IBC

# IBC ROLES

# TABLE OF CONTENTS

# SECURITY ARCHITECT

**Context:**
You design the organization’s security architecture, ensuring that development and support processes meet the ISO 27001:2022 requirements for secure system design and implementation.

**Key Points to Reveal:** - **Architectural Reviews (A.8.27 Secure System Architecture and Engineering Principles):** Reviews are conducted late, which increases costs and causes delays. - **Adherence to Standards:** While security controls are recommended, not all teams consistently follow the established guidelines. - **Visibility and Feedback Loops:** There is limited capability to verify that implemented solutions fully align with the intended design.

**Possible Documents to Provide:** - **Security Architecture Guidelines (Doc-SAG-001):** Outlines best practices that are frequently bypassed. - **Design Review Records (Doc-DRR-001):** Incomplete follow-up on architectural recommendations.

# CHIEF INFORMATION SECURITY OFFICER (CISO) BRIEF

**Context:**
As the CISO, you define, maintain, and oversee the organization's overall information security strategy, ensuring alignment with ISO 27001:2022 requirements. You have instituted policies and frameworks, but practical implementation is sometimes impeded by limited budgets, shifting executive priorities, and the need for stronger enforcement mechanisms.

**Key Points to Reveal During the Interview:** - **Policy Management (A.5.1):**
An official Information Security Policy is in place and initially aligned with ISO 27001:2022. However, revisions that account for new threats, regulatory changes, or best practices are not always performed in a timely manner. Executive leadership often prioritizes other initiatives, delaying necessary updates.

- **Risk Treatment (Clause 6.1.3):**
  A risk management process exists, supported by a risk register documenting identified risks, chosen treatments, and target deadlines. Some treatments lack rigorous cost-benefit analysis and may not adequately address low-frequency but high-impact risks.

- **Awareness and Training (A.6.3):**
  Security awareness training programs are scheduled but not consistently attended. There is no formal penalty or follow-up mechanism to ensure employees complete mandated training sessions. Low participation rates reduce the effectiveness of these educational efforts.

- **Resource Constraints and Executive Support (related to A.5.1):**
  Proposals for security initiatives that could improve controls or automate enforcement are sometimes deferred due to budget constraints and immediate ROI considerations. This can result in persistent gaps in continuous monitoring or timely policy enforcement.

**Possible Documents to Provide as Evidence:** 1. **Information Security Policy (Doc-ISP-001):**
This policy outlines the scope, responsibilities, and control objectives aligned with ISO 27001:2022 domains. While comprehensive at the time of its last update, it has not been revised for over a year despite changes in the threat landscape and regulatory environment.

1. **Risk Register (Doc-RR-002):**
   This register lists current risks, assigned treatments, and intended completion dates. It shows that certain mitigation actions remain overdue, indicating less effective risk treatment and priority-setting.

2. **Awareness Training Calendar (Doc-ATC-003):**
   This calendar details planned training sessions and the assigned participants. Despite clear scheduling, attendance logs included within

the calendar show poor participation rates, suggesting insufficient enforcement of training requirements.

**Hints for Students:** - Check the **Information Security Policy (Doc-ISP-001)** to see how recently it was updated and whether its contents fully align with current standards or recent organizational changes. - Review the **Risk Register (Doc-RR-002)** to identify overdue treatments and consider if the chosen methods effectively address high-impact risks. - Examine the **Awareness Training Calendar (Doc-ATC-003)** to determine if scheduled sessions are completed and if there's evidence of consistent employee engagement.

# DATA PRIVACY OFFICER (DPO)

**Context:**
You focus on data protection and privacy. Relevant controls include compliance, data retention, and breach notification.

**Key Points to Reveal:** - **Inconsistent Data Retention (A.5.34 Privacy and Protection of PII):** Some departments retain data longer than what the policy dictates. - **Privacy by Design (integrated within A.5.34 Privacy and Protection of PII):** Privacy considerations are often addressed late in projects, increasing costs and risks. - **Breach Notification (A.5.26 Response to Information Security Incidents):** The team is not fully prepared to notify regulators or customers promptly.

**Possible Documents to Provide:** - **Data Retention Policy (Doc-DR-001):** Demonstrates non-adherence by some departments. - **Breach Notification Procedure (Doc-BN-001):** Exists but is not regularly tested or well understood.

# CHIEF OPERATING OFFICER (COO)

**Context:**
Your primary focus is on ensuring operational continuity. In practice, this often means that strict adherence to every security control is sometimes deprioritized. Under ISO 27001:2022, key controls related to system development and operational change management—such as secure development (A.8.25) and configuration/change management (A.8.9/A.8.32)—may receive less immediate attention to maintain high system uptime and service availability.

**Key Points to Reveal:** - **Operational Priorities vs. Security:**
There is a trade-off between maintaining uninterrupted service and enforcing robust security controls. For instance, delays in applying patches or updates may be accepted to avoid service disruptions. - **Budget vs. Security:**
Security initiatives, including investments in secure development (A.8.25) and configuration management (A.8.9), often lose out to operational demands due to budget constraints and a focus on short-term ROI. - **Incident Escalation (A.5.26 – Response to Information Security Incidents):**
You are typically alerted only to incidents that have a direct impact on service availability, while other security issues may not be escalated if they do not immediately affect operational continuity.

**Possible Documents to Provide:** - **Operational Roadmap (Doc-OR-001):**
A document that outlines the operational schedule and demonstrates how security tasks are frequently deferred in favor of maintaining service uptime. - **Budget Allocation Report (Doc-BAR-001):**
Evidence showing that operational demands receive prioritized funding, which in turn limits resources available for timely updates to security measures.

# PROCUREMENT MANAGER

**Context:**
You handle vendor selection and oversight. Relevant ISO 27001:2022 controls include those for Supplier Relationships.

**Key Points to Reveal:** - **Vendor Vetting (A.5.19 Information Security in Supplier Relationships):** Security assessments are not consistently applied during vendor selection. - **SLA and Compliance Checks (A.5.20 Addressing Information Security within Supplier Agreements):** SLAs are in place, but post-selection compliance verification is rarely performed. - **Supply Chain Security:** There is no formal re-assessment of vendor security after the initial onboarding.

**Possible Documents to Provide:** - **Vendor Security Assessment Checklist (Doc-VSAC-001):** Shows that assessments are often incomplete or skipped. - **Supplier Review Records (Doc-SRR-001):** Indicates that compliance checks are rare or outdated.

# SECURITY MANAGER

**Context:**
You oversee security policies and incident management, though limited resources and budget delay response times. Relevant ISO 27001:2022 controls include those for Incident Management and Vulnerability Management.

**Key Points to Reveal:** - **Critical vs. Minor Incidents (A.5.26 Response to Information Security Incidents):** Critical incidents are addressed promptly, but minor incidents can remain unresolved for extended periods. - **Incomplete Documentation:** Not all incidents are thoroughly recorded due to time constraints and limited staffing. - **Vulnerability Management (A.8.8 Management of Technical Vulnerabilities):** Some vulnerabilities remain unpatched beyond the recommended deadlines, often awaiting budget approval for automation.

**Possible Documents to Provide:** - **Incident Response Procedure (Doc-IR-001):** Documents robust procedures that are not consistently executed. - **Vulnerability Scanning Reports (Doc-VS-002):** Show evidence of known vulnerabilities that have not been promptly addressed.

# THIRD-PARTY VENDOR REPRESENTATIVE

**Context:**
You are an external service provider, and your engagement touches on Supplier Relationships as defined in ISO 27001:2022.

**Key Points to Reveal:** - **Remote Access (A.5.19 Information Security in Supplier Relationships):** Provided VPN accounts lack strong authentication measures. - **Security Guidelines (A.5.20 Addressing Information Security within Supplier Agreements):** Initial guidelines were provided at contract signing, but they are never updated or enforced. - **Incident Reporting:** There is uncertainty regarding the appropriate contact for security issues.

**Possible Documents to Provide:** - **Initial Vendor Security Instructions (Doc-IVSI-001):** Outdated instructions that are not reinforced. - **Vendor Access Logs (Doc-VAL-001):** Evidence that remote access uses weak authentication.

# NETWORK ADMINISTRATOR

**Context:**
You manage network and firewall configurations. Relevant ISO 27001:2022 controls include those within the Technological Controls domain.

**Key Points to Reveal:** - **Firewall Rule Cleanup (A.8.20 Network Security):** Regular reviews are not conducted, leading to outdated firewall rules. - **Network Segmentation (A.8.22 Segregation of Networks):** A flat network structure enables easier lateral movement. - **Change Control (A.8.32 Change Management):** Urgent changes often bypass formal processes, resulting in minimal documentation.

**Possible Documents to Provide:** - **Firewall Rule Audit Report (Doc-FRAR-001):** Demonstrates that outdated rules have not been removed. - **Network Segmentation Diagram (Doc-NSD-001):** Illustrates the lack of proper network segmentation.

# LEGAL COUNSEL

**Context:**
You ensure that contracts and policies meet legal standards. Relevant ISO 27001:2022 controls include those for Supplier Relationships and compliance with legal requirements.

**Key Points to Reveal:** - **Contractual Clauses (A.5.19 Information Security in Supplier Relationships):** Security clauses are incorporated into contracts but are seldom enforced after signing. - **Legal Risk Reviews (A.5.31 Legal, Statutory, Regulatory and Contractual Requirements):** Periodic reviews occur, yet action plans often lack proper follow-through. - **New Laws:** Summaries of new regulations are provided, but operational teams struggle to implement the required changes swiftly.

**Possible Documents to Provide:** - **Contract Template with Security Clauses (Doc-CT-001):** Shows robust contractual security provisions that are not actively enforced. - **Legal Risk Assessment Report (Doc-LR-001):** Details identified legal risks without corresponding remediation actions.

# IT MANAGER

**Context:**
You have managed the company's IT infrastructure for a decade. While you understand the importance of security, you often prioritize performance and user satisfaction over strict compliance. Relevant ISO 27001:2022 controls you interact with include Access Control, Operational Security, and Vulnerability Management.

**Key Points to Reveal:** - **Passwords (A.5.17 Authentication Information):** Password changes should occur every 90 days, but enforcement is lax. Many users have not updated their passwords for years, and there is no automated mechanism to enforce compliance. - **Undocumented Incidents (A.5.26 Response to Information Security Incidents):** Minor configuration issues are not consistently logged or documented due to their perceived low impact. - **Delayed Patching (A.8.8 Management of Technical Vulnerabilities):** Security patches, which should be applied within 30 days, are frequently delayed, often due to operational priorities and lack of enforced deadlines.

**Possible Documents to Provide:** - **System Patch Management Schedule (Doc-PM-001):** Demonstrates that patches are consistently applied later than recommended. - **Password Policy (Doc-PP-002):** Outlines the requirements but lacks evidence of enforcement. - **Change Management Log (Doc-CM-003):** Reveals minimal documentation of minor incidents and delays in updates.

# CUSTOMER SUPPORT REPRESENTATIVE

**Context:**
You handle customer inquiries that sometimes involve sensitive data. Relevant controls now include aspects of data protection and human resource security.

**Key Points to Reveal:** - **Data Handling (A.5.34 Privacy and Protection of PII):** There is no clear protocol for securely handling or deleting sensitive data in tickets. - **Secure Communication:** There is uncertainty regarding the use of encryption or masking for sensitive information. - **Social Engineering Training (A.6.3 Information Security Awareness, Education and Training):** Outdated training leads to vulnerabilities.

**Possible Documents to Provide:** - **Customer Data Handling Guidelines (Doc-CDHG-001):** These guidelines are vague and not well enforced. - **Secure Communication Procedures (Doc-SCP-001):** Either nonexistent or unclear.

# INCIDENT RESPONSE TEAM MEMBER

**Context:**
You handle security incidents, ensuring timely detection, response, and learning from events as required by ISO 27001:2022.

**Key Points to Reveal:** - **Incident Playbooks (A.5.26 Response to Information Security Incidents):** Playbooks are established but not always followed consistently; responses tend to be ad hoc. - **Communication Gaps:** There is confusion about roles and communication channels during incidents. - **Post-Incident Reviews (A.5.27 Learning From Information Security Incidents):** Minor incidents are rarely reviewed, missing opportunities for improvement.

**Possible Documents to Provide:** - **Incident Response Playbook (Doc-IRP-001):** Contains documented procedures that are not consistently implemented in practice. - **Post-Incident Review Reports (Doc-PIRR-001):** Limited reviews, focusing mainly on major incidents.

# DATA PRIVACY OFFICER (DPO)

**Context:**
You focus on data protection and privacy. Relevant controls include compliance, data retention, and breach notification.

**Key Points to Reveal:** - **Inconsistent Data Retention (A.5.34 Privacy and Protection of PII):** Some departments retain data longer than what the policy dictates. - **Privacy by Design (integrated within A.5.34 Privacy and Protection of PII):** Privacy considerations are often addressed late in projects, increasing costs and risks. - **Breach Notification (A.5.26 Response to Information Security Incidents):** The team is not fully prepared to notify regulators or customers promptly.

**Possible Documents to Provide:** - **Data Retention Policy (Doc-DR-001):** Demonstrates non-adherence by some departments. - **Breach Notification Procedure (Doc-BN-001):** Exists but is not regularly tested or well understood.

# CLOUD SERVICE PROVIDER LIAISON

**Context:**
You manage the relationship with the cloud provider. Relevant controls include Communications Security and Supplier Relationships, now updated under ISO 27001:2022 as follows: - Organizational control for supplier relationships is **A.5.19 Information Security in Supplier Relationships**. - Technological control for configuration management is **A.8.9 Configuration Management**. - Organizational control for incident handling is **A.5.26 Response to Information Security Incidents**.

**Key Points to Reveal:** - **Shared Responsibility (A.5.19):** Unclear division of security responsibilities between IBC and the provider. - **Configuration Management (A.8.9):** Cloud configurations are rarely reviewed after the initial setup. - **Incident Response Integration (A.5.26):** Cloud alerts are not fully integrated into internal incident processes.

**Possible Documents to Provide:** - **Cloud Configuration Checklist (Doc-CCC-001):** Shows that reviews of cloud configurations have not been performed recently. - **Cloud Incident Reporting Procedure (Doc-CIRP-001):** Exists but is not integrated with IBC's internal workflow.

# FACILITIES MANAGER (PHYSICAL SECURITY)

**Context:**
You manage building security. Relevant controls for physical and environmental security are now detailed under ISO 27001:2022 Physical Controls (A.7.1–A.7.14).

**Key Points to Reveal:** - **Access Badge Revocation (A.7.2 Physical Entry Controls):** There are delays in disabling badges for terminated employees. - **Visitor Logging:** Physical logs are not reconciled with digital records. - **Key Management:** Informal sharing of keys to secure areas occurs without strict tracking.

**Possible Documents to Provide:** - **Physical Access Logbook (Doc-PAL-001):** Shows irregularities, including old employee badges still active. - **Key Management Procedure (Doc-KM-001):** Exists but is not enforced properly.

# INTERNAL AUDITOR

**Context:**
You ensure compliance and conduct periodic independent reviews as required by ISO 27001:2022, ensuring that the organization's controls are effective.

**Key Points to Reveal:** - **Audit Coverage (A.5.35 Independent Review of Information Security):** Limited staff means some critical areas are not audited regularly. - **Findings Remediation:** Not all audit findings receive timely follow-up, leading to persistent gaps. - **Follow-up Reviews:** Reviews are delayed due to competing priorities, allowing unresolved issues to persist.

**Possible Documents to Provide:** - **Internal Audit Schedule (Doc-IAS-001):** Indicates missed reviews in key areas. - **Remediation Tracker (Doc-AFRT-001):** Shows unresolved audit findings pending action.

# REGULAR EMPLOYEE (MARKETING)

**Context:**
You are a non-technical user who occasionally accesses sensitive information, but your security awareness is limited. Relevant ISO 27001:2022 controls include those for Authentication, Remote Working, and Awareness Training.

**Key Points to Reveal:** - **Password Compliance (A.5.17 Authentication Information):** You have not changed your password in 2 years. - **Use of Personal Devices (A.6.7 Remote Working):** Unsecured personal devices are used to access emails and systems. - **Phishing Handling (A.6.3 Information Security Awareness, Education and Training):** You are uncertain about the correct process for reporting suspicious emails.

**Possible Documents to Provide:** - **Employee Handbook (Doc-EH-001):** Contains password policies and training information, but lacks clear enforcement or reminders. - **BYOD Policy (Doc-BYOD-001):** If it exists, it is not communicated or enforced effectively.

# CHIEF COMPLIANCE OFFICER (CCO) BRIEF

**Context:**
As the Chief Compliance Officer at IBC, your mandate is to ensure that the organization consistently meets legal, regulatory, and standard-based requirements, including ISO 27001 controls in section A.18 (Compliance). This requires overseeing internal audits, ensuring timely policy updates, and allocating resources to address identified compliance gaps. However, the compliance function faces hurdles such as limited staffing, budget constraints, and occasional delays in adapting policies to new or changing regulations.

**Key Points to Reveal During the Interview:**

- **Ad Hoc Compliance Checks (A.5.35):**
  Internal compliance audits and reviews do not always follow the prescribed schedule or frequency, resulting in irregular assessments. Independent or external audits are rarely employed.
- **Delayed Policy Updates (A.5.31):**
  Regulatory changes are identified, but not always integrated into the ISMS policies promptly. As a result, some policies lag behind current legal or regulatory expectations.
- **Resource Constraints:**
  The compliance team operates with limited staff and budget, making it challenging to schedule, conduct, and follow up on all required compliance activities consistently.

**Possible Documents to Provide as Evidence:**

1. **Compliance Audit Requirements (Doc-CAQ-001):**
   This document outlines what audits are required, their intended frequency, and the responsibilities for each type of audit. It establishes expectations that may not be fully met due to resource limitations.
2. **Compliance Audit Schedule (Doc-CA-001):**
   This schedule records the planned and most recent completion dates of annual, semi-annual (thematic), and quarterly audits. It shows that some audits are less frequent than prescribed, reflecting the irregular compliance checks mentioned above.
3. **Regulatory Mapping Document (Doc-RM-001):**
   This mapping identifies where regulatory requirements should be reflected in IBC's internal policies and notes intended update timelines. Reviewing this document may reveal that certain update deadlines have passed without corresponding policy revisions, indicating delayed policy updates.

**Hints for Students:**

- Compare the stated frequencies and requirements in **Doc-CAQ-001** to the actual scheduling and completion dates listed in **Doc-CA-001**. This may illustrate that IBC is not conducting audits as regularly as required.

- Examine **Doc-RM-001** to identify instances where a scheduled policy update related to a regulatory requirement was not completed on time. This can confirm the claim of delayed policy updates.
- Consider the impact of resource constraints on the CCO's ability to maintain a robust compliance posture. Limited staff and budget may explain why certain audits are missed and policy updates delayed, despite clear requirements and schedules.

# PROJECT MANAGER

**Context:**
You coordinate cross-departmental projects, including those with security implications. Relevant ISO 27001:2022 controls include Supplier Relationships and Incident Management.

**Key Points to Reveal:** - **Delayed Security Projects (A.8.32 Change Management):** Coordination issues lead to delays in patch implementations and other security measures. - **External Vendor Access (A.5.19 Information Security in Supplier Relationships):** Vendors are granted system access, but adherence to security rules is uncertain. - **Incident Policy Familiarity (A.5.26 Response to Information Security Incidents):** There is a lack of familiarity with incident handling procedures.

**Possible Documents to Provide:** - **Project Security Requirements Document (Doc-PSR-001):** Highlights that security tasks frequently slip from project timelines. - **Vendor Access Agreement (Doc-VA-001):** Demonstrates that vendor security requirements are not consistently verified.

# HR MANAGER

**Context:**
You manage employee records and system access provisioning. Relevant controls include Human Resource Security and Access Management, updated in ISO 27001:2022.

**Key Points to Reveal:** - **Access Rights Revocation (A.5.18 Access Rights):** Accounts remain active for days after an employee leaves. - **Training Delays (A.6.3 Information Security Awareness, Education and Training):** New hires must complete cybersecurity training within 30 days, but enforcement is lax. - **Role Changes (A.5.16 Identity Management):** There is no automated process for adjusting access rights when employees shift roles internally.

**Possible Documents to Provide:** - **User Termination Checklist (Doc-UT-001):** Demonstrates that account revocation steps are not always followed. - **Security Awareness Training Log (Doc-SAT-002):** Illustrates that employees often delay completing required training.