Risk Assessment for UNICEF Global Operations

1. Asset Inventory with Quantities and Specific Locations

1.1 Hardware Assets

- **Laptops and Desktops**:
  - **Dell Latitude Series (5000, 7000, 9000)** and **XPS Series**:
    - **Quantity**: ~12,000 units.
    - **Primary Use**: Administrative staff, office operations, general employee functions.
    - **Geographic Distribution**:
      - **Headquarters**: **New York**, **Geneva**, **Nairobi**, **Bangkok**, **Cairo**
      - **Regional Offices**: In key locations such as **Mexico City**, **Abuja (Nigeria)**, **Bangladesh**, **Zimbabwe**, and **South Africa**.
      - **Other Locations**: Country offices in Asia, Europe, and Latin America.
  - **HP EliteBook** and **HP ProBook**:
    - **Quantity**: ~10,000 units.
    - **Primary Use**: Field staff, operational personnel in high-risk areas, health, education, and emergency response workers.
    - **Geographic Distribution**:
      - **Conflict Zones**: **South Sudan**, **Syria**, **Afghanistan**, **Yemen**, **Haiti**, **Colombia**.
      - **Developing Regions**: **Bangladesh**, **Ethiopia**, **Nigeria**.
      - **Field Operations**: In volatile or remote areas with urgent program delivery needs.
  - **Apple MacBook Pro**:
    - **Quantity**: ~3,000 units.
    - **Primary Use**: Senior leadership, IT developers, specialized teams (research, health analysis, crisis management).
    - **Geographic Distribution**: **New York**, **Geneva**, **Singapore**, and **HQ (regional offices)**.
  - **Lenovo ThinkPad**:
    - **Quantity**: ~2,000 units.
    - **Primary Use**: Project-based work in challenging field offices with a focus on remote, temporary operations.
    - **Geographic Distribution**: Mainly in **Africa**, **Asia**, and **Latin America**.

  Total Laptops/Desktops: ~25,000 units.

1.2 Mobile Devices

- **Apple iPhone 12, 13, 14 Pro Max**:
  - **Quantity**: ~5,000 units.
  - **Primary Use**: Essential mobile devices for field staff in remote or high-risk zones requiring secure, real-time communication.
  - **Geographic Distribution**: **South Sudan**, **Syria**, **Afghanistan**, **Colombia**, **Yemen**.

- **Samsung Galaxy S20/S21**:
    - **Quantity**: ~8,000 units.
    - **Primary Use**: Mobile communication for operations in developing regions and emergency settings.
    - **Geographic Distribution**: **Bangladesh**, **South Africa**, **Nepal**, **India**, **Zambia**.
- **Apple iPad (10.2 & Pro Models)**:
    - **Quantity**: ~7,500 units.
    - **Primary Use**: Data collection and service delivery in education, health, and child protection.
    - **Geographic Distribution**: **Bangladesh**, **Uganda**, **Haiti**, **India**, **Syria**.

  Total Mobile Devices: ~20,500 units.

1.3 External Devices (USB Drives, External Hard Drives)

- **USB Flash Drives (32GB - 512GB)** and **External Hard Drives (1TB - 5TB)**:
    - **Quantity**: ~20,000 units.
    - **Primary Use**: Storing and transferring sensitive operational, health, and emergency response data where internet connectivity is unreliable.
    - **Geographic Distribution**: Primarily used in **South Sudan**, **Syria**, **Yemen**, **DRC**, and **Haiti**.
- **Network-Attached Storage (NAS) Devices**:
    - **Quantity**: ~500TB of storage.
    - **Primary Use**: Data backups for field operations, safeguarding critical information during regional crises.
    - **Geographic Distribution**: Primarily in **Nairobi**, **Bangkok**, **Geneva**, and other regional offices.

  Total External Devices: ~20,000 units.

1.4 Data Centers and Servers

- **Physical Data Centers**:
    - **New York, USA**:
        - **Servers**: 3 physical servers, total storage capacity of **20TB**.
        - **Primary Use**: Operational data storage and hosting for financial systems, regional operational data for North America.
    - **Geneva, Switzerland**:
        - **Servers**: 2 physical servers, total storage capacity of **15TB**.
        - **Primary Use**: Health and humanitarian data storage, European and Middle Eastern program management.
    - **Nairobi, Kenya**:
        - **Servers**: 2 physical servers, total storage capacity of **10TB**.
        - **Primary Use**: East African operations, including programs in child protection, health, and education.

- **Bangkok, Thailand**:
    - **Servers**: 2 physical servers, total storage capacity of **10TB**.
    - **Primary Use**: Asia-Pacific emergency response programs, relief operations, and data storage for regional programs.

Total Physical Servers: 9 servers with **55TB** of stored data.

1.5 Cloud-based Infrastructure

- **Amazon Web Services (AWS)**:

    - **500 EC2 Instances**: Active for data processing and computation needs across global operations.
    - **250TB S3 Storage**: For storing operational data, donor information, child health data, and educational materials.
    - **75 RDS Databases**: In use globally for managing UNICEF's operational systems (financial, programmatic, HR systems).

- **Microsoft Azure**:

    - **25,000 Active Users**: Managed via Azure Active Directory, representing UNICEF staff worldwide.
    - **30 SQL Databases**: For hosting critical operational systems including HR, finance, and programmatic applications.
    - **50TB Blob Storage**: Used for disaster recovery and storing sensitive program data, including emergency response records and child welfare data.

- **Google Cloud**:

    - **100TB Cloud Storage**: For research and data storage, particularly for child health and education data across **Asia-Pacific**.

---

2. Software Assets

2.1 UNICEF-Developed Applications

- **U-Report**:

    - **Active Users**: ~200,000 users.
    - **Primary Use**: A tool for engaging young people and gathering critical real-time data from over **50 countries** in Africa, Asia, and Latin America.

- **CommCare**:

    - **Active Users**: ~15,000 users.
    - **Primary Use**: Mobile application used in **30+ countries** for data collection in health, education, and child welfare programs.

- **Salesforce**:

    - **Active Users**: ~2,500 users.
    - **Primary Use**: For donor relations, fundraising, and communication, particularly in large fundraising campaigns like **Giving Tuesday**.

- **Sage Intacct**:

    - **Active Users**: ~1,000 users.
    - **Primary Use**: Financial reporting and management for tracking donations, grants, and government funding.

- **ProMIS**:

    - **Active Users**: ~500 users.
    - **Primary Use**: Asset and logistics management system, used globally by field staff to manage supplies.

---

3. Data Assets

3.1 Sensitive Personal Data

- **Children's Data**:
    - **~10 million records** of sensitive data on children, families, and communities, encompassing health, education, and emergency assistance data.
    - **Primary Storage Locations**: AWS, Azure, and Google Cloud, with a distributed infrastructure across global offices.

3.2 Research Data

- **Annual Research Data**:
    - Collected from **5 million children** annually across areas such as health, education, poverty, and development.
    - Data informs **State of the World’s Children Reports**, annual **education assessments**, and other global humanitarian research.

3.3 Financial Data

- **Annual Donations**:
    - **~$6 billion** tracked globally using **Salesforce** and **Sage Intacct**.
    - **Global Financial Users**: ~1,000 financial users across various UNICEF country offices.

---

4. Personnel and External Partners

4.1 Employees

- **Total Employees**: 15,000 employees spread across **190 country offices** worldwide.
- **Key Areas of Work**: Field operations, logistics, health, education, child protection, emergency response, and policy development.

- **Cybersecurity Risks**: Employees in remote or high-risk regions such as **South Sudan**, **Syria**, and **Venezuela** may be more vulnerable to phishing or social engineering attacks.

4.2 External Partners and Vendors

- **External Contractors**:
  - Thousands of contractors working in conflict and post-crisis zones, including **South Sudan**, **Syria**, **Afghanistan**, and **Yemen**.
  - Tasks include emergency response coordination, logistics support, and IT services.
- **IT Service Providers**:
  - Managed IT services provided by **AWS**, **Microsoft**, **Salesforce**, and **Google**.

---

5. Threat Identification and Impact Analysis

5.1 External Threats

- **Cybersecurity Threats**:
  - **Phishing**: High

likelihood of phishing attempts, especially targeting staff with access to donor databases and operational systems.

- **Ransomware**: Increased risk of data encryption attacks, especially on donor-related financial data or field data (health, education).
- **DDoS Attacks**: Potential risk to online fundraising platforms during peak donation periods such as **Giving Tuesday** or holiday campaigns.
- **Data Breaches**: High risk in conflict zones, where digital infrastructure may be compromised.
- **Natural Disasters**:
  - **Floods, Earthquakes, Hurricanes** affecting data centers and field offices, notably in areas such as **South Asia**, **Latin America**, and **Caribbean**.

5.2 Internal Threats

- **Insider Threats**: Risk from internal staff or contractors who may misuse or leak sensitive data, particularly in high-stress or crisis settings.
- **Human Error**: Accidental loss or deletion of data, particularly in emergency response or field operations where data handling is manual and urgent.

---

6. Risk Assessment & Prioritization

Risk	Likelihood	Impact	Risk Rating	Details

Risk	**Likelihood**	**Impact**	**Risk Rating**	**Details**
Phishing Attacks	High	High	**High**	Phishing attacks are one of the most frequent cybersecurity threats faced by international organizations like UNICEF. These attacks exploit human error to gain access to sensitive information through deceptive emails or fake websites. UNICEF’s decentralized structure, with a large number of field offices in conflict zones and high-risk areas, makes it a prime target for cybercriminals. Phishing campaigns have become more sophisticated, using personalized tactics such as spear-phishing and business email compromise (BEC), targeting senior executives, field staff, and partners. The consequences can include financial loss, exposure of confidential data (e.g., donor information, emergency response plans), and damage to organizational reputation. UNICEF must continuously update its training, awareness, and detection systems.

Risk	Likelihood	Impact	Risk Rating	Details
Ransomware/External Cyber Attacks	Medium	High	**High**	UNICEF's increasing reliance on cloud platforms (e.g., AWS, Azure) and external contractors heightens the risk of ransomware attacks. These attacks can cripple critical infrastructure, compromise sensitive data, and cause significant operational disruptions. Cloud-based applications used by UNICEF to manage large datasets (e.g., child protection data, education programs, emergency relief databases) are at high risk, particularly as attackers often target weaknesses in third-party suppliers or service providers. This risk is further compounded by the threat of Distributed Denial of Service (DDoS) attacks, which can disrupt online services and data availability. In conflict zones, where UNICEF's data infrastructure is less resilient, cyber-attacks could delay or halt humanitarian operations, making it a top priority for mitigation.

Risk	Likelihood	Impact	Risk Rating	Details
Data Breaches	High	Very High	**High**	Data breaches are a critical concern due to the sensitive nature of UNICEF’s work. The organization collects a wide range of sensitive information, including health data, financial records, and child protection data, which is a prime target for malicious actors. A breach could lead to the unauthorized release of personally identifiable information (PII), putting vulnerable populations at risk and potentially violating privacy regulations such as the GDPR (General Data Protection Regulation). The growing use of third-party contractors, partners, and field offices increases the number of access points for potential breaches, especially in areas with poor cyber hygiene. In the event of a breach, the trust between UNICEF, donors, and beneficiaries could be severely compromised, leading to reputational damage and loss of funding.

Risk	Likelihood	Impact	Risk Rating	Details
Natural Disasters (Flood, Earthquake)	Medium	Very High	**High**	Natural disasters, such as floods, earthquakes, and hurricanes, have an outsized impact on UNICEF's operations, especially in vulnerable and low-resilience regions like the Philippines, Haiti, and parts of Africa and Asia. These events can disrupt supply chains, destroy physical infrastructure (e.g., offices, warehouses), and displace millions of people, creating a surge in demand for UNICEF's emergency services. Natural disasters also pose risks to data loss or system downtime if critical hardware or servers are damaged. Field staff working in disaster-prone areas face additional challenges with communication and mobility, further complicating humanitarian efforts. Despite the organization's disaster preparedness strategies, the unpredictability and magnitude of such events require continuous investment in mitigation measures to ensure business continuity during and after disasters.

Risk	Likelihood	Impact	Risk Rating	Details
Theft/Loss of Devices	Medium	High	**High**	With over 10,000 staff members across more than 190 countries, the risk of theft or loss of devices (e.g., laptops, mobile phones, USB drives) is a constant threat. This is particularly problematic in regions with high rates of crime or during the transportation of staff or materials to conflict zones and humanitarian settings. A lost or stolen device could lead to exposure of highly sensitive data, including donor records, health data, and security information. The use of unsecured devices or failure to implement proper security measures (e.g., password protection, device encryption) increases this risk. Specific examples of incidents, such as the theft of laptops containing sensitive data from field offices or the loss of devices during emergencies, have already been reported in the past. Therefore, strict policies regarding device management, security protocols, and remote wipe capabilities are necessary.

Risk	Likelihood	Impact	Risk Rating	Details
Insider Threat	Low	Very High	**Medium**	Insider threats, while less common, carry substantial risk due to the sensitivity of the data handled by UNICEF employees and contractors. The organization relies on a large, diverse workforce, including employees in high-risk regions. Insider threats can include malicious actions (e.g., data theft, sabotage) or inadvertent mishandling of sensitive information (e.g., failing to follow data access protocols). Although the risk is relatively low, the consequences can be devastating, particularly for staff working in conflict zones with access to sensitive child protection and health data. Insider threats can also extend to contractors, partners, or vendors who have access to critical data systems. Regular monitoring, robust access controls, and internal audits are essential to minimizing the risk of insider threats.
Human Error (Data Loss)	High	Medium	**Medium**	Human error is one of the most common causes of data loss or exposure in global organizations. UNICEF's global operations, combined with the diversity of languages, cultures, and levels of technological literacy among staff, increase the likelihood of mistakes such as accidental data deletion, improper sharing of files, or failure to comply with data security policies. In field offices, where staff are under pressure to deliver quick responses, human error can lead to the accidental exposure or loss of critical information. The use of manual processes or outdated systems in certain regions may further exacerbate the likelihood of mistakes. Training, clear data management policies, and automated data backup systems are necessary to minimize human error.

7. Mitigation Strategies

1. Phishing Awareness Campaign

- **Action**:
  - Implement a global **phishing awareness program** that is tailored for regional contexts and local threats. The program will include **interactive training sessions**, **simulated phishing exercises**, and **ongoing assessments** to test staff preparedness.
  - Engage **third-party cybersecurity experts** to conduct in-depth phishing simulations, and provide regional offices with specific guidelines based on the most common attack types in their geography.
  - Educate staff on **red flags** such as unfamiliar senders, suspicious attachments, and unsolicited links in emails, with a special focus on **spear-phishing** and **CEO fraud** that often target senior leaders.
  - Collaborate with global email filtering services and ensure **automatic blocking** of phishing-related emails and malicious attachments.
- **Timeline**:
  - Immediate training for **high-risk regions** (e.g., conflict zones, emerging markets) within **1 month**.
  - Full global program rollout within **3 months**, with regular **bi-annual refresher courses**.
- **Impact**:
  - Significant reduction in phishing-related incidents and a more informed staff capable of recognizing and preventing phishing attempts. Improved resilience to social engineering attacks.

2. Data Encryption

- **Action**:
  - Ensure **end-to-end encryption** is applied across all mobile devices, laptops, and cloud-based services (e.g., AWS, Azure) to secure data during transmission and storage.
  - Integrate encryption solutions that comply with **GDPR** and other regional data protection laws, ensuring that all sensitive data, including child protection and health records, is encrypted both in transit and at rest.
  - Implement **hardware-based encryption** solutions for field staff devices, with automatic encryption triggered upon boot-up.
  - Regularly update encryption standards and assess their effectiveness to counter emerging threats (e.g., quantum computing).
- **Timeline**:
  - **Immediate encryption implementation** for high-risk field operations and critical systems (e.g., donor data, child protection records).
  - **Full implementation** globally within **6 months**, with periodic **annual audits**.
- **Impact**:
  - Data remains secure even in the event of device theft or breach, significantly lowering the risk of unauthorized access to sensitive information.

3. Multi-Factor Authentication (MFA)

- **Action**:

  - Require MFA for all employees and contractors accessing critical systems (e.g., cloud services, financial data, internal databases) to prevent unauthorized access, even if credentials are compromised.
  - Provide support for **biometric authentication** or **hardware tokens** for high-ranking personnel and those working in sensitive regions or on high-stakes projects.
  - Integrate MFA with **VPNs** and ensure secure access to remote systems for field staff.
- **Timeline**:
  - Implement MFA for **critical systems** within **2 months** (e.g., AWS, Salesforce, and donor platforms).
  - Full **organization-wide MFA** deployment across all systems within **4 months**.
- **Impact**:
  - Drastically reduces the chances of unauthorized access to sensitive systems, especially in case of phishing or credential theft.

4. Backup and Disaster Recovery Plans

- **Action**:
  - Create **regional disaster recovery hubs** to ensure that data can be recovered quickly even in regions prone to natural disasters or conflict. Backup systems should be diversified across cloud and physical locations.
  - Conduct **biannual disaster recovery drills** to test system resilience and the readiness of field staff to recover data remotely or in person.
  - Improve **data redundancy**, ensuring that key data (such as donor records, health data, and project plans) is backed up across multiple geographies, minimizing data loss risk.
- **Timeline**:
  - **1-month review** of current disaster recovery capabilities, followed by **immediate improvements**.
  - Full **testing and implementation** of cloud-based and physical backup redundancies within **6 months**.
- **Impact**:
  - Reduces data loss in case of disasters or ransomware attacks, ensuring that UNICEF’s critical operations can continue even in the face of disruptions.

5. Data Access Control

- **Action**:
  - Enforce **Role-Based Access Control (RBAC)** for all systems to limit access to sensitive data based on the individual’s role, responsibilities, and need-to-know basis.
  - Implement **frequent audits** of access logs to detect unauthorized attempts and anomalies, and conduct **quarterly reviews** of user access rights.
  - Establish **least-privilege access** protocols and ensure that employees only have access to the data required to perform their job functions.
  - Implement **automated access reviews** for third-party contractors and vendors with access to critical systems and data.
- **Timeline**:
  - **Ongoing implementation**, with an initial review within **3 months** to ensure that the RBAC model is functioning across all major systems.

- **Impact**:
  - Improved control over sensitive data, with reduced risks of insider threats or accidental data exposure through access rights that align with job needs.