# Human Resources Security Management towards ISO/IEC 27001:2005 accreditation of an Information Security Management System

Professor PhD. **Constantin MILITARU**
Polytechnic University of Bucharest, Romania
PhD Student **Daniel COSTIN**
Polytechnic University of Bucharest, Romania

**ABSTRACT**

*Currently, ISO/IEC 27001:2005 is the formal specification standard for Information Security Management System (ISMS), against which organizations may seek certification. This International Standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's ISMS. The "Human Resources Security" main clause deals with all three phases of employment: prior, during, and post-employment. There are critical information security controls and safeguards within each of these three elements. This clause helps management evaluate and deploy important controls within these three dimensions of the employment life cycle. People will always be an organization's greatest asset and its greatest risk.*

**KEYWORDS:** *ISO/IEC 27001; ISMS; Screening; Security Control; Security Policy.*

The ISO/IEC 27001:2005 Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving formalized **information security management systems** (ISMS) within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. This International Standard is universal for all types of organizations.

Benefits of pursuing certification to ISO/IEC 27001:2005 include:

- Certification allows organizations to mitigate the risk of information security breaches;
- Certification allows organizations to mitigate the impact of information security breaches when they do occur;
- In the event of a security breach, certification should reduce the penalty imposed by regulators, since the organization's security and record-handling procedures will be seen as following internationally accepted best practices;
- Certification allows organizations to demonstrate due diligence and due care to shareholders, customers and business partners, through strategic thinking;
- Certification allows organizations to demonstrate proactive compliance to legal, regulatory and contractual requirements;
- Certification provides independent third-party validation of an organization's ISMS;
- ISO/IEC 27001 is the most comprehensive information security management certification that is internationally accepted.

The ISO/IEC 27001:2005 Standard contains 11 security control clauses, illustrated in figure 1. Each clause contains a number of main security categories. Depending on the circumstances, all clauses could be important; each organization applying this standard should identify applicable clauses to the individual business processes.

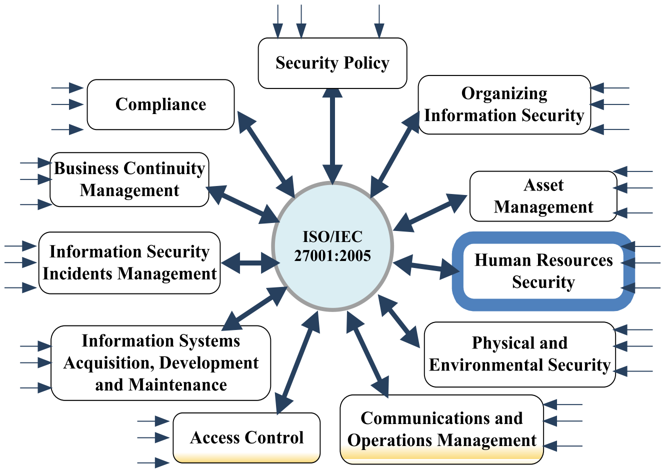
Security Policy
Compliance
Organizing Information Security
Business Continuity Management
Asset Management
ISO/IEC 27001:2005
Information Security Incidents Management
Human Resources Security
Information Systems Acquisition, Development and Maintenance
Physical and Environmental Security
Access Control
Communications and Operations Management

**Figure 1 The 11 security control clauses of the ISO/IEC 27001:2005 Standard**

The "Human Resources Security" main clause deals with all three phases of employment: prior, during, and post, as illustrated in Figure 2. There are critical information security controls and safeguards within each of these three elements. This clause helps management evaluate and deploy important controls within these three dimensions of the employment life cycle. People will always be an organization's greatest asset and its greatest risk.

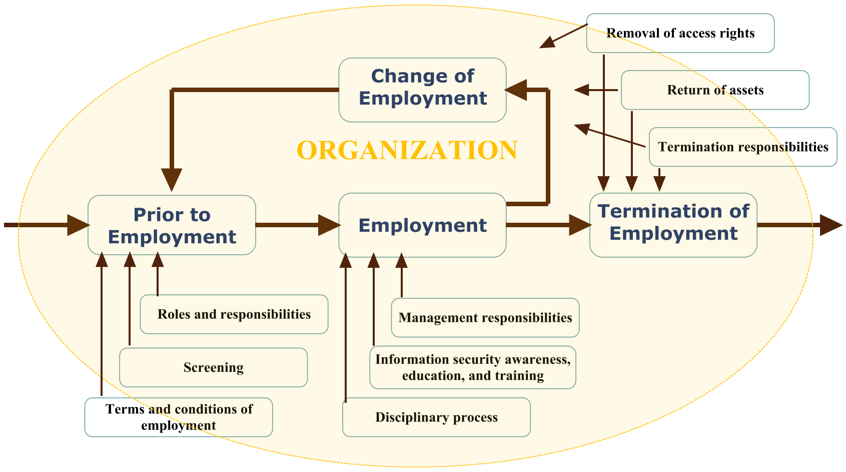
Removal of access rights
Change of Employment
Return of assets
ORGANIZATION
Termination responsibilities
Prior to Employment
Employment
Termination of Employment
Roles and responsibilities
Management responsibilities
Screening
Information security awareness, education, and training
Terms and conditions of employment
Disciplinary process

**Figure2 Employment Life Cycle in the organization**

The "**PRIOR TO EMPLOYMENT"** control objective is focused on ensuring that all relevant parties, including employees, consultants, contractors, and third-party users, understand their role and responsibility to information security. Furthermore, measures should be taken on the part of management and human resources to reduce some of the most common threats by properly screening and educating all users of the organization's information systems and resources.

**Security roles and responsibilities** should be defined and clearly communicated to job candidates during the pre-employment process.

Job descriptions can be used to document security roles and responsibilities. Every job description should contain:

1) a description of the competencies required for the role; and

2) a statement that every employee is required to be aware of the organization's policy on information security: the responsibility to protect assets from unauthorized access, disclosure, modification, destruction or interference, the information classification and handling rules, the access controls (both physical and logical), the incident reporting procedure, the requirements to carry out any other specific procedures and processes, the requirement to improve his competence and skills in this area, and the fact that the employee will be held accountable for his acts.

The "**screening**" control stipulates that all candidates for employment, consultants, contractors, and third-party users should undergo a background check that is proportional to their position and the risk they pose to the organization. Background checks should be in alignment with any applicable laws or regulations and to meet all specific business requirements. These verification checks should include the following:

a) availability of satisfactory character references, at least one business and one personal;

b) A completeness and accuracy check of the employee's curriculum vitae; this is usually carried out by means of written references supplied by previous employers

c) confirmation of claimed academic and professional qualifications, either by means of obtaining from the candidate copies of the certificates or other statement of qualification or through an independent CV checking service;

d) independent identity check (ID, passport or similar document);

Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities, and in particular if these are handling sensitive information, financial information or highly confidential information, the organization should also consider further, more detailed checks such as checks of criminal records or credit checks.

A screening process should also be carried out for contractors, and third party users. If contractors are provided through an agency, then the contract with the agency should clearly specify the agency's responsibilities for screening and the notification procedures.

The control "**Terms and conditions of employment**" of the standard ISO/IEC 27001:2005 requires the organization to ensure that employees, contractors and third parties all agree and sign an employment contract that contains terms and conditions covering their and the organization's responsibilities for information security. These terms and conditions should include a confidentiality or non-disclosure agreement, constructed in accordance with local legal guidance, that covers information acquired prior to and during the employment. This confidentiality agreement should be drafted by the organization's lawyers. It should form an integral part of the contract of employment, so that acceptance of terms of employment automatically includes acceptance of the confidentiality agreement.

In the event an employee disregards the information security policy and requirements, the actions taken by the company should be included in this agreement.

Responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment.

A code of conduct may be used to cover the employee's, contractor's or third party user's responsibilities regarding confidentiality, data protection, ethics, appropriate use of the organization's equipment and facilities, as well as reputable practices expected by the organization.

The “**DURING EMPLOYMENT”** control objective of the standard ISO/IEC 27001:2005 requires the organization to ensure that its employees, contractors and third-party users are aware of information security threats as well as their responsibilities and liabilities, and that it has trained its personnel appropriately.

The objective is simply to ensure that all users of the organization’s information assets are aware of information security threats and are competent and adequately equipped to perform the requested tasks and to support the organization’s information security policy in their work.

**Management has a responsibility** to the organization to document and publish information security policies, procedures, and guidelines to protect the organization and employees. The policy should clearly describe the requirement for all parties, internal or external, to follow and adhere to the published policies, procedures, and guidelines.

The ISO/IEC 27002:2005’s guidance on this control includes ensuring that staff (employees, contractors, third parties):

- are *properly briefed* on their information security roles and responsibilities prior to being granted access to sensitive information or information systems;
- are provided with *guidelines* to state security expectations of their role within the organization;
- are *motivated* to fulfill the security policies of the organization;
- achieve a level of *awareness* on security relevant to their roles and responsibilities within the organization;
- *conform* to the terms and conditions of employment, which includes the organization’s information security policy and appropriate methods of working;
- continue to have the appropriate *skills and qualifications*.

If employees, contractors and third party users are not made aware of their security responsibilities, they can cause considerable damage to an organization. Motivated personnel are likely to be more reliable and cause less information security incidents. Also, poor management may cause personnel to feel undervalued resulting in a negative security impact to the organization.

The control “**Information security awareness, education, and training”** follows on from the previous control. All users of the organization’s information processing facilities should receive information security awareness, education, or training that is specifically targeted for their role and function within the organization and regular updates in organizational policies and procedures, as relevant for their job function.

A cohesive **information security awareness policy**, tailored to the organizational culture, gives the SMSI credibility and visibility. It shows that management recognizes that security is important and that individuals will be held accountable for their actions.

An awareness policy should address three basic concepts:

1. Participation in the awareness program is required for everyone, including senior management, part-time and full-time staff, new hires, contractors, or other outsiders who have access to the organization’s information systems. For example, new hires might be required to receive an information security awareness briefing within a specific time frame (e.g., 30 days after hire) or before being allowed system access. Existing employees might be required to attend an awareness activity or take a course within one month of program initiation and periodically thereafter (e.g., quarterly or annually). Existing employees might also be required to refresh their security awareness when the organization’s IT environment changes significantly.

2. Everyone will be given sufficient time to participate in awareness activities. In many organizations, security policy also requires that employees sign a statement indicating that they understand the material presented and will comply with security policies.

3. Responsibility for conducting awareness program activities is assigned. The program might be created and implemented by one or a combination of the following: the training department; the security staff; or an outside organization, consultant, or security awareness specialist.

The "**Disciplinary process**" control of the standard requires the organization to deal with employee (and contractor and third-party) violations of its information security policy and procedures through a formal disciplinary process.

No disciplinary process can start until the existence of a security breach has been verified.

The formal disciplinary process should ensure correct and fair treatment for employees who are suspected of committing breaches of security and should provide for a graduated response considering the following factors:

- nature and gravity of the breach and its impact on business,
- whether or not this is a first or repeat offence,
- whether or not the violator was properly trained,
- relevant legislation,
- business contracts.

The disciplinary process should also be used as a deterrent to prevent employees, contractors and third party users in violating organizational security policies and procedures, and any other security breaches.

The "**TERMINATION OR CHANGE OF EMPLOYMENT"** control objective is to ensure that internal and external parties (employees, consultants, contractors, third-party users, etc.) end or change employment status in a secure manner, with the return of all equipment and removal of all access rights.

The control deals with termination responsibilities and simply requires the organization to document clearly who is responsible for performing terminations and what these responsibilities are. These responsibilities should clearly include dealing with the ongoing clauses in the contract of employment. Usually, the Human Resources department (together with the supervising manager of the person leaving) will be responsible for ensuring that all the termination aspects of an employment contract have been dealt with and these may be standard aspects of a termination interview, which is carried out in a standard way, using a standard checklist.

The control "**Return of assets**" requires all employees, third parties and contractors to return all organizational assets upon termination. These assets fall into four categories: software, hardware, information and knowledge. Other organizational assets such as mobile computing devices, credit cards, access cards, software, manuals, and information stored on electronic media also need to be returned. In cases where an employee uses their own personal equipment, procedures should be followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment.

In cases where an employee, contractor or third party user has knowledge that is important to ongoing operations, that information should be documented and transferred to the organization. Unless this step is taken, the knowledge (particularly if the emplyee is being unwillingly terminated) will leave the company with the employee. It is recommended for organizations to delay commencing termination procedures with employees until the employees have successfully transferred their knowledge.

"**Removal of access rights**" control states that the access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.

The organization needs a clear documented procedure to ensure that upon termination, an employee's access rights are also terminated. Similarly, any change in employment should also lead to a review and adjustment of existing access rights.

The access rights that should be removed or adapted include physical and logical access, tokens, keys, identification cards, information processing facilities, e-mail and internet user accounts, subscriptions, and removal from any documentation that identifies them as a current member of the organization.

Access rights for information assets and information processing facilities should be reduced or removed before the employment terminates or changes, depending on the evaluation of risk factors such as:

a) whether the termination or change is initiated by the employee, contractor or third party user, or by management and the reason of termination;

b) the current responsibilities of the employee, contractor or any other user;

c) the value of the assets currently accessible.

In cases of management-initiated termination, disgruntled employees, contractors or third party users may deliberately corrupt information or sabotage information processing facilities. In cases of persons resigning, they may be tempted to collect information for future use.

## Conclusion

The concept of "Human Resources Security" is a critical part of the overall information security posture for every organization. People are central to the success of virtually every organization, and they also pose many risks. Prior to employment, users must be made aware of their roles and responsibilities for information security. Management must take the appropriate steps and screen employees and external employees before hiring or engaging them as authorized users of organizational resources and assets. To uphold the integrity of the information security policy in the event of employee or external party abuse, management should require all parties to sign a terms and conditions agreement.

During the employment or engagement phase of the relationship, management has the responsibility to make users aware of their information security responsibilities and provide appropriate awareness, education, and training specifically targeted at their role within the organization. In the event that an employee or external party refuses to follow the published information security policy, management should document, publish, and communicate a formal disciplinary process.

When an employee or external party either terminates or changes their responsibility, management must have a documented and clear process for this transition as it relates to information security matters. All users must be required to return all assets in their possession, and all logical and physical rights should be terminated immediately.

## REFERENCES

1. ISO/IEC 27001:2005 Information technology - Security techniques - Information Security Management Systems - Requirements
2. ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management
3. Bidgoli, Hossein: *Handbook of Information Security*, Volume 3, Published by John Wiley & Sons, Inc., Hoboken, New Jersey. 2006
4. Coyne, Edward J.; Davis, John: *Role Engineering for Enterprise Security Management.* Artech House, Inc., 2008
5. Khadraoui, Djamel; *Francine, Herrmann: Advances in Enterprise Information Technology Security Information*, Science Reference (IGI Global), New York 2007
6. Subramanian, Ramesh: "Computer Security, Privacy and Politics": Current Issues, *Challenges and Solutions.* IRM Press, New York, 2008