

## A.3.1 Document: Risk Acceptance Policy

- **Purpose:** This policy defines the formal process and criteria by which the World Bank will evaluate and accept identified cybersecurity risks that, for valid reasons, will not be fully mitigated, avoided, or transferred. The policy ensures that risk acceptance is a conscious, documented, and authorized decision, reflecting a clear understanding of potential impacts and the presence of any compensating controls. Financial institutions operate under significant regulatory scrutiny, and a robust risk acceptance process is a key indicator of mature risk management.
- **Scope:** This policy applies to all information systems, services, data, and processes within the World Bank where cybersecurity risks are identified.
- **Principles:**
  - Risk acceptance is considered only when other risk treatment options (mitigation, avoidance, transfer) are demonstrated to be impractical, excessively costly relative to the risk, or would unacceptably impede critical business functions.
  - All risks subject to acceptance must be clearly identified, analyzed, and documented, including their potential impact on the Bank's operations, finances, reputation, and legal/regulatory obligations.
  - Risk acceptance decisions must be justified by a clear business rationale.
  - Where a risk is accepted, any existing or planned compensating controls designed to reduce the likelihood or impact of the risk must be documented and maintained.
  - Risk acceptance is not permanent and is subject to periodic review and re-approval.
- **Process:**
  1. **Risk Identification and Assessment:** Cybersecurity risks are identified through various means (e.g., risk assessments, vulnerability scans, audits, incident analysis), consistent with the Bank's overall risk management framework (Phase 3 of the user's study plan).
  2. **Evaluation of Treatment Options:** For each significant identified risk, potential treatment options (mitigate, avoid, transfer) are evaluated.
  3. **Formal Request for Risk Acceptance:** If acceptance is deemed the most appropriate option, the Risk Owner (typically the Information Asset Owner or a relevant business/IT manager) must submit a formal "Risk Acceptance Form" (an appendix to this policy, inspired by templates such as those related to NIST 800-53 deficiencies ). This form will include:

- A detailed description of the risk and the specific control deficiency or vulnerability.
- The potential business impact if the risk materializes (financial, operational, reputational, legal/regulatory).
- A clear justification for why the risk cannot be reasonably mitigated, avoided, or transferred.
- A description of any existing or proposed compensating controls.
- The requested duration for the risk acceptance (e.g., not to exceed one year without review ).

4. **Review and Approval:** The submitted Risk Acceptance Form is reviewed by the CISO (for cybersecurity implications) and other relevant stakeholders. Approval authority depends on the assessed level of the risk:

- Low-level risks: May be approved by the relevant Head of Department in consultation with the CISO.
- Medium-level risks: May require approval from a Director-level manager and the CISO.
- High-level risks: Must be escalated to the Security Steering Committee or a higher-level Risk Committee, potentially requiring approval from an Executive Vice President or equivalent.

5. **Documentation:** All approved risk acceptances, along with their justifications and compensating controls, are recorded in a central Risk Register maintained by the Office of Risk Management or the Cybersecurity Department.

6. **Monitoring and Review:** Accepted risks and the effectiveness of their compensating controls are subject to regular monitoring. The acceptance itself must be reviewed and re-validated before its expiration date. Changes in the threat landscape, business environment, or availability of new mitigation technologies may necessitate a re-evaluation of the acceptance decision.

- **Roles and Responsibilities:**

- **Risk Owner:** Initiates the risk acceptance request and is responsible for implementing and monitoring compensating controls.
- **CISO:** Reviews risk acceptance requests for cybersecurity implications, advises on compensating controls, and ensures consistency with overall security strategy.
- **Business Unit Heads/Management:** Provide business context and approval for accepting risks within their areas of responsibility.

- **Security Steering Committee/Risk Committee:** Reviews and approves high-level risk acceptances, ensuring alignment with the Bank's overall risk appetite.
- **Alignment with Enterprise Risk Management (ERM):** The cybersecurity risk acceptance process is an integral part of, and must align with, the World Bank's overarching Enterprise Risk Management framework. Accepted cybersecurity risks are reported to the ERM function as appropriate.

The formality of this process, including defined approval thresholds and time-limited acceptances, reflects the due diligence expected of a global financial institution. It ensures that decisions to accept risk are transparent, accountable, and regularly revisited.

### A.3.2 Document: Escalation Policy (for security incidents)

- **Purpose:** This policy defines the standardized procedures for escalating security incidents within the World Bank. The primary objectives are to ensure that incidents are addressed by the appropriate personnel in a timely manner, that necessary resources are allocated effectively, and that the impact of incidents on the Bank's operations, assets, and reputation is minimized.
- **Scope:** This policy applies to all detected or reported security events and incidents affecting WDB information systems, data, personnel, or facilities.
- **Severity Levels:** Incidents are classified based on their actual or potential impact. The WDB uses a four-tier severity scale :
  - **SEV 1 (Critical):** Incidents that cause or have the imminent potential to cause severe disruption to critical Bank operations, significant financial loss, widespread unauthorized disclosure of highly sensitive data (e.g., Level 4 or Level 3 data), major regulatory breaches, or extensive reputational damage. Requires immediate, highest-priority response.
  - **SEV 2 (High):** Incidents that cause or could cause significant disruption to important services, moderate financial loss, unauthorized disclosure of sensitive data (e.g., Level 3 or some Level 2 data), notable regulatory impact, or reputational harm. Requires urgent response.
  - **SEV 3 (Medium):** Incidents that cause or could cause minor disruption to non-critical services, limited financial loss, unauthorized disclosure of internal or less sensitive data (e.g., Level 2 data), or minor policy violations. Requires timely response.
  - **SEV 4 (Low):** Incidents with minimal impact, such as isolated attempts to exploit non-critical vulnerabilities, minor policy deviations, or localized malware infections with no significant spread. Handled through standard operational procedures.

- **Escalation Triggers:** Escalation may be triggered by:
  - **Severity Level:** The initial assessed severity of the incident automatically dictates the initial response level and potential immediate escalations (e.g., all SEV 1 incidents are immediately escalated to the CISO and relevant executive management).
  - **Time-Based Triggers:** If an incident is not contained, resolved, or adequately addressed within predefined timeframes for its severity level (e.g., a SEV 2 incident not contained within 4 hours may be escalated).
  - **Impact-Based Triggers:** If the scope or impact of an incident increases beyond its initial assessment (e.g., an incident initially thought to be SEV 3 is found to affect critical systems or data, requiring reclassification and escalation to SEV 1 or SEV 2).
  - **Resource/Expertise-Based Triggers:** If the current response team lacks the necessary authority, skills, or resources to effectively manage the incident.
  - **External Requirements:** If the incident triggers mandatory external reporting or communication requirements (e.g., to regulators, law enforcement).
- **Escalation Paths:**
  - **Technical/Hierarchical Escalation:** Incidents are escalated through tiers of technical support and management within the IT and Cybersecurity departments, up to the IT Manager, CISO, and potentially the CIO/CTO.
  - **Functional Escalation:** Incidents are escalated to other relevant departments or specialized teams based on the nature of the incident. This includes:
    - **Data Protection Officer (DPO):** For any incident involving personal data.
    - **Legal Department:** For incidents with legal implications, contractual breaches, or potential litigation.
    - **Human Resources:** For incidents involving employee misconduct or requiring internal investigations.
    - **Communications Department:** For incidents that may require internal or external communication (media, clients, public).
    - **Business Unit Management:** For incidents impacting specific business operations or services, to inform the relevant Information Asset Owners or business leaders.
    - **Forensics Team:** For incidents requiring in-depth investigation and evidence preservation.

- **Management Escalation:** For SEV 1 and significant SEV 2 incidents, escalation proceeds to senior executive management, the Security Steering Committee, and potentially the Board or a Board committee, as defined in the Incident Management Policy.
- The WDB Security Operations Center (SOC), if established, or a central IT Service Desk often serves as the initial point for incident reporting and may coordinate initial escalation steps.
- **Notification Procedures:**
  - **Who to Notify:** Defined lists of internal and external contacts for each severity level and incident type.
  - **How to Notify:** Primary and backup communication channels (e.g., dedicated incident response platform, secure email, phone calls, SMS alerts). Automated alerting systems are used where appropriate.
  - **Content of Notifications:** Notifications must be clear, concise, factual, and provide necessary context for the recipient to understand the situation and their required actions. Standardized templates may be used.
- **Roles and Responsibilities:**
  - **First Responders (e.g., SOC Analysts, Help Desk Staff):** Initial detection, logging, preliminary assessment, and initiation of escalation as per this policy.
  - **Incident Handlers/CIRT Members:** Manage the technical response, escalate as needed.
  - **Incident Manager:** Coordinates the overall response for significant incidents (see Incident Management Policy A.3.3).
  - **CISO, DPO, IT Management, Business Unit Liaisons:** Participate in escalated incidents according to their roles.
- **Global Operations Considerations:** Given WDB's global presence, this policy must account for incidents occurring across different time zones. "Follow-the-sun" operational models for SOC or incident response teams may be implemented, with clear hand-off procedures. Contact information and availability schedules for key personnel in different regions must be maintained and readily accessible. Escalation thresholds and communication protocols are designed to ensure timely response regardless of where or when an incident occurs.

This Escalation Policy is a component of the broader Incident Management Policy (Section A.3.3) and is regularly reviewed and updated based on lessons learned from incidents and exercises.

## A.3.3 Document: Incident Management Policy

- **Purpose:** This policy establishes a comprehensive and consistent framework for the World Bank to prepare for, detect, analyze, contain, eradicate, recover from, and conduct post-incident analysis of cybersecurity incidents. The aim is to minimize operational, financial, and reputational damage, restore affected services promptly and securely, preserve evidence for potential investigations, and meet all legal and regulatory obligations.
- **Scope:** This policy applies to all World Bank information systems, applications, data, networks, personnel (including employees, contractors, and third parties with access to WDB systems), and facilities.
- **Objectives:**
  - To ensure a rapid, effective, and orderly response to security incidents.
  - To limit the immediate impact and prevent further escalation of incidents.
  - To restore normal Bank operations as quickly and securely as possible.
  - To preserve forensic evidence in a manner that supports internal reviews and potential legal or disciplinary actions.
  - To meet all applicable legal, regulatory, and contractual requirements for incident reporting and notification.
  - To identify lessons learned from incidents to improve security controls, policies, and procedures.
- **Incident Response Lifecycle:** The WDB adopts an incident response lifecycle aligned with industry best practices, such as the NIST Cybersecurity Framework, encompassing the following phases :

### 1. **Preparation:**

- Conducting regular risk assessments to identify potential threats and vulnerabilities.
- Developing and maintaining specific incident response playbooks for common and high-impact incident types (e.g., ransomware, data breaches involving sensitive client data, denial-of-service attacks, insider threats).
- Establishing and training the Cyber Incident Response Team (CIRT).
- Acquiring, configuring, and maintaining necessary incident response tools and technologies (e.g., SIEM, EDR, forensics tools).
- Conducting regular incident response training and simulation exercises.

2. **Detection and Analysis:**

- Utilizing various monitoring sources (e.g., SIEM alerts, IDS/IPS, antivirus, firewall logs, user reports, external intelligence) to detect potential security events.
- Establishing clear mechanisms for reporting suspected incidents by all personnel.
- Performing initial triage to validate whether a reported event constitutes a security incident.
- Assessing the severity and potential impact of the incident (linking to the Escalation Policy A.3.2).
- Initiating evidence gathering and preservation procedures.

3. **Containment:**

- Taking immediate actions to limit the scope and impact of the incident (e.g., isolating affected systems or network segments, blocking malicious IP addresses, disabling compromised accounts).
- Implementing short-term fixes to prevent further damage while a long-term solution is developed.
- Preserving data and logs that could be critical for eradication and recovery.

4. **Eradication and Recovery:**

- Identifying and eliminating the root cause of the incident (e.g., removing malware, patching vulnerabilities, addressing misconfigurations).
- Securely restoring affected systems and data from clean backups.
- Validating that systems are clean and functioning normally.
- Implementing additional monitoring or hardening measures to prevent recurrence.

5. **Post-Incident Activity (Lessons Learned):**

- Conducting a thorough post-incident review to analyze the cause, the Bank's response, and the effectiveness of existing controls and procedures.
- Documenting lessons learned and identifying areas for improvement.
- Updating security policies, procedures, playbooks, and controls as necessary.

- Preparing and disseminating internal and external incident reports as required.
- **Cyber Incident Response Team (CIRT):**
  - **Mandate:** The CIRT is the designated team responsible for coordinating and executing the response to significant security incidents.
  - **Composition:**
    - **Core Team:** Comprised of dedicated security analysts, incident responders, forensics specialists, and IT operations personnel.
    - **Extended Team:** Activated as needed, including representatives from the DPO's office (for personal data breaches), Legal, Human Resources, Communications, Risk Management, Internal Audit, and relevant business units (including Information Asset Owners).
  - **Incident Manager:** For each significant incident, an Incident Manager is designated (often a senior member of the CISO's team or the CISO themselves for critical incidents). The Incident Manager has the authority to coordinate all response activities, make critical decisions during the incident, and serve as the primary point of contact for internal and external stakeholders.
- **Communication Plan:** Effective communication is critical during and after an incident.
  - **Internal Communication:** Procedures for informing relevant internal stakeholders, including technical teams, management, affected employees, and the Security Steering Committee. Communication channels and frequency are defined based on incident severity.
  - **External Communication:** Procedures for communicating with external parties. This is particularly vital for a financial institution like WDB. This includes:
    - **Affected Clients/Partners:** Timely and transparent communication if their data or services are impacted.
    - **Regulatory Bodies:** Adherence to all mandatory breach notification requirements under applicable financial and data protection regulations (e.g., timelines and content of notifications for frameworks like DORA or national banking supervisor rules). The WDB operates in multiple jurisdictions, necessitating a clear understanding of varied reporting obligations.
    - **Law Enforcement:** Cooperation with law enforcement agencies as appropriate.

- **Media:** Coordinated responses through the Communications Department, using pre-approved statement templates where possible, to manage reputational impact.
- **Reporting Requirements:**
  - **Internal Incident Reports:** Detailed reports are prepared for all significant incidents, documenting the timeline, impact, response actions, root cause, and lessons learned.
  - **Regulatory Breach Notifications:** The Legal department, in conjunction with the DPO and CISO, manages all required notifications to regulatory authorities.
- **Training and Awareness:**
  - Regular, specialized training for all CIRT members on incident response procedures, tools, and techniques.
  - General awareness training for all Bank personnel on how to identify and report suspected security incidents promptly.
- **Coordination with Business Continuity (BC) and Disaster Recovery (DR) Plans:** This policy defines clear triggers and interfaces for invoking the Bank's BC and DR plans in the event an incident causes significant disruption to critical business processes or IT systems. The CIRT works closely with BC/DR teams during such events.