scaut

The standards

Are your hiring practices meeting today's standards?

As geopolitical tensions increase and threats to strategic resources, critical infrastructure and national security become more prevalent, many organizations are required by law to meet mandated security requirements.

Are you on this list?

- **Energy**
  Electricity, oil, gas, and hydrogen.
- **Transport**
- **Banking and financial markets**
- **Healthcare**
- **Drinking and waste water**
- **Digital infrastructure**
- **Digital services**
  Search engines, online markets, and social networks.
- **Space**
- **Postal and courier services**
- **Waste management**
- **Chemicals**
- **Food**
  Production, processing, and distribution.
- **Manufacturing**
  Medical, computer, and transport equipment.
- **Military & Defense**

Secure workforce supply chain

Making sure your contractor and fully remote workers are thoroughly screened can be critical when it comes to ensuring you are compliant.

Remote workers and contractors often have extensive access to physical and digital resources that could be compromised if the wrong people are given freedom to operate.

Standards compliance will be more demanding in the future as governments pivot to address rising global tensions, and your workforce must be secured.

Standards: 2025 and beyond

Standards and Directives	What is expected of you?
NIS2 Coming into effect on January 16, 2023, the NIS2 Directive is a continuation of the EU cybersecurity directive, NIS. Member States have until October 17, 2024 to transpose the Directive into national law. This means that affected organizations will be legally obligated to meet its requirements by Q4 2024.	• Regularly conduct security clearance checks to verify the expertise, reliability, and integrity of employees working with sensitive information and technologies. • Establish risk management measures. • Establish mechanisms for managing cybersecurity incidents. • Address cybersecurity risks in the supply chain (including third-party service providers) . • Adhere to national supervision and reporting requirements.
CER The **Critical Entities Resilience Directive** lays down obligations on EU Member States to take specific measures, to ensure that essential services for the maintenance of vital societal functions or economic activities are provided in an unobstructed manner in the internal market.	• Implement employee screening process, verify expertise, reliability, and integrity for those accessing critical infrastructure. Identity and criminal checks are a minimum standard. • Establish and maintain a tailored risk management framework. • Implement procedures for incident reporting and crisis management. • Regularly test and audit the effectiveness of security measures and resilience strategies.
DORA The Digital Operational Resilience Act (DORA) is an EU regulation strengthening the financial sector's digital resilience. It sets clear standards for financial firms and third-party providers to manage technology risks—including governance, incident reporting, and testing—to ensure continuous operations, even under severe disruptions.	• DORA demands strong governance, including verifying staff suitability. Background checks confirm credentials and integrity. • Thorough screening will deter insider threats and reduce operational risk. • Vetting external partners aligns with DORA's supplier requirements, minimizing external vulnerabilities. • Documenting screening processes demonstrate consistent risk management to regulators. • Regular re-screening detects potential issues early, strengthening operational continuity.
SOC 2 SOC 2 is a voluntary compliance standard for service organizations, developed by the American Institute of CPAs (AICPA), which specifies how organizations should manage customer data.	• Implement thorough employee screening processes to ensure expertise, reliability, and integrity for individuals handling sensitive data. • Develop and maintain policies and procedures that govern the operation of services. • Conduct risk assessments to identify potential threats. • Regularly monitor and audit controls for effectiveness. • Ensure that information related to the controls is communicated.
ISO 27001 ISO 27001 is an international standard for Information Security Management Systems (ISMS). It provides a framework for establishing, implementing, maintaining, and continually improving an organization's information security management system. Its aim is to protect sensitive information from threats such as hackers and malware through policies, procedures, and controls.	• As per Control 6.1, companies must establish a screening process that vets all full-time, part-time and casual/temporary staff and suppliers, to ensure that only fit and proper personnel are able to access information. • Implement an Information Security Management System (ISMS) tailored to the risks. • Conduct comprehensive risk assessments and implement controls to mitigate these risks. • Apply the Plan-Do-Check-Act (PDCA) cycle to ensure continuous improvement of the ISMS • Educate employees about their roles in the ISMS.