**Appendix 3 – Internal Audit Checklist for ISO 27001 and ISO 22301**

# Internal audit checklist for ISO 27001

|  |  |  |  |
| --- | --- | --- | --- |
| Clause | Requirement of the standard | Compliant Yes/No | Evidence |
| 4.2 | Did the organization determine interested parties? |  |  |
| 4.2 | Does the list of all of interested parties’ requirements exist? |  |  |
| 4.3 | Is the scope documented with clearly defined boundaries and interfaces? |  |  |
| 5.1 | Are the general ISMS objectives compatible with the strategic direction? |  |  |
| 5.1 | Does management ensure that ISMS achieves its objectives? |  |  |
| 5.2 | Does Information Security Policy exist with objectives or framework for setting objectives? |  |  |
| 5.2 | Is Information Security Policy communicated within the company? |  |  |
| 5.3 | Are roles and responsibilities for information security assigned and communicated? |  |  |
| 6.1.2 | Is the risk assessment process documented, including the risk acceptance criteria and criteria for risk assessment? |  |  |
| 6.1.2, 8.2 | Are the risks identified, their owners, likelihood, consequences, and the level of risk; are these results documented? |  |  |
| 6.1.3 | Is the risk treatment process documented, including the risk treatment options? |  |  |
| 6.1.3, 8.3 | Are all the unacceptable risks treated using the options and controls from Annex A; are these results documented? |  |  |
| 6.1.3 | Is Statement of Applicability produced with justifications and status for each control? |  |  |
| 6.1.3, 8.3 | Does Risk treatment plan exist, approved by risk owners? |  |  |
| 6.2 | Does Risk treatment plan define who is responsible for implementation of which control, with which resources, what are the deadlines, and what is the evaluation method? |  |  |
| 7.1 | Are adequate resources provided for all the elements of ISMS? |  |  |
| 7.2 | Are required competences defined, trainings performed, and records of competences maintained? |  |  |
| 7.3 | Is the personnel aware of Information security policy, of their role, and consequences of not complying with the rules? |  |  |
| 7.4 | Does the process for communication related to information security exist, including the responsibilities and what to communicate? |  |  |
| 7.5 | Does the process for managing documents and records exist, including who reviews and approves documents, where and how they are published, stored and protected? |  |  |
| 7.5 | Are documents of external origin controlled? |  |  |
| 8.1 | Are outsourced processes identified and controlled? |  |  |
| 9.1 | Is it defined what needs to be measured, by which method, who is responsible, who will analyze and evaluate the results? |  |  |
| 9.1 | Are the results of measurement documented and reported to responsible persons? |  |  |
| 9.2 | Does an audit program exist that defines the timing, responsibilities, reporting, audit criteria and scope? |  |  |
| 9.2 | Are internal audits performed according to audit program, results reported through the Internal audit report and relevant corrective actions raised? |  |  |
| 9.3 | Is management review regularly performed, and are the results documented in minutes of the meeting? |  |  |
| 9.3 | Did management decide on all the crucial issues important for the success of the ISMS? |  |  |
| 10.1 | Does the organization react to every nonconformity? |  |  |
| 10.1 | Does the organization consider eliminating the cause of nonconformity and, where appropriate, take corrective action? |  |  |
| 10.1 | Are all nonconformities recorded, together with corrective actions? |  |  |
| A.5.1.1 | Are all necessary information security policies approved by management and published? |  |  |
| A.5.1.2 | Are all information security policies reviewed and updated? |  |  |
| A.6.1.1 | Are all information security responsibilities clearly defined through one or several documents? |  |  |
| A.6.1.2 | Are duties and responsibilities defined in such a way to avoid conflict of interest, particularly with the information and systems where high risks are involved? |  |  |
| A.6.1.3 | Is it clearly defined who should be in contact with which authorities? |  |  |
| A.6.1.4 | Is it clearly defined who should be in contact with special interest groups or professional associations? |  |  |
| A.6.1.5 | Are information security rules included in every project? |  |  |
| A.6.2.1 | Are there rules for secure handling of mobile devices? |  |  |
| A.6.2.2 | Are there rules defining how the company information is protected at teleworking sites? |  |  |
| A.7.1.1 | Are background checks performed on candidates for employment or for contractors? |  |  |
| A.7.1.2 | Do the agreements with employees and contractors specify the information security responsibilities? |  |  |
| A.7.2.1 | Is management actively requiring all employees and contractors to comply with information security rules? |  |  |
| A.7.2.2 | Are all relevant employees and contractors being trained to perform their security duties, and do the awareness programs exist? |  |  |
| A.7.2.3 | Have all employees who have committed a security breach been subject to a formal disciplinary process? |  |  |
| A.7.3.1 | Are information security responsibilities that remain valid after the termination of employment defined in the agreement? |  |  |
| A.8.1.1 | Is an Inventory of assets drawn up? |  |  |
| A.8.1.2 | Does every asset in Inventory of assets have a designated owner? |  |  |
| A.8.1.3 | Are the rules for appropriate handling of information and assets documented? |  |  |
| A.8.1.4 | Did all the employees and contractors return all the company assets when their employment was terminated? |  |  |
| A.8.2.1 | Is the information classified according to specified criteria? |  |  |
| A.8.2.2 | Is the classified information labeled according to the defined procedures? |  |  |
| A.8.2.3 | Are there procedures which define how to handle classified information? |  |  |
| A.8.3.1 | Are there the procedures which define how to handle removable media in line with the classification rules? |  |  |
| A.8.3.2 | Are there formal procedures for disposing of the media? |  |  |
| A.8.3.3 | Is the media that contains sensitive information protected during transportation? |  |  |
| A.9.1.1 | Is there an Access control policy which defines business and security requirements for access control? |  |  |
| A.9.1.2 | Do the users have access only to those networks and services they are specifically authorized for? |  |  |
| A.9.2.1 | Are access rights provided via a formal registration process? |  |  |
| A.9.2.2 | Is there a formal access control system when logging into information systems? |  |  |
| A.9.2.3 | Are privileged access rights managed with special care? |  |  |
| A.9.2.4 | Are initial passwords and other secret authentication information provided in a secure way? |  |  |
| A.9.2.5 | Do asset owners periodically check all the privileged access rights? |  |  |
| A.9.2.6 | Have the access rights to all employees and contractors been removed upon the termination of their contracts? |  |  |
| A.9.3.1 | Are there clear rules for users on how to protect passwords and other authentication information? |  |  |
| A.9.4.1 | Is the access to databases and applications restricted according to the Access control policy? |  |  |
| A.9.4.2 | Is secure log-on required on systems according to the Access control policy? |  |  |
| A.9.4.3 | Are the systems that manage passwords interactive, and enable the creation of secure passwords? |  |  |
| A.9.4.4 | Is the use of utility tools that can override the security controls of applications and systems strictly controlled and limited to narrow circle of employees? |  |  |
| A.9.4.5 | Is the access to source code restricted to authorized persons? |  |  |
| A.10.1.1 | Does the policy that regulates encryption and other cryptographic controls exist? |  |  |
| A.10.1.2 | Are the cryptographic keys properly protected? |  |  |
| A.11.1.1 | Do secure areas that protect sensitive information exist? |  |  |
| A.11.1.2 | Is the entrance to secure areas protected with controls that allow only the authorized persons to enter? |  |  |
| A.11.1.3 | Are secure areas located in such a way that they are not visible to outsiders, and not easily reached from the outside? |  |  |
| A.11.1.4 | Are the alarms, fire-protection, and other systems installed? |  |  |
| A.11.1.5 | Are working procedures for secure areas defined and complied with? |  |  |
| A.11.1.6 | Are delivery and loading areas controlled in such a way that unauthorized persons cannot enter the company premises? |  |  |
| A.11.2.1 | Is the equipment sited in such a way to protect it from unauthorized access, and from environmental threats? |  |  |
| A.11.2.2 | Does the equipment have an uninterruptible power supply? |  |  |
| A.11.2.3 | Are the power and telecommunication cables adequately protected? |  |  |
| A.11.2.4 | Is the equipment maintained regularly according to manufacturers’ specifications and good practice? |  |  |
| A.11.2.5 | Is the authorization for information and other assets given each time they are taken out of the company premises? |  |  |
| A.11.2.6 | Are the company assets adequately protected when they are not located at the company premises? |  |  |
| A.11.2.7 | Are all the information and licensed software removed from media or equipment containing media when disposed of? |  |  |
| A.11.2.8 | Are users protecting their equipment when not in physical possession of it? |  |  |
| A.11.2.9 | Is there a policy which forces users to remove papers and media when not present, and lock their screens? |  |  |
| A.12.1.1 | Have the operating procedures for IT processes been documented? |  |  |
| A.12.1.2 | Are all the changes to IT systems, but also to other processes that could affect information security, strictly controlled? |  |  |
| A.12.1.3 | Does someone monitor use of resources and project the required capacity? |  |  |
| A.12.1.4 | Are development, testing and production environments strictly separated? |  |  |
| A.12.2.1 | Are anti-virus software, and other software for malware protection, installed and updated? |  |  |
| A.12.3.1 | Is the backup policy developed; is the backup performed according to this policy? |  |  |
| A.12.4.1 | Are all user logs, faults and other events from IT systems logged, and does someone check them? |  |  |
| A.12.4.2 | Are logs protected in such a way that unauthorized persons cannot change them? |  |  |
| A.12.4.3 | Are administrator logs protected in such a way that system administrators cannot change them or delete them; are they regularly checked? |  |  |
| A.12.4.4 | Are clocks on all IT systems synchronized with a single source of correct time? |  |  |
| A.12.5.1 | Is installation of software strictly controlled; do procedures exist for that purpose? |  |  |
| A.12.6.1 | Is there someone in charge of collecting information about vulnerabilities, and are those vulnerabilities promptly resolved? |  |  |
| A.12.6.2 | Are there specific rules that define restrictions of software installation by users? |  |  |
| A.12.7.1 | Are audits of production systems planned and executed in such a way that they minimize the risk of disruption? |  |  |
| A.13.1.1 | Are the networks controlled in such a way that they protect information in systems and applications? |  |  |
| A.13.1.2 | Are security requirements for in-house and external network services defined, and included in agreements? |  |  |
| A.13.1.3 | Are groups of users, services and systems segregated in different networks? |  |  |
| A.13.2.1 | Is the protection of information transfer regulated in formal policies and procedures? |  |  |
| A.13.2.2 | Do agreements with third parties exist which regulate the security of information transfer? |  |  |
| A.13.2.3 | Are the messages that are exchanged over the networks properly protected? |  |  |
| A.13.2.4 | Did the company list all the confidentiality clauses that need to be included in agreements with third parties? |  |  |
| A.14.1.1 | Are security requirements defined for new information systems, or for any changes to them? |  |  |
| A.14.1.2 | Is the information involved in applications that is transferred through the public networks appropriately protected? |  |  |
| A.14.1.3 | Is the information involved in transactions that is transferred through the public networks appropriately protected? |  |  |
| A.14.2.1 | Are the rules for the secure development of software and systems defined? |  |  |
| A.14.2.2 | Do formal change control procedures exist for making any changes to the new or existing systems? |  |  |
| A.14.2.3 | Are critical applications tested after the operating systems have been changed or updated? |  |  |
| A.14.2.4 | Are only the changes that are really necessary performed to information systems? |  |  |
| A.14.2.5 | Are the principles for engineering secure systems documented and implemented? |  |  |
| A.14.2.6 | Is the development environment appropriately secured from unauthorized access and change? |  |  |
| A.14.2.7 | Is the outsourced development of systems monitored? |  |  |
| A.14.2.8 | Is testing for proper implementation of security requirements performed during the development? |  |  |
| A.14.2.9 | Are the criteria for accepting the systems defined? |  |  |
| A.14.3.1 | Are the test data carefully selected and protected? |  |  |
| A.15.1.1 | Is the policy on how to treat the risks related to suppliers and partners documented? |  |  |
| A.15.1.2 | Are all the relevant security requirements included in the agreements with the suppliers and partners? |  |  |
| A.15.1.3 | Do the agreements with cloud providers and other suppliers include security requirements for ensuring the reliable delivery of services? |  |  |
| A.15.2.1 | Are suppliers regularly monitored for compliance with the security requirements, and audited if appropriate? |  |  |
| A.15.2.2 | When making changes to arrangements and contracts with suppliers and partners, are risks and existing processes taken into account? |  |  |
| A.16.1.1 | Are procedures and responsibilities for managing incidents clearly defined? |  |  |
| A.16.1.2 | Are all information security events reported in a timely manner? |  |  |
| A.16.1.3 | Are employees and contractors reporting on security weaknesses? |  |  |
| A.16.1.4 | Are all security events assessed and classified? |  |  |
| A.16.1.5 | Are procedures on how to respond to incidents documented? |  |  |
| A.16.1.6 | Are security incidents analyzed in order to gain knowledge on how to prevent them? |  |  |
| A.16.1.7 | Do procedures exist which define how to collect evidence that will be acceptable during the legal process? |  |  |
| A.17.1.1 | Are requirements for continuity of information security defined? |  |  |
| A.17.1.2 | Do procedures exist that ensure the continuity of information security during a crisis or a disaster? |  |  |
| A.17.1.3 | Is exercising and testing performed in order to ensure effective response? |  |  |
| A.17.2.1 | Does IT infrastructure have redundancy (e.g. secondary location) to fulfill the expectations during disasters? |  |  |
| A.18.1.1 | Are all legislative, regulatory, contractual and other security requirements listed and documented? |  |  |
| A.18.1.2 | Do procedures exist that ensure the enforcement of intellectual property rights, in particular, the used of licensed software? |  |  |
| A.18.1.3 | Are all the records protected according to identified regulatory, contractual and other requirements? |  |  |
| A.18.1.4 | Is personally identifiable information protected as required in laws and regulations? |  |  |
| A.18.1.5 | Are cryptographic controls used as required in laws and regulations? |  |  |
| A.18.2.1 | Is information security regularly reviewed by an independent auditor? |  |  |
| A.18.2.2 | Do the managers regularly review if the security policies and procedures are performed properly in their areas of responsibility? |  |  |
| A.18.2.3 | Are information systems regularly reviewed to check their compliance with the information security policies and standards? |  |  |

# Internal audit checklist for ISO 22301

|  |  |  |  |
| --- | --- | --- | --- |
| Clause | Requirement of the standard | Compliant Yes/No | Evidence |
| 4.2 | Did the organization determine interested parties? |  |  |
| 4.2 | Does the list of all of interested parties’ requirements exist? |  |  |
| 4.3 | Is the scope documented, defining which products and services are included, and are exclusions explained? |  |  |
| 5.1 | Does top management actively support the business continuity activities? |  |  |
| 5.2 | Is the BCMS compatible with the strategy of the company? |  |  |
| 5.2 | Does top management show commitment by providing all the resources and communicate the importance of business continuity? |  |  |
| 5.2 | Is the person responsible for BCMS appointed, and does this person have enough authority? |  |  |
| 5.3 | Does Business continuity policy exist, and does it define the framework for setting objectives? |  |  |
| 5.3 | Is Business continuity policy communicated within the company? |  |  |
| 5.4 | Are roles and responsibilities for business continuity assigned and communicated? |  |  |
| 6.1 | Did the organization determine all the risks and opportunities? |  |  |
| 6.1 | Did the organization plan the actions to address identified risks and opportunities? |  |  |
| 6.2 | Are the business continuity objectives set, and are they communicated to all relevant employees? |  |  |
| 6.2 | Are the business continuity objectives measurable; are they monitored and updated? |  |  |
| 6.2 | Are the following defined: steps required to achieve objectives, who is responsible, what are the deadlines and which resources are required? |  |  |
| 7.1 | Are adequate resources provided for all the elements of the BCMS? |  |  |
| 7.2 | Are required competences defined, trainings performed, and records of competences maintained? |  |  |
| 7.3 | Is the personnel aware of Business continuity policy, their role, and consequences of not complying with the rules? |  |  |
| 7.4 | Do procedures exist which define what to communicate related to business continuity, when to communicate it, and to whom? |  |  |
| 7.5 | Does the process for managing documents and records exist, including who reviews and approves documents, where and how they are published, stored and protected? |  |  |
| 7.5 | Are documents of external origin controlled? |  |  |
| 8.1 | Are outsourced processes identified and controlled? |  |  |
| 8.2.1 | Are processes for risk assessment and business impact analysis defined and documented? |  |  |
| 8.2.2 | Is business impact analysis performed, including all the activities, and are impacts of not performing these activities over time assessed? |  |  |
| 8.2.2 | Are maximum acceptable outages set for each activity; are the dependencies between activities and interested parties identified? |  |  |
| 8.2.3 | Is risk assessment performed for all the activities, processes and assets, and are disruptions that need to be treated identified? |  |  |
| 8.3.1 | Are recovery time objectives set for each activity? |  |  |
| 8.3.1 | Are business continuity capabilities of suppliers and partners evaluated? |  |  |
| 8.3.2 | Are the resources needed for the recovery identified: people, information, buildings & utilities, equipment, IT and communication systems, transportation, finance, partners and suppliers? |  |  |
| 8.3.3 | Is the mitigation for the identified risks defined, and are proactive measures implemented? |  |  |
| 8.4.1 | Do the business continuity procedures or plans have these elements: define communications protocols, have specific steps, are flexible for all kinds of threats, are focused on minimizing the consequences? |  |  |
| 8.4.2 | Do incident response procedures exist with initiation thresholds and procedures of response? |  |  |
| 8.4.3 | Does a procedure exist for detecting and monitoring the incident, and communicating with interested parties, which defines how the means of communication will be available? |  |  |
| 8.4.4 | Do business continuity plans exist that include roles and responsibilities and detailed steps for the recovery of activities? |  |  |
| 8.4.5 | Are the procedures that define the restoration of activities documented? |  |  |
| 8.5 | Are regular exercising and testing performed, are they based on scenarios, and are post-exercise test reports produced? |  |  |
| 9.1.1 | Is it defined what needs to be measured, by which method, who is responsible, who will analyze and evaluate the results? |  |  |
| 9.1.1 | Are the results of measurement and monitoring documented and reported to responsible persons? |  |  |
| 9.1.2 | Are periodic reviews of the documentation performed, and compliance with all the requirements evaluated? |  |  |
| 9.1.2 | Are post-incident reviews performed after the business continuity procedures are activated? |  |  |
| 9.2 | Is there an audit program which defines the timing, responsibilities, reporting, audit criteria and scope? |  |  |
| 9.2 | Are internal audits performed according to audit program, results reported through the Internal audit report and relevant corrective actions raised? |  |  |
| 9.3 | Is management review regularly performed, and are the results documented in minutes of the meeting? |  |  |
| 9.3 | Did management decide on all the crucial issues important for the success of the BCMS? |  |  |
| 10.1 | Does the organization react to every nonconformity? |  |  |
| 10.1 | Does the organization consider eliminating the cause of nonconformity and, where appropriate, take corrective action? |  |  |
| 10.1 | Are all nonconformities recorded, together with corrective actions? |  |  |