HEPro

📄 Assignment: Migration Planning from ISO 27001:2015 to ISO 27001:2022

Department Focus: Human Resources & Administration
Organization Type: Manufacturing (500 Employees)

---

1. Case Scenario

Your organization, **Alpha Manufacturing Ltd.**, currently complies with **ISO/IEC 27001:2015** standards for Information Security Management. As per the latest updates, ISO has released **ISO/IEC 27001:2022**, which introduces new controls and restructuring.

As the **HR & Admin Compliance Officer**, you are tasked with **developing a migration plan** for your department to align with the **2022 standard** within the next **12 months**.

The plan should cover:

- Comparison of clauses and Annex A controls in **2015 vs 2022 versions**.
- Specific **HR & Admin-related controls** (recruitment, access management, confidentiality, physical security, etc.).
- Step-by-step **migration roadmap**.
- Documentation and compliance tracking templates.

---

2. Comparison of Standards – ISO 27001:2015 vs 2022

Main Clauses (Management System Requirements)

Clause No.	ISO 27001:2015	ISO 27001:2022	Remarks
4	Context of the Organization	Context of the Organization	No major change
5	Leadership	Leadership	No major change
6	Planning	Planning	More emphasis on risk/opportunity management

Clause No.	ISO 27001:2015	ISO 27001:2022	Remarks
7	Support	Support	Same, but refined
8	Operation	Operation	Aligned
9	Performance Evaluation	Performance Evaluation	Strengthened KPIs, monitoring
10	Improvement	Improvement	No major change

Annex A – Controls (Detailed Differences)

ISO 27001:2015 Annex A

14 Domains, 114 Controls:

1. A.5 Information Security Policies
2. A.6 Organization of Information Security
3. A.7 Human Resource Security
4. A.8 Asset Management
5. A.9 Access Control
6. A.10 Cryptography
7. A.11 Physical & Environmental Security
8. A.12 Operations Security
9. A.13 Communications Security
10. A.14 System Acquisition, Development & Maintenance
11. A.15 Supplier Relationships
12. A.16 Information Security Incident Management
13. A.17 Business Continuity Management
14. A.18 Compliance

ISO 27001:2022 Annex A

4 Themes, 93 Controls (restructured + new controls):

1. **Organizational Controls (37)**
2. **People Controls (8)**
3. **Physical Controls (14)**
4. **Technological Controls (34)**

New Controls in 2022 relevant to HR & Admin include:

- Threat intelligence (A.5.7)
- Information security for use of cloud services (A.5.23)
- ICT readiness for business continuity (A.5.30)
- Physical security monitoring (A.7.4)
- Data masking (A.8.11)
- Data leakage prevention (A.8.12)
- Web filtering (A.8.23)
- Secure coding (A.8.28)

---

3. HR & Admin Focus Areas in Migration

HR Department (People Controls):

- Background verification during recruitment.
- Confidentiality agreements (NDAs).
- Access rights management on joining/exit.
- Regular ISMS awareness training.
- Disciplinary process for security breaches.

Admin Department (Physical Controls):

- Access card and visitor management system.
- CCTV and physical surveillance monitoring.

- Protection of physical records.
- Clean desk policy enforcement.
- Fire safety and disaster recovery preparedness.

---

4. Migration Roadmap

Phase 1: Gap Assessment (Months 1–2)

- Review **current HR/Admin policies** against new ISO 27001:2022 controls.
- Conduct **risk assessment** for people & physical security.
- Prepare a **gap analysis matrix**.

Phase 2: Policy & Control Update (Months 3–6)

- Update **HR onboarding/offboarding policies** to include stronger access control and NDAs.
- Revise **admin policies** for physical security monitoring and visitor logs.
- Implement **new awareness training modules** for employees.

Phase 3: Implementation (Months 7–10)

- Migrate from 2015 Annex A mapping → 2022 Annex A (93 controls).
- Align HR practices with **People Controls** (Annex A, 8 controls).
- Align Admin practices with **Physical Controls** (Annex A, 14 controls).
- Conduct internal audits on compliance.

Phase 4: Certification Prep (Months 11–12)

- Conduct **mock audit** and review corrective actions.
- Prepare final compliance documentation.
- Schedule audit with certification body.

---

5. Sample Migration Template (Gap Analysis for HR & Admin)

Control Reference (2015)	Control Reference (2022)	Current HR/Admin Practice	Gap Identified	Action Required
A.7.1.1 Screening	A.6.1 Background Verification	Basic reference check	No structured screening policy	Implement detailed verification checklist
A.7.2.2 Information Security Awareness	A.6.3 Awareness, Education & Training	One-time induction	No refresher trainings	Quarterly security awareness workshops
A.9.2.1 User Access Management	A.5.18 Access Rights	Email access removed on exit	Physical access not revoked timely	Create exit checklist including access removal
A.11.1.1 Physical Security Perimeter	A.7.1 Physical Security Perimeter	Factory has guards	No CCTV monitoring policy	Add surveillance monitoring policy
A.18.1.4 Privacy & Protection of PII	A.5.34 Data Protection & Privacy	HR maintains employee files	Not aligned to GDPR-like standards	Introduce data retention & masking policy

---

6. Expected Outcomes

- Complete migration of **HR & Admin policies** from ISO 27001:2015 → ISO 27001:2022.
- HR processes aligned with **People Controls** (training, screening, NDAs, awareness).
- Admin processes aligned with **Physical Controls** (access, monitoring, visitor management).
- Compliance readiness for external certification audit.
- Improved employee awareness & reduced information security risk.

---

7. Assignment Submission Guidelines

Report Format:

1. Cover Page – Assignment Title, Name, Batch, Date
2. Executive Summary – Migration Objective
3. Overview of ISO 27001:2015 vs 2022 (with clause/control comparison tables)
4. HR & Admin Gap Analysis Matrix (Template-based)
5. Migration Roadmap (Phased plan)
6. Policy Alignment Samples (Leave/Access Control/Visitor Management)
7. Expected Outcomes
8. Annexures – Gap checklist, audit templates

File Type: PDF or Word
Length: 12–15 pages
Font: Times New Roman, Size 12, 1.5 Line Spacing
Deadline: [Insert Date]

📄 Assignment: Migration Planning – ISO 27001:2015 to ISO 27001:2022

Context

Your organization, a **manufacturing company with 500 employees**, is currently certified under **ISO 27001:2015**. With the release of **ISO 27001:2022**, the HR and Administration department must align their policies, processes, and compliance frameworks with the updated requirements to ensure successful migration during the recertification cycle.

Part 1 – Comparison of Clauses (2015 vs 2022)

ISO 27001:2015 Structure

- **Clause 4**: Context of the organization
- **Clause 5**: Leadership
- **Clause 6**: Planning
- **Clause 7**: Support
- **Clause 8**: Operation

- **Clause 9**: Performance evaluation
- **Clause 10**: Improvement
- **Annex A**: 114 controls grouped into 14 categories

ISO 27001:2022 Structure

- **Clauses 4–10** remain the same (minor editorial changes).
- **Annex A** controls reduced from **114 to 93**, restructured into **4 main themes**:
    1. **Organizational (37 controls)**
    2. **People (8 controls)**
    3. **Physical (14 controls)**
    4. **Technological (34 controls)**
- New/updated controls relevant for **HR & Admin**:
    - Threat intelligence
    - Information security for cloud services
    - ICT readiness for business continuity
    - Physical security monitoring
    - Data masking & data leakage prevention
    - Secure coding awareness & skills (linked with HR training policies)

Part 2 – Migration Plan for HR & Admin Department

Step 1: Gap Analysis

- Map existing **HR & Admin policies** under ISO 27001:2015 to the new 2022 controls.
- Identify gaps, especially in **cloud security, data privacy, remote work, and workforce awareness**.

Step 2: Stakeholder Engagement

- Form an **HR-Admin ISMS Migration Team**.

- Roles:
    - **HR Head** – Policy alignment & employee awareness
    - **Admin Head** – Physical security & monitoring compliance
    - **IT Security Lead** – Coordination with HR for training & access control
    - **Legal/Compliance Officer** – Regulatory compliance (labor laws, data protection laws like GDPR/DPDP Act)

Step 3: Policy & Process Updates

- Update **HR policies**:
    - Employee onboarding & exit checklists → include info-security clauses.
    - Remote work policy → include monitoring & access controls.
    - Training & awareness → mandatory ISO 27001:2022 awareness for all staff.
- Update **Admin policies**:
    - Physical security controls → surveillance, access monitoring, visitor logs.
    - Business continuity planning (BCP) → include ICT readiness.

Step 4: Training & Awareness

- HR to create **role-based training**:
    - **General employees**: Data privacy, phishing awareness, AI/bot security.
    - **HR team**: Data masking, personal information handling, regulatory compliance.
    - **Admin team**: Physical monitoring, ICT business continuity readiness.

Step 5: Implementation Roadmap

- **Month 1–2**: Gap analysis & stakeholder meetings
- **Month 3–5**: Update HR & Admin policies, draft new SOPs
- **Month 6–8**: Awareness training, pilot implementation
- **Month 9–10**: Internal audit of HR & Admin practices under ISO 27001:2022
- **Month 11–12**: External certification audit readiness

Part 3 – Sample Policy & Process Alignment Templates

Template 1 – Policy Alignment (HR Example)

Policy Area	ISO 27001:2015 Reference	ISO 27001:2022 Updated Control	Required Action
Employee Onboarding	A.7.1.2 (Terms & conditions of employment)	A.6.3 (Information security in project management)	Add confidentiality & info-security clauses to contracts
Remote Work Policy	A.9.2.3 (Management of privileged access rights)	A.5.23 (Information security for use of cloud services)	Create remote access guidelines & monitoring
Employee Training	A.7.2.2 (Information security awareness, education, and training)	A.6.3 (Skills & awareness)	Introduce annual refresher + phishing simulation training

---

Template 2 – Process Alignment (Admin Example)

Process Area	Current Practice (2015)	Updated Requirement (2022)	Migration Action
Physical Access	Manual visitor log	A.7.4 (Physical security monitoring)	Install CCTV, automate visitor access system
BCP	Paper-based checklist	A.5.29 (ICT readiness for business continuity)	Implement digital backup & resilience planning
Asset Disposal	Physical record shredding	A.8.10 (Information deletion)	Secure data deletion protocols for IT assets

---

Part 4 – Expected Outcomes

1. **Aligned HR & Admin policies** with ISO 27001:2022 requirements.
2. **Increased employee awareness** of information security risks.
3. **Improved physical and ICT readiness** for business continuity.

4. **Successful internal audit** showcasing HR & Admin compliance.
5. **External certification readiness** within the 12-month migration timeline.

✅ **Assignment Deliverable (Project Submission Guidelines):**

- Word/PDF Report (15–20 pages) covering:
    1. Gap Analysis Report (2015 vs 2022) for HR & Admin.
    2. Updated Policy Drafts.
    3. Training & Awareness Plan.
    4. Implementation Roadmap.
    5. Audit & Monitoring Plan.