A.1.1 Document: Organigram of "World Bank" with a focus on IT and Security departments

The World Bank operates under a hierarchical and functional organizational structure, designed to support its diverse global operations. Key divisions include, but are not limited to: Finance, Operations (covering lending and project implementation), Legal, Human Resources, Economic Research, and Communications. Crucially, for the purposes of this simulation, the **Technology and Digital Transformation Division** and the **Office of Risk Management** play pivotal roles.

The Technology and Digital Transformation Division

It falls under a Vice Presidency for Human Resources and Digital Transformation (akin to structures seen in institutions like the Inter-American Development Bank (IDB)), is the custodian of the Bank's IT infrastructure and digital initiatives. Within this division, the Information Technology (IT) Department and the Cybersecurity Department operate. The IT Department is responsible for core IT operations, infrastructure, application development, and support services. The Cybersecurity Department, led by the Chief Information Security Officer (CISO), is responsible for defining and implementing the Bank's cybersecurity strategy, policies, and controls. It may include specialized units, such as a Cybersecurity and Compliance Unit (inspired by the Asian Development Bank's ITOD-CS), focusing on standards, policy development, incident management, and compliance monitoring.

The Office of Risk Management

It is a central function reporting at a high executive level, responsible for enterprise-wide risk oversight, including operational, financial, and strategic risks. Cybersecurity risk is a significant component of this, and the CISO works in close collaboration with this office. The Data Protection Officer (DPO), while potentially having an administrative link to a department like Legal or the Office of the President, operates with functional independence, reporting to the highest level of management to ensure unbiased oversight of data protection matters.

Reporting lines for key security and IT roles are designed to ensure appropriate authority and visibility. The CISO typically reports to the Head of the Technology and Digital Transformation Division or, in some models, directly to the Chief Risk Officer (CRO) to emphasize the risk management aspect of cybersecurity. The DPO, as mandated by data protection principles, reports directly to the highest executive level, such as the Executive Vice President or an equivalent senior management body, and may have a dotted line to a Board-level Audit or Risk Committee. The Head of IT Operations and other senior IT managers report to the Head of the Technology and Digital Transformation Division (often titled Chief Information Officer - CIO or Chief Technology Officer - CTO).

A.1.2 Document: Roles and Responsibilities (CISO, DPO, IT Manager, Security Committee, etc.)

Clear delineation of roles and responsibilities is fundamental to effective cybersecurity governance. For the WDB, key roles include:

- **Chief Information Security Officer (CISO):**
    - **Responsibilities:** The CISO is responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected. This includes developing and enforcing security policies and standards; overseeing security operations (including threat detection, vulnerability management, and security engineering); planning and testing responses to security incidents; managing the cybersecurity budget; promoting security awareness and training across the Bank; and acting as the primary liaison with external entities such as law enforcement and other security forums. A key function is to balance security needs with the Bank's strategic business objectives, identify risk factors, and determine appropriate solutions. The CISO is responsible for presenting cybersecurity risks and their potential impacts to executive management and relevant committees. Management, in turn, is responsible for deciding on the acceptance or mitigation of these risks, ensuring that security measures are aligned with the Bank's overall risk appetite. This separation of risk presentation (by CISO) and risk decision-making (by management) is crucial, particularly in ensuring that the CISO's primary focus is on objective security assessment rather than sole ownership of risk acceptance.
    - **Reporting Line:** Typically reports to the Chief Technology Officer (CTO), Chief Information Officer (CIO), or Chief Risk Officer (CRO).
    - **Qualifications:** Extensive experience in information security, risk management, relevant certifications (e.g., CISSP, CISM), strong leadership and communication skills.
    - **Key Performance Indicators (KPIs):** Reduction in security incidents, compliance with security policies, maturity level of security controls, effectiveness of security awareness programs.
- **Data Protection Officer (DPO):**
    - **Responsibilities:** The DPO is an independent role mandated to ensure the Bank's compliance with applicable data protection laws and regulations (e.g., principles analogous to GDPR for WDB's global operations). Key tasks include informing and advising the Bank and its employees of their data protection obligations; monitoring compliance with these obligations and with the Bank's

data protection policies, including the assignment of responsibilities, awareness-raising, and staff training; providing advice where requested regarding data protection impact assessments (DPIAs) and monitoring their performance; and acting as the contact point for and cooperating with supervisory authorities on issues relating to data processing.

- **Reporting Line:** The DPO reports directly to the highest management level of the Bank (e.g., Office of the President, Executive Vice President) to ensure independence and avoid conflicts of interest. The DPO must not receive any instructions regarding the exercise of their tasks and must be supported by the Bank with the necessary resources to carry out these tasks and maintain their expert knowledge.
- **Qualifications:** Expert knowledge of data protection law and practices, understanding of IT systems and security, ability to promote a data protection culture within the organization.
- **KPIs:** Compliance with data protection regulations, timely handling of data subject requests, effectiveness of data protection training, outcomes of DPIAs.

The distinct roles and reporting lines of the CISO and DPO are critical. The CISO is responsible for implementing and managing security measures to protect all information assets, while the DPO has a specific mandate to oversee the lawful and fair processing of personal data, which includes assessing the adequacy of security measures applied to such data. If the CISO were also the DPO, or if the DPO reported to the CISO, a conflict of interest could arise where the DPO would essentially be auditing functions they are also responsible for managing. By ensuring the DPO's independence and direct access to top management, the WDB can maintain a robust system of checks and balances for both information security and data protection.

- **IT Manager (e.g., Head of IT Operations, Head of IT Development):**
  - **Responsibilities:** Depending on the specific IT managerial role, responsibilities include overseeing the day-to-day operations of the IT department, managing IT infrastructure (servers, networks, storage), ensuring the availability and performance of IT services, managing IT support and help desk functions, system administration, database administration, network management, and potentially leading software development teams and managing the software development lifecycle (SDLC). They are responsible for implementing security controls as defined by the CISO and ensuring IT systems comply with security policies.
  - **Reporting Line:** Reports to the Chief Technology Officer (CTO) or Chief Information Officer (CIO).

    - **Qualifications:** Strong technical background in relevant IT domains, experience in IT management, project management skills.
    - **KPIs:** System uptime and availability, mean time to resolution (MTTR) for IT incidents, successful project delivery (for development managers), adherence to IT budgets.
- **Security Steering Committee:**
    - **Composition:** Chaired by a senior executive (e.g., CTO, CRO, or CIO), with members including the CISO, DPO, and senior representatives from Legal, Risk Management, IT Operations, Application Development, and key business divisions.
    - **Responsibilities:** Provides strategic oversight for the Bank's cybersecurity program. This includes reviewing and approving major security policies, strategies, and significant investments in security technologies or initiatives. The committee also reviews reports on significant security risks, major incidents, and the overall status of the cybersecurity program, ensuring alignment between security initiatives and the Bank's broader business objectives and risk appetite.
- **IT Director / Chief Information Officer (CIO) / Chief Technology Officer (CTO):**
    - **Responsibilities:** Responsible for the overall IT strategy of the Bank, ensuring it aligns with and supports the Bank's business goals. This role oversees all aspects of the IT department, including infrastructure, operations, application development, and innovation. The CIO/CTO works closely with the CISO to integrate security into all IT initiatives.
    - **Reporting Line:** Typically reports to a member of the executive management team (e.g., Executive Vice President, Chief Operating Officer).
- **Compliance Manager (IT):**
    - **Responsibilities:** Ensures that IT processes, systems, and controls comply with applicable legal, regulatory, and internal policy requirements. This role works closely with the CISO, DPO, and Legal department to identify compliance obligations and implement measures to meet them. This is particularly important for a financial institution like WDB, which would be subject to numerous financial and data-related regulations.

The organizational structure of international development banks often reflects their complex operational mandates and global presence. Specialized units for cybersecurity and compliance, distinct Vice Presidencies for areas like "Technology and Transformation," and high-level Offices of Risk Management and Legal Departments are common. The WDB's structure, therefore, incorporates a dedicated Cybersecurity department under the CISO,

likely situated within a broader Technology or Digital Transformation division, and a functionally independent DPO office. Both functions maintain strong collaborative links with central Risk Management, Legal, and Internal Audit departments to ensure a holistic approach to governance.

Summary of Key Roles, Responsibilities, and Reporting Lines

To provide a clear overview, the following table summarizes the key roles, their primary responsibilities, reporting lines, and crucial interaction points within the WDB's governance framework.

Role	Key Responsibilities Summary	Reports To	Key Interactions
Chief Information Security Officer (CISO)	Develop & implement security strategy, risk management, incident response, policy enforcement, security awareness.	Chief Technology Officer / Chief Risk Officer	DPO, IT Heads, Legal, Risk Management, Business Units, Security Steering Committee
Data Protection Officer (DPO)	Monitor data protection compliance, advise on DPIAs, manage data subject rights, liaise with regulators.	Executive Vice President / Board Audit Committee	CISO, Legal, IT Heads, HR, Business Units processing personal data
Head of IT Operations	Manage IT infrastructure, service delivery, support, system administration, network operations.	Chief Technology Officer (CTO) / CIO	CISO, Application Development Head, Business Units
Head of Application Development	Oversee software development lifecycle, application security (DevSecOps), manage development teams.	Chief Technology Officer (CTO) / CIO	CISO, IT Operations Head, Business Units, Project Management Office
Chair, Security Steering Committee	(Usually a senior executive, e.g., CRO or CTO) Provide oversight, approve security budget/policies, champion security culture.	Board Risk Committee / CEO	CISO, DPO, Senior Management from various divisions

This table serves as a quick reference for understanding accountability and collaboration pathways, which is invaluable for simulating governance scenarios, such as responding to a major data breach or implementing a new security initiative.