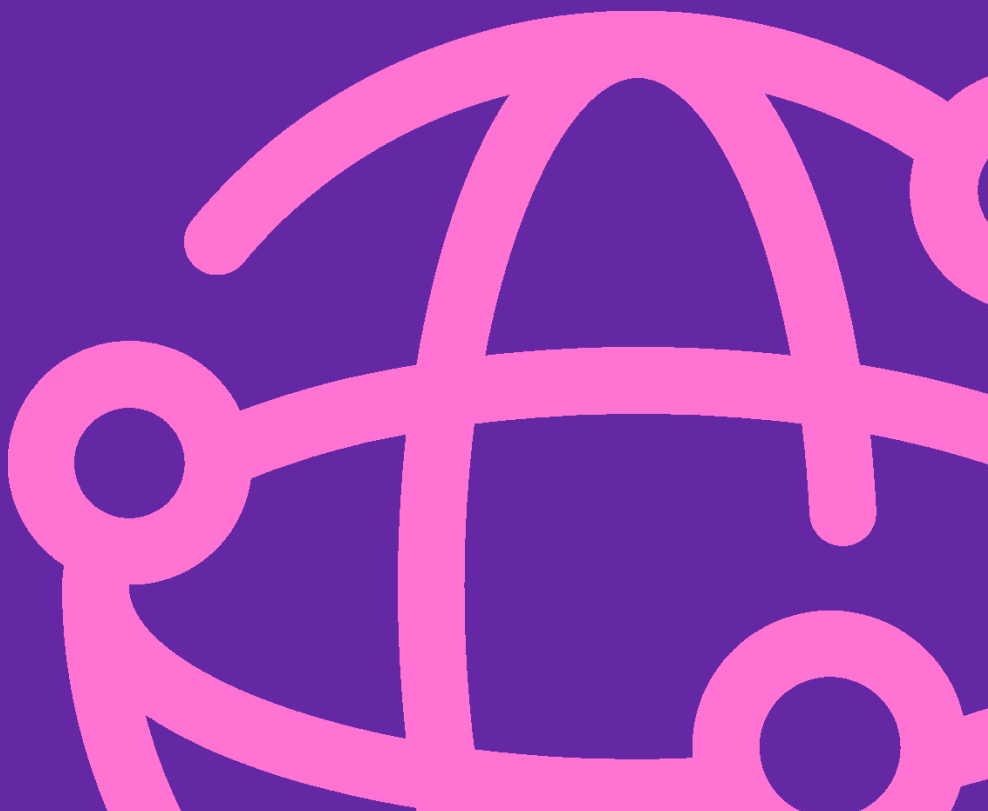
Deviceology

The Market Access People



Audit Briefing for a Resource Lead

Audit Type: ISO/IEC 27001:2022 including human resources security lifecycle (recruitment to termination), awareness, training, access control, and disciplinary procedures.

Objective: Verify effective security control through human resources lifecycle (recruitment to termination) including security awareness, training, access control, and disciplinary procedures.

Your Role & Accountability

As Resource Lead, you are responsible for enforcing personnel-related security controls including background checks, confidentiality agreements, role-specific security clauses in employment contracts, security training logs, awareness initiatives, and ongoing refreshers, records of disciplinary actions related to security policy breaches, competency and performance management framework.

Key Evidence Auditors Will Expect

- Signed employment contracts with explicit information security responsibilities
- Background screening results and onboarding security checklists
- Training completion logs for all employees, contractors, and temps
- Exit procedures, including access revocation and asset return logs

Audit Readiness Advice

Make sure training and onboarding records are complete, traceable, and signed.

Be ready to walk through an example of an employee onboarding and offboarding.

Every workflow and policy must be backed by logs or documented outputs

Avoid abstract or off the cuff responses — show proof from source systems and dev tooling.

Prepare examples of controls and processes working effectively in advance of the audit

ISO27001 Internal Audit Questions

Resourcing

These questions can be used to conduct a mock audit or assess readiness for a conformity assessment. Failure to provide a satisfactory response indicates a potential non-compliance.

Questions

- [ ] Submit documented procedures for screening new hires, including evidence of background checks conducted.
- [ ] Provide signed employment agreements including confidentiality clauses and information security responsibilities.
- [ ] Show how job descriptions include role-specific security obligations and are approved by HR and management.
- [ ] Show onboarding checklists and security induction training completion records.
- [ ] Provide training logs and results for ISMS awareness programmes across all departments.
- [ ] Submit proof of security briefings for high-privilege roles and signing of acceptable use terms.
- [ ] Show documented linkage between job termination and system deprovisioning procedures.
- [ ] Submit the disciplinary procedure for ISMS breaches and examples of enforcement.
- [ ] Submit examples showing HR's role in initiating the offboarding process securely.
- [ ] Provide HR records confirming communication of post-employment confidentiality obligations.
- [ ] Submit documented procedures for screening new hires, including evidence of background checks conducted.
- [ ] Provide signed employment agreements including confidentiality clauses and information security responsibilities.

Supplementary Higher Scrutiny Questions

- Submit examples of onboarding training specific to privileged access roles.
- Submit evidence of contractor or third-party HR due diligence, including confidentiality and onboarding controls.
- Provide documentation showing approval processes for contractor access to systems or premises.
- Submit logs of phishing or awareness campaign metrics and improvement tracking.
- Demonstrate escalation records involving HR, management, and ISMS leads.
- Show audit logs of user account removal with timestamps aligned to departure dates.

ISO27001 Annex A Development Controls

This is a summary of select information security control objectives of particular note to resource management.

Ref	Type of Control	Control and Purpose	Purpose
A 6.1	Preventive	**Screening** Background verification checks on all candidates to become personnel should be carried out prior to joining the organisation and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	To ensure we have checked people to an appropriate level before they get access to our data and information. It is proportionate to risk and done in the framework of applicable laws but the purpose is to reduce risk by making sure that people are who they say they are, can do the things they say they can do and don't have any indicators they will do something to compromise the CIA of our Information Assets.
A 6.2	Preventive	**Terms of Employment** The employment contractual agreements should state the personnel's and the organisations responsibilities for information security.	To control that employees are fully aware of their information security responsibilities in relation to their role.
A 6.3	Preventive	**Information Security Awareness, Education and Training** Personnel of the organisation and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organisations information security policy, topic-specific policies and procedures, as relevant for their job function.	To ensure that people are aware of their responsibilities for information security and that they meet them.
A 6.4	Preventive, Corrective	**Disciplinary Process** A disciplinary process should be formalised and communicated to take actions against personnel and other relevant interested	To ensure that people understand what will happen, and the consequences of a violation of information security policy. The intent is to deter people from not following

		parties who have committed an information security policy violation.	and adhering to policies and appropriately deal with those that do.
A 6.5	Preventive	**Responsibilities After Termination or Change of Employment** Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.	To ensure that you are protecting the organisation even after someone leaves.
A 6.6	Preventive	**Confidentiality or Non-Disclosure Agreements** Confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	To ensure you maintain confidentiality for information that is accessed by people, external parties and suppliers.
A 6.7	Preventive	**Remote Working** Security measure should be implemented when personnel are working remotely to protect information accessed, processed or stored outside of the organizations premises.	To ensure the security of information when personnel are working remotely.
A 6.8	Detective	**Information security event reporting** The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	To support timely, consistent and effective reporting of information security events that can be identified by personnel.