in and out of the building. Visitors are required to surrender these badges before leaving the Bloomberg location. Security staff enforce the wearing and display of photo badge identification at all times.

The following controls are deployed in Bloomberg office areas:

- Personnel and visitor access is recorded, and all visitors are supervised in critical areas. This control also helps prevent tailgating from unauthorized visitors.
- Video servers are monitored and checked frequently to ensure proper functionality.
- Where we use external vendors to provide security services, Bloomberg's internal security team is responsible for the vendor's performance.
- In accordance with applicable laws, CCTV cameras are installed in some Bloomberg facilities, including data centers, for safety and security purposes.
    - Cameras include a combination of fixed devices and PTZ (pan-tilt-zoom) technologies as appropriate for the particular type, use, and sensitivity of the covered space; and
    - Security guards monitor live feeds and recorded images as appropriate.

9.3 Environmental Security Controls

The following environmental security controls are in place at Bloomberg Data Centers:

- Dedicated battery / uninterruptible power supply ("UPS") room with hydrogen sensors;
- Generator area with readily available fuel supply to supply power for over 48 hours;
- Air conditioning with humidity controls;
- Fluid sensors;
- Heat and smoke detectors;
- Fire suppression systems;
- Multiple power feeds to ensure uninterrupted supply; and
- Multiple communication feeds.

There is a preventative maintenance program in place. Security equipment is tested periodically.

9.4 Data Center Security and Controls

Bloomberg also operates data centers and network node sites. These areas are highly secure, unmarked facilities, and access is controlled through the implementation of measures such as security officers, CCTV video surveillance, keycard identification and visitor escort policies. All console rooms are staffed 24 hours per day and 7 days per week. Security officers monitor the console rooms with CCTV surveillance cameras.

Bloomberg annually engages a third-party to perform a Data Center SOC Report. The study reported on the effectiveness of the controls over the Data Centers and operational services, focusing on security, availability, and confidentiality. To request a copy of the report, please contact bcro@bloomberg.net.

10. Incident Management

Bloomberg adopts a proactive, pragmatic, and risk-informed approach to incident management – aligned with strategic objectives and relevant legal and regulatory requirements – so incidents are addressed as swiftly and effectively as possible. Bloomberg has established an Incident Management program to implement this approach, setting out the processes and protocols which are adhered to when responding as part of the Incident Management lifecycle:

- **Incident Handling**: Bloomberg establishes and maintains a process and defined criteria for incident monitoring, identification, escalation, classification, categorization and prioritization to ensure consistent approaches for handling incidents.
- **Internal and External Communication:** Bloomberg considers a number of factors when determining external communication and notification requirements, such as the scope of the issue, legal and regulatory requirements and the impact to clients and other affected parties
- **Incident Resolution**: Bloomberg strives to remediate all incidents that affect operations, technology, people and clients as quickly, effectively and with as little business disruption as possible.
- **After-Action Analysis**: Relevant stakeholders collaborate to identify remediation activities as appropriate, intended to prevent future related incidents from occurring and opportunities for continual improvement

The Incident Management program is reinforced by a holistic management process to ensure the program's effectiveness, based on a Plan, Do, Check, Act cycle for continuous improvement, including:

- **Exercising and Testing**: Establishing schedules that include the exercising and/or testing of Incident Management processes at least annually.
- **Training**: Maintaining a training program that includes awareness training for general Personnel and more specialized training for those with Incident Management Team responsibilities (conducted at least annually).
- **Monitoring and Feedback**: Capturing metrics and feedback with an intent to drive continual improvement.
- **Maintenance**: Establishing maintenance schedules that include updating plans and domain specific standards.
- **Documentation and Distribution**: Ensuring that Incident Management program information is stored in a central repository and available to Personnel as appropriate

11. Access Control

Bloomberg has an Identity and Access Management Standard in place to govern the process of restricting system access to products, services, and data. The implementation of access management is supported by a selection of tools, the responsibility for which rests with each of the various business lines. Access management at Bloomberg is based on the principle of "least privilege," whereby authorized users are granted access to information systems, networks, and data as necessary to carry out their roles and responsibilities.

11.1 Access Management Procedures

Formal procedures are used to manage the allocation of access rights. Bloomberg has the following access controls in place:

- Access authorization – Access to systems, networks, and data is granted based on the employee's department and role. Where necessary, individual lines of business may opt to employ additional controls for specific groups due to considerations for the role.
- Role-based access – Employees, contractors, and vendors are assigned roles throughout the user life cycle (hire, department moves, and terminations) based on their department and job responsibilities.
- Individualized access – There are also options to provision access to systems as named individuals.
- Emergency access – When required, emergency access is granted on a case-by-case basis. Emergency access is temporary in nature and expires when no longer necessary.
- Role transitions – Any change in roles (promotion, demotion, or transfer) is accompanied by a review of access requirements by the new manager of the transitioning employee.
- Access termination – Upon employee termination, HR works with the relevant department manager to immediately disable all of that employee's system accounts.
- User Access Rights Review – Reviews of user access rights occur on a regular basis.
- Access attempts are logged – Regular and administrative account login attempts are automatically logged by the system. Logs are reviewed as required.

11.2 User Authentication

User authentication controls are implemented to prevent unauthorized access to Bloomberg systems and networks. Users are authenticated using a combination of user ID, password, and biometric authentication; the combination is designed to provide strong authentication for Bloomberg products and services. Each user is assigned a unique user ID and user IDs cannot be shared among users. Workstations are locked after 15 minutes of inactivity.

The Bloomberg Terminal employs the following authentication and password controls:

- Multifactor authentication, including the use of a biometric device for Bloomberg Anywhere subscribers
- The ability to authenticate on any Terminal with an individual account is disabled after six unsuccessful login attempts
- A session is terminated if the authenticated user initiates a second session
- Sessions are automatically terminated daily and users must re-authenticate
- Controls are in place to automatically lock screens and terminate remote sessions after a period of inactivity.

11.3 Management and Oversight

Bloomberg has a dedicated Access Control Team to centrally manage the configuration of roles.

This team also approves the creation and modification of new roles based on business requirements. Additionally, each line of business identifies at least one Business Administrator for Roles (BAR) to manage roles and entitlements for that line of business.

11.4 Password Requirements

Usernames for Terminal users are generated upon the creation of their account. Users create their own passwords during the account set up process. They can change their Terminal passwords at any time. User identity is verified prior to resetting of passwords for Terminal accounts.

In addition to the previously listed authentication controls, clients may enforce the following password policies by submitting a request to their Bloomberg account manager:

- A minimum password length (minimum of 2 characters, maximum of 12 characters)
- The ability to require a password to contain alpha, numeric, upper case, lower case and/or special characters
- The ability to require a minimum number of non-duplicated passwords (minimum of 2, maximum of 100 passwords)
- A password expiration date after a number of days (minimum of 1 day, maximum of 365 days)
- The ability to lock out a user after a number of invalid password attempts (minimum of 1 attempt, maximum of 6 attempts)
- The ability to lock out a user after a number of inactive days (minimum of 1 day, maximum of 100 days)
- The ability to set a start date for this policy (for the present date, or a future date)

Bloomberg utilizes and maintains secure back-end systems that are designed to store and maintain passwords that are part of the Bloomberg Professional service authentication process. All user passwords are stored as a salted one-way hash on systems in which access is controlled and logged.

11.5 Corporate Environment Access Control

In addition to access controls for the Terminal, additional access controls are in place to restrict employee, vendor, and contractor access within the corporate network environment. This includes access to physical assets (e.g., servers and workstations) and software assets (e.g., databases and fileshares). Access to assets is granted based on their department.

Corporate accounts are automatically created as part of the onboarding process. Users create their own passwords during the account setup process and can change them at any time. Users' identities are verified prior to the changing of corporate account passwords. Passwords must be changed regularly. When an employee changes roles or departments, their access is adjusted based on their new department. When employees leave Bloomberg, their corporate accounts are immediately disabled upon processing of the termination by HR. Additionally, for the corporate environment, administrators are provided separate accounts with elevated privileges and activity from these accounts is monitored closely.

11.5.1 Access to the Production Environment

The development and production environments are separated and access to each environment is restricted to authorized personnel. Access controls are designed to control production access based on job function. Normally, development teams are not provided production access and any emergency access is granted in line with the documented requirements.

11.5.2 Remote Access

Bloomberg uses multiple technologies to support secure remote access by employees, including mandatory multifactor authentication, encrypted network traffic, and a physical separation between the corporate and production networks

12. Business Continuity

Bloomberg maintains a comprehensive Business Continuity Program to ensure a timely response to and effective recovery from unanticipated business disruptions that may affect facilities, infrastructure, or personnel. This program takes into consideration a wide range of threats both natural and manmade- including but not limited to, severe weather, natural disasters, and power outages, etc. - through the coordination of various groups responsible for business continuity, disaster recovery, incident management, and emergency response processes.

Bloomberg has Business Continuity policies and associated standards and procedures to drive the operating framework for the program. The objective of the program is to meet the following goals:

- Maintain the ability to serve clients;
- Maintain the resiliency of business operations and infrastructure through viable recovery strategies;
- Provide for timely and complete resumption of operations following a disruption;
- Minimize financial loss;
- Minimize risk exposure in the event of a business interruption; and
- Ensure compliance with other policies and relevant regulations.

12.1 Governance

Bloomberg is committed to maintaining and overseeing a Business Continuity Program governance framework to ensure that the Company's overall approach to Business Continuity (BC) is supported by high standards of governance.

BC responsibilities are distributed among each line of business. Business Continuity Planning Managers are appointed to implement BC strategies for their line of business. The Business Continuity Planning Managers are supported by regional Business Continuity Coordinators, who are responsible for ensuring regional BC strategies are in alignment with the department's BC Plan. Business Continuity Planning Managers and Coordinators work closely with the Enterprise Resilience and Incident Management (ERIM) team for the effective adoption and implementation of BC strategies across their business line.

The ERIM team oversees coordination of the BC program at an enterprise level and reports to Bloomberg's Management Committee.

The key processes within the BC Program are the following:

12.2 Business Impact Analysis

Business Impact Analyses ("BIA") are conducted to identify critical business processes and establish recovery strategies. The BIA are conducted at a business process level and consider impacts at varied timeframes in order to establish recovery priorities, strategies, dependencies, and resources.

12.3 Plan Development

Business continuity planning takes into consideration information gathered from the BIA. BC Plans contain the strategies and procedures for business process recovery in the event of a business disruption, taking into account staffing requirements, recovery strategies, workplace requirements, supporting technology requirements, and other general dependencies.

Key considerations during the development of the BC Plan include:

- Establishing a process to activate the BC Plan
- Recovery procedures in the event of an emergency
- Findings and observations from previous BC testing

12.4 Plan Testing

BC Plans are tested on a regular basis. BC Plan testing may include:

- Call Tree Notification Test: Ensures that department managers are able to communicate critical information to their personnel in the event of an incident, or as otherwise necessary, in a timely manner.
- Table-top Exercise: Enables department managers to analyze their BC Plan and evaluate whether or not they have the capabilities to fulfill the outlined requirements in the BC Plan.
- Recovery Strategy Testing:
    - Work from Anywhere: Remote access tests validate that critical business processes may be successfully completed outside of a Bloomberg facility. They also demonstrate to the department managers that designated personnel have the capabilities to work efficiently from a non-Bloomberg facility.
    - Work-Handoff: Work-handoff exercises test the ability of personnel in other locations to assume critical processes for other personnel in the event of an incident. This test also ensures that the location receiving the work can and will accommodate the combination of their normal workload with the additional activities or increased volume, and to determine whether necessary expertise is available in the alternate location.
    - Recovery Site Relocation: Bloomberg has established dedicated recovery sites for critical departments that enable the resumption of critical business operations at the alternative location in the event of a business disruption or incident at the primary location.

12.5 Plan Maintenance

BC Plans are reviewed and updated on a regular basis (annually, at a minimum) or when a determination is made that more frequent updates are warranted. The review process includes checking for continued adequacy of resources (people, supporting technologies, and facilities).

12.6 Plan Training

BC Planning Managers and Coordinators, in collaboration with the ERIM team, are responsible for ensuring personnel are aware of the BC plans for their department. General BC awareness includes internal communication of BC Plans, ongoing participation in BC Plan testing, and formal business continuity training, where necessary.

13. Disaster Recovery

In order to continue to serve its customers in the event of a disaster, Bloomberg designs for high availability via redundancy in both its data center and application architectures. Bloomberg maintains and tests contingency procedures to minimize the impact to service delivery in the event of a disaster.

13.1 Recovery of Services

Regarding RTOs and RPOs, Bloomberg strives to maintain robust resiliency levels. In the event of a service disruption, Bloomberg seeks to restore service as quickly and as reasonably practicable. Bloomberg has proper controls in place to account for external and internal factors that can impact service availability and service performance. Bloomberg manages its own infrastructure and architects its networks, systems, and applications with multiple layers of redundancy. Bloomberg designs for high availability with multiple layers of resiliency at each layer of the technology stack, including running applications on multiple servers in multiple data centers concurrently. An extensive monitoring and alarming system is in place to identify issues, and where appropriate automation is utilized to fix issues before they impact service availability. Instructions for responding to alarms are maintained and engineers are available 24x7 to address issues that might arise. Our goals are to minimize the likelihood, impact, and duration of any service disruption.

13.2 Data Center Operational Controls

Bloomberg maintains multiple data centers across locations. Bloomberg implements measures to protect the data centers and their contents from unauthorized access, malicious information system attacks, and natural and man-made disasters.

13.3 Machine Backups and Storage

Bloomberg has defined a formal backup and restoration process to prevent the loss of data in the case of data corruption, system failure, theft, or other disasters. The process maintains the confidentiality, integrity, and availability of information assets. Various automated tools are used to backup data from servers on an hourly, daily, weekly, and/or monthly basis based on the nature of the data. An industry-standard encryption key management system is used to encrypt data as it is copied from our servers to the backup media. The Storage Administration team is responsible for ensuring that the backed-up data is stored for specific retention periods. The backup restoration process is evaluated during Disaster Recovery (DR) tests. Bloomberg works with an external vendor for secure off-site storage of information assets. Tapes are transported securely between locations through closely tracked shipments.

13.4 Hardware and Operational Controls Redundancy

Bloomberg deploys clusters of servers to deliver continued operations in the event of a hardware failure. Routing to alternate hardware is automated through load balancers where possible. Hardware health monitoring is designed for high availability and is automated. Applications are deployed to multiple servers across multiple data centers to provide additional redundancy.

13.5 Network Redundancy

Network devices are deployed in pairs with load balancers configured to automatically route traffic away from failing devices. Network device pairs are comprised of hardware from multiple vendors. Bloomberg has multiple communication lines in and out of its data centers and between its data centers, provisioned by multiple providers. The network management systems are mirrored, allowing for diverse monitoring capabilities.

13.6 Change Control

Changes to infrastructure within the Bloomberg data centers are managed and tracked. Access to deploy infrastructure changes is restricted and controlled.

13.7 Redundant Power

Bloomberg has redundant power feeds into its data centers with redundant power distribution units within its data centers. Uninterruptable Power Supply ("UPS") modules provide first level power backup and generators provide second level backup.

13.8 Contingency Procedures

Bloomberg maintains and tests contingency procedures to help ensure that service can continue with little to no disruption. Procedures are documented, maintained, and tested.

13.9 Testing

DR is supported by active and ongoing testing. DR testing parameters are defined prior to testing and results are tracked internally. Bloomberg remediates any findings from DR testing, and re-tests accordingly. Throughout the year, regular tests are conducted based on a program that is determined by Bloomberg's Engineering department. Tests are conducted every 6 months for at least 72 consecutive hours during the Monday-Friday work week when our data centers experience maximum load.

- Specific tests are designed to confirm that proper sizing and capacity are maintained to support user load in the event we lose a data center.
- Application teams conduct regular cluster failover testing to certify disaster recovery capability and readiness.

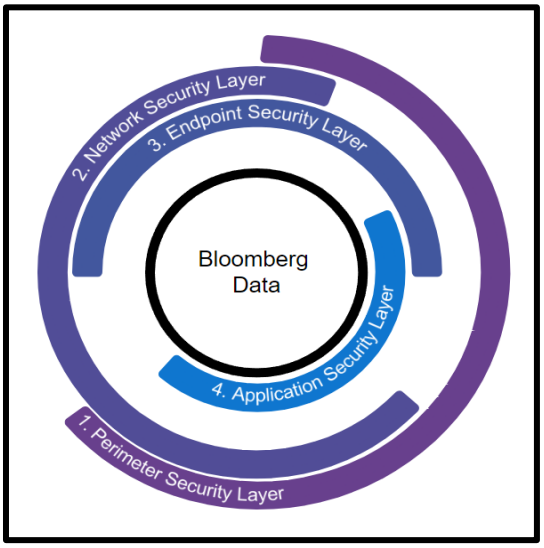
14. Chief Information Security Office

14. 1 Overview

The Chief Information Security Office (CISO) aims to safeguard Bloomberg and its subsidiaries' ("Bloomberg") digital assets and foster a secure technology environment. CISO is committed to implementing robust cybersecurity measures, promoting awareness, and cultivating a culture of resilience against evolving cyber threats.

Bloomberg's information security program encompasses a wide range of initiatives dedicated to safeguarding our data, systems, and clients from malicious actors.

The assorted prevention measures and detection capabilities are purposely designed to work together to form a layered defense that provides multiple opportunities to block and/or discover malicious activity.

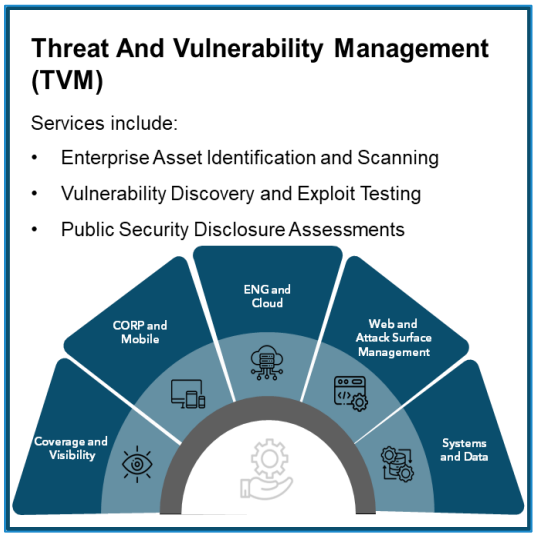


14.2 CISO Capabilities

- Program Assurance and Strategy: Fosters effective security programs through continuous monitoring and evaluation. Provides decision support, oversight, and delivery of an accurate, data-driven CISO strategy.
- Governance, Risk and Compliance: Oversees an information security governance framework that applies high governance standards aligned with regulatory guidelines and industry standards to Bloomberg's approach to information security.
- Training and Knowledge Capture: Maintains an information security training and awareness program to educate personnel on information security and to foster a security-minded culture that establishes a shared responsibility model.
- Cyber Security Operations Centre (CSOC): Defends Bloomberg and our partners from information security threats by gaining insight from intelligence, hunting for suspicious activity, implementing detection mechanisms, and monitoring for meaningful security events.
- Threat and Vulnerability Management: Oversees the vulnerability management program to discover, assess, prioritize, remediate, and report technical vulnerabilities.
- Product Security: Evaluates the security posture of applications built and/or deployed at Bloomberg.
- Business Information Security Office (BISO): Partners with business units to identify and evaluate security risks and vulnerabilities.
- Security Data Science: Collects, processes, and curates data to generate context that helps CISO teams make time-critical security decisions more accurately and efficiently.
- Staff Risk and Investigations: Assists the organization with detecting, assessing, and managing the broad range of risks and threats associated with insiders.

14.3 Threat and Vulnerability Management

Bloomberg has a Threat and Vulnerability Management program in place, managed by a dedicated team within CISO. The Threat and Vulnerability Management team systematically identifies, evaluates, and prioritizes security vulnerabilities across Bloomberg's technology estate. The team conducts asset discovery and inventory, automated vulnerability scanning, and regular manual assessments to ensure comprehensive coverage. Additionally, they perform targeted vulnerability scans on Bloomberg's assets, including internet-facing systems, to identify and mitigate potential security threats effectively.



14.3.1 Threat and Vulnerability Management Functions

- Asset Identification and Scanning: The team collaborates with partners across the company to identify assets and conduct scanning, maintaining an up-to-date inventory and ensuring that all assets, including hardware, software, and network components, are regularly monitored for vulnerabilities.
- Vulnerability Prioritization: Vulnerability prioritization is based on a risk assessment process that considers the potential impact and exploitability of each vulnerability. High-risk vulnerabilities are addressed promptly with focused remediation efforts, while lower-risk issues are managed through ongoing monitoring and scheduled updates. This approach ensures that resources are allocated efficiently, and critical assets are protected against the most significant threats.
- Vulnerability Assessment: Vulnerabilities identified within our estate are ranked from critical to very low using a risk-based framework that considers their potential impact and exploitability.
- Remediation Coordination: The effective management of known vulnerabilities is a shared responsibility. Bloomberg's Vulnerability Management Team engages with stakeholders inside and outside of the company to ensure that remediation activities are effective and well-coordinated.
- Tooling, Reporting and Analytics: Bloomberg leverages industry standard technologies to augment vulnerability scanning and evaluation procedures, resulting in thorough coverage and prompt vulnerability identification. In-depth reporting offers useful information and transparency into the security posture, and analytics support trend identification, assessment of remediation operations' efficacy, and strategic decision-making for ongoing development.

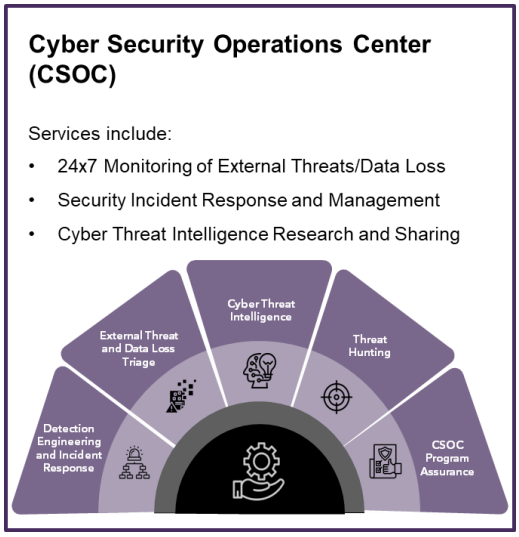
14.3.2 Key Threat and Vulnerability Management Capabilities

- Advanced Threat Intelligence: Ability to gather, analyze, and apply threat intelligence to predict and mitigate risks.
- Vulnerability Assessment: Expertise in identifying, prioritizing, and addressing vulnerabilities across various systems and applications.
- Continuous Monitoring: Implementing real-time monitoring tools to detect threats and vulnerabilities proactively.
- Automation and Orchestration: Use of automation tools to streamline vulnerability scanning, patch management, and response actions.
- Collaboration and Communication: Strong internal and external communication skills to coordinate with various teams and stakeholders.
- Reporting and Analytics: Ability to generate actionable reports and insights from threat data to guide decision-making.

14.4 Cyber Security Operations Center (CSOC)

The Cyber Security Operations Center (CSOC) is a specialized unit within CISO dedicated to monitoring, detecting, and responding to cyber threats and incidents on a 24x7x365 basis. The team responds to and helps contain security incidents that emerge, involving appropriate stakeholders as required. Staffed by a team of skilled cybersecurity professionals, the CSOC utilizes advanced tools and technologies to analyze network traffic, scrutinize logs, and identify potential security breaches.

Additionally, the CSOC disseminates both business-specific and enterprise-wide security advisories, ensuring that stakeholders are informed about emerging threats and vulnerabilities.



14.4.1 Cyber Security Operations Center Functions

- Event Triage and Data Loss Protection: Ensures 24x7 monitoring of external threats and potential data loss, providing continuous oversight to detect and respond to cybersecurity threats. It includes strategic enhancements to Bloomberg's data loss program, aimed at improving detection, prevention, and response mechanisms. Additionally, this capability manages data loss and exposure incidents, facilitating effective mitigation to protect sensitive information.
- Threat Hunting and Intelligence (THI): Drives intelligence-led threat hunting, utilizing open and closed source threat intelligence to actively seek out potential threats within the organization's environment before they can cause harm. Additionally, it serves as the escalation point for cyber threats, ensuring that critical threats are identified, prioritized, and integrated into detection and response capabilities promptly.

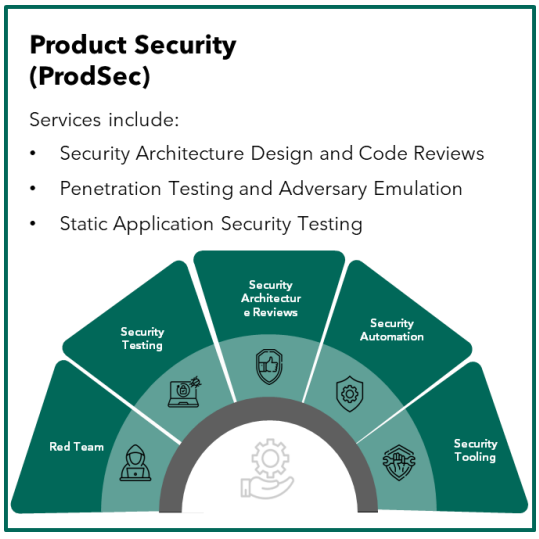
- Cyber Incident Response Team (CIRT): Works with stakeholders across the firm to promptly and effectively manage cybersecurity incidents to minimize damage and restore normal operations. It encompasses incident investigation, containment, and coordinated recovery efforts, ensuring resolution. Additionally, this capability includes post-incident analysis to enhance future incident handling and strengthen the organization's overall cybersecurity posture.

14.4.2 Key Capabilities

- 24/7 Threat Monitoring: Continuous surveillance of networks and systems to detect and respond to threats.
- Incident Detection and Response: Rapid identification and mitigation of security incidents, minimizing impact and recovery time.
- Intrusion Detection Capabilities: Utilizes intrusion detection capabilities to detect and react to known attacks in real time. Intrusion Detection signatures are updated periodically to update detections for specific threats, intruder profiles, and attack patterns.
- Log Management and Aggregation: Implementing centralized logging and aggregation systems to monitor, analyze, and respond to security events across technology assets, ensuring traceability and accountability in the event of a security incident.
- Security Information and Event Management (SIEM): Proficient use of SIEM tools to collect, analyze, and correlate security data across the environment.
- Threat Hunting: Proactively searching for threats within the network before they can cause harm.
- Malware Analysis: Ability to analyze and respond to malware threats, understanding their behavior and mitigating their impact.
- Forensics and Root Cause Analysis: Conducting post-incident investigations to determine the root cause of security breaches and ensuring they do not recur.
- Automation and Orchestration: Leveraging automation tools to streamline response actions and improve the efficiency of security operations.
- Collaboration and Communication: Effectively communicating and collaborating with other teams (e.g., Engineering, Legal, and Compliance) to ensure cohesive security strategies.

14.5 Product Security

Bloomberg has a Product Security program in place, managed by a dedicated team within CISO. Product Security works with partners to evaluate the security posture of applications built and/or deployed at Bloomberg. This is accomplished through security-focused design reviews and static/dynamic security testing of applications.



14.5.1 Product Security Functions

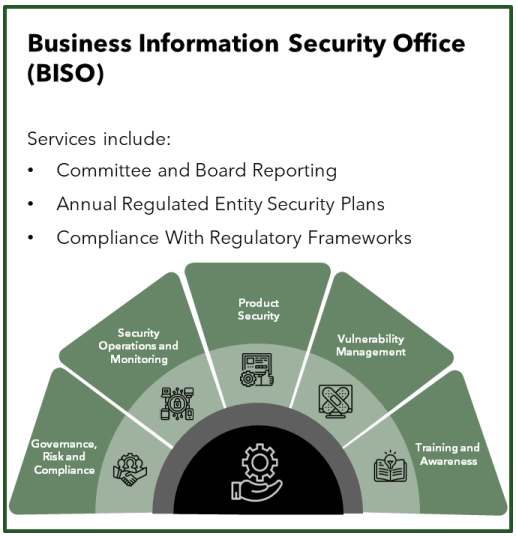
- Security Testing and Architecture: Bloomberg develops and supports a range of technologies and products, so security reviews are customized for each request. A security review may include a design review, code review, penetration test, or a combination of these activities depending upon the technologies involved, the sensitivity of the data and functionality, how it's exposed to users, and the project timeline.
- Security Automation: Responsible for implementing and maintaining automated security testing processes to identify vulnerabilities in applications and systems. This team leverages automated tools and scripts to conduct regular security assessments, reducing manual effort and increasing testing coverage.
- Penetration Testing: To proactively identify and address potential security risks, Bloomberg conducts regular penetration testing to evaluate the security posture of our external and internal applications, as well as technology components. Penetration tests are completed by a combination of third parties and qualified internal personnel.
- Red Team Testing: Red Team testing simulates real-world cyber-attacks to test Bloomberg's defenses and identify vulnerabilities. This team utilizes threat intelligence and employs advanced tactics, techniques, and procedures to mimic the behavior of malicious actors, challenging the organization's detection and response capabilities. The insights gained from Red Team activities help enhance the overall security strategy and are fed back into our response and detection capabilities.

14.5.2 Key Capabilities

- Secure Development Lifecycle (SDLC) Integration: Embedding security practices throughout the product development lifecycle, from design to deployment.
- Threat Modeling: Identifying and mitigating potential security threats early in the product design phase.
- Code Review and Static Analysis: Conducting rigorous security code reviews and using static analysis tools to identify vulnerabilities.
- Security Testing: Performing regular security assessments, including penetration testing, static testing, and dynamic analysis.
- Compliance and Standards Adherence: Designing products to meet industry-specific security standards and regulatory requirements.
- Customer and Stakeholder Communication: Effectively communicating security practices, risks, and incidents to customers and stakeholders.
- Security Feature Design: Designing and integrating security features into the product design phase, such as authentication, access control, and secure data storage.
- Open-Source Security: Managing the security risks associated with the use of open-source components in products.

14.6 Business Information Security Office

The Business Information Security Office (BISO) acts as the bridge between business units and the central CISO function, ensuring alignment of security practices with business objectives. The team works with stakeholders from business units across Bloomberg, including relevant Boards and Senior Management, to effectively implement Bloomberg's information security program. Additionally, the team gathers and relays insights and lessons learned back to the CISO organization to continuously enhance security practices.



14.6.1 BISO Functions

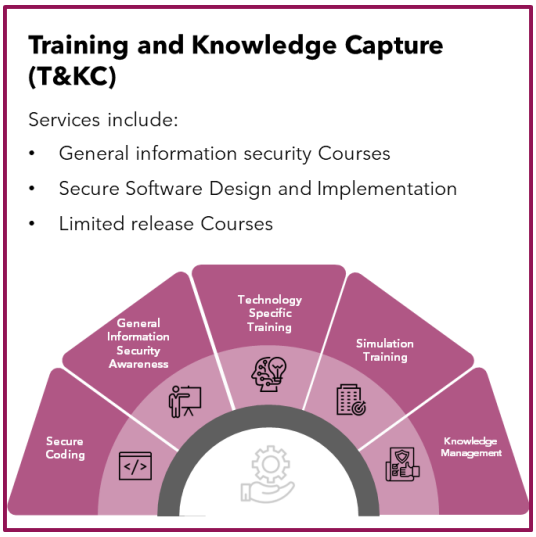
- Partnership: The BISO team partners with business units to integrate tailored security plans, ensuring alignment with organizational goals while enhancing overall risk management and compliance.
- Governance and Board Reporting: The BISOs attend various boards and governance forums across the Company to report on the security posture of the business units.
- Compliance with Regulatory Frameworks: The BISO team helps achieve compliance with regulatory frameworks by aligning business unit practices with security policies and industry standards.

14.6.2 Key Capabilities

- Strategic Alignment: Ensuring security strategies align with business objectives and regulatory requirements.
- Risk Management: Working with others in the CISO organization to identify, assess, mitigate existing, and prevent future information security risks across the organization.
- Security Governance: Establishing and enforcing information security policies, standards, and frameworks within the business unit.
- Incident Response Coordination: Leading incident response efforts within the business units and coordinating with central security teams.
- Security Awareness and Training: Educating business unit staff, including relevant Boards and Governance Committees, on security best practices and emerging threats.
- Compliance Monitoring: Ensuring the business units adhere to relevant regulatory requirements and industry standards.
- Collaboration and Communication: Facilitating communication between business units, relevant Board and Governance Committees, and central security teams to ensure consistent security practices.
- Security Metrics and Reporting: Developing and reporting on security metrics to demonstrate the effectiveness of security initiatives and inform decision-making.
- Security Architecture Review: Assessing and advising on the security architecture of new projects and business initiatives.

14.7 Training and Knowledge Capture Team

Our Cyber Training and Knowledge Capture Team (T&KC) is dedicated to identifying, documenting, and disseminating critical cybersecurity knowledge and best practices across Bloomberg. This team is responsible for developing and delivering comprehensive training programs, workshops, and awareness campaigns to educate employees on various cybersecurity topics, including threat intelligence, vulnerability management, incident response, and secure coding.



14.7.1 T&KC Functions

- Cybersecurity Training Development: Design and deliver training and awareness programs covering various information security topics.
- Online training: Develop and maintain online training modules and resources including the annual mandatory training which must be completed by all Bloomberg employees.
- Evaluate Training Effectiveness: Measure the impact of training activities through the analysis of performance metrics, employee feedback, and test results.

14.8 Key Capabilities

- Mandatory Learning: To ensure that all employees are equipped with the necessary knowledge and skills to protect our organization's digital assets, we have implemented an annual mandatory cyber learning program.
- Enhanced Information Security Training: To ensure that employees who handle high-risk activities or have access to sensitive information are properly trained and equipped to manage these risks, we have implemented a high-risk training program.
- Engineering Training: To ensure that our engineers are equipped with the necessary skills and knowledge to design, develop, and deploy high-quality products and solutions, we have implemented a comprehensive engineering training program.
- Job-Specific Training: To ensure that employees have the necessary skills and knowledge to perform their job duties effectively, we have implemented a job-specific training program.