# 30 IT Risk Controls for Banks

## Access & Identity Management

* C-01 | User Access Provisioning\*\*

Description: New user access to IT systems is granted only upon formal approval by the responsible system owner.

Frequency: Event-driven

Owner: IT Access Management

Evidence: Approved access request forms / tickets.

* C-02 | Periodic User Access Review\*\*

Description: User access rights are reviewed at least quarterly by system/application owners to ensure appropriateness.

Frequency: Quarterly

Owner: Application Owner / Business Process Owner

Evidence: Access review logs, sign-offs.

* C-03 | Segregation of Duties (SoD) Control\*\*

Description: Critical system roles are monitored to prevent toxic combinations of duties (e.g., developer + production access).

Frequency: Ongoing / Quarterly review

Owner: IT Security

Evidence: SoD matrix, review reports.

* C-04 | Privileged Access Management\*\*

Description: Administrative and privileged accounts are centrally managed and usage is logged and reviewed.

Frequency: Ongoing, with monthly review

Owner: IT Security / System Administrators

Evidence: PAM tool logs, review reports.

* C-05 | Leaver Access Removal\*\*

Description: IT disables or removes access rights of departing employees within 24 hours of termination.

Frequency: Event-driven

Owner: HR & IT Access Management

Evidence: De-provisioning tickets.

## Change & Development Management

* C-06 | Change Request Approval\*\*

Description: All system changes require documented approval from business and IT owners before implementation.

Frequency: Event-driven

Owner: Change Manager

Evidence: Change request system logs.

* C-07 | Segregation of Change Duties\*\*

Description: Developers cannot migrate their own code into production; separate roles enforce this.

Frequency: Ongoing

Owner: IT Operations

Evidence: Deployment logs, access restrictions.

* C-08 | Pre-Implementation Testing\*\*

Description: System changes are tested in a controlled test environment before release to production.

Frequency: Event-driven

Owner: IT Development / QA

Evidence: Test scripts, test results.

* C-09 | Emergency Change Management\*\*

Description: Emergency changes follow an expedited approval process and are documented and retrospectively reviewed.

Frequency: Event-driven

Owner: Change Manager

Evidence: Emergency change logs, approval evidence.

* C-10 | Code Version Control\*\*

Description: Source code is maintained in a version control system with restricted access and logging.

Frequency: Ongoing

Owner: IT Development

Evidence: Version control logs.

## IT Operations & Infrastructure

* C-11 | Daily Backup Execution\*\*

Description: Critical data and systems are backed up daily, and backup success is monitored.

Frequency: Daily

Owner: IT Infrastructure

Evidence: Backup logs.

* C-12 | Backup Restoration Testing\*\*

Description: Backup restorations are tested periodically to ensure data integrity.

Frequency: Semi-annual

Owner: IT Infrastructure

Evidence: Test reports.

* C-13 | Patch Management\*\*

Description: Security patches are assessed, approved, and deployed according to defined timelines (e.g., critical within 30 days).

Frequency: Monthly

Owner: IT Security / Infrastructure

Evidence: Patch logs, vulnerability scans.

* \*\*C-14 | Malware Protection\*\*

Description: Anti-malware software is installed, updated, and monitored across all endpoints and servers.

Frequency: Ongoing

Owner: IT Security

Evidence: AV monitoring reports.

* \*\*C-15 | Log Monitoring & Alerting\*\*

Description: Security and system logs are monitored daily, and critical alerts are investigated promptly.

Frequency: Daily

Owner: IT Security Operations (SOC)

Evidence: SIEM reports, incident tickets.

## Business Continuity & Incident Management

* \*\*C-16 | IT Incident Management\*\*

Description: IT incidents are logged, classified, and resolved according to defined procedures and SLAs.

Frequency: Ongoing

Owner: IT Service Desk

Evidence: Incident tickets.

* \*\*C-17 | Root Cause Analysis (RCA)\*\*

Description: Major IT incidents undergo documented RCA, and corrective actions are tracked.

Frequency: Event-driven

Owner: IT Problem Management

Evidence: RCA reports.

* \*\*C-18 | Disaster Recovery (DR) Plan\*\*

Description: A documented DR plan exists and is updated annually.

Frequency: Annual

Owner: IT Continuity Manager

Evidence: DR documentation.

* \*\*C-19 | DR Testing\*\*

Description: DR tests (failover / recovery drills) are conducted at least annually.

Frequency: Annual

Owner: IT Continuity Manager

Evidence: Test results, lessons learned.

* \*\*C-20 | Critical System Monitoring\*\*

Description: Critical banking applications are monitored 24/7 with automated alerts for downtime or performance issues.

Frequency: Ongoing

Owner: IT Operations

Evidence: Monitoring dashboards.

## Cybersecurity & Data Protection

* \*\*C-21 | Network Security Monitoring\*\*

Description: Firewalls, IDS/IPS, and security gateways are configured and monitored for suspicious activity.

Frequency: Ongoing

Owner: IT Security

Evidence: Firewall logs, SOC alerts.

* \*\*C-22 | Data Encryption\*\*

Description: Sensitive customer and financial data is encrypted in transit (TLS) and at rest (AES-256 or equivalent).

Frequency: Ongoing

Owner: IT Security / Data Owners

Evidence: Encryption settings, configs.

* \*\*C-23 | Secure Configuration Management\*\*

Description: Systems are hardened according to secure baseline configurations and deviations are remediated.

Frequency: Quarterly

Owner: IT Infrastructure

Evidence: Baseline reports, vulnerability scans.

* \*\*C-24 | Vendor Security Assessment\*\*

Description: Third-party IT service providers undergo security risk assessments before onboarding and periodically thereafter.

Frequency: Annual / Event-driven

Owner: Vendor Management / IT Security

Evidence: Vendor risk reports.

* \*\*C-25 | Phishing Simulation & Awareness\*\*

Description: Periodic phishing simulations and mandatory user training to improve awareness.

Frequency: Quarterly

Owner: IT Security / HR Training

Evidence: Training logs, simulation reports.

## Governance & Compliance

* \*\*C-26 | IT Risk Assessment\*\*

Description: Annual risk assessment of IT processes, infrastructure, and applications.

Frequency: Annual

Owner: IT Risk Management

Evidence: Risk assessment report.

* C-27 | Policy & Procedure Review\*\*

Description: IT security and risk policies are reviewed and updated at least annually.

Frequency: Annual

Owner: IT Governance

Evidence: Approved policies.

* C-28 | Data Loss Prevention (DLP)\*\*

Description: DLP tools are configured to detect and prevent unauthorized transfer of sensitive data.

Frequency: Ongoing

Owner: IT Security

Evidence: DLP monitoring reports.

* C-29 | User Security Awareness Training\*\*

Description: All employees complete mandatory annual IT security awareness training.

Frequency: Annual

Owner: HR & IT Security

Evidence: Training records.

* C-30 | Compliance Monitoring & Reporting\*\*

Description: Compliance with IT regulations (FINMA, ISO 27001, GDPR, etc.) is monitored and reported regularly.

Frequency: Quarterly

Owner: IT Compliance

Evidence: Compliance reports.