Overview

**T**his section contains ready-to-go audit checklists for getting new programs up and running, for checking those that already exist, and for establishing and maintaining a program of *continuous improvement*. They are:

* Appendix One: Environmental Management
* Appendix Two: Corporate Security Management
* Appendix Three: Corporate Responsibility Management
* Appendix Four: Business Continuity Management
* Appendix Five: CTPAT/ISO 28000 Self-Audit Checklist
* Appendix Six: Key Performance Indicators
* Appendix Seven: CMMI Audit Checklist (EXCEL file Information SecuritySummary2)

These are actual checklists that I use on audits and consulting projects, and I am pleased to share them with you. The format of each differs are slightly from the others, and they are both repetitive and comprehensive. Some of the sub-topics may not be applicable to your mission or organization. However, it is better to belabor something than to miss it.

The U.S. Customs-Trade Partnership Against Terrorism (C‐TPAT) seeks to safeguard the world’s vibrant trade industry from terrorists, maintaining the economic health of the U.S. and its neighbors. The partnership develops and adopts measures that add security but do not have a chilling effect on trade, a difficult balancing act. I urge you to audit your organization against Appendix Five. It combines C-TPAT with ISO 28000.

Check Appendix Six: Summary of Key Performance Indicators. You can use these to develop other areas to explore and assess on a continuing basis.

Appendix Seven is a ready-to-go checklist for the Cybersecurity Maturity Model Certification (CMMC) model and its requirements. This is a large EXCEL spreadsheet, and a separate link on this website.

I hope that these checklists take you places that you never thought about. They are ready to go. Tailor the checklists to your organization as necessary and let’s get to work.

Remember: You are your best auditor!

***Gene Razzetti***

***Alexandria, VA.***

***September 2021***

## APPENDIX ONE – ENVIRONMENTAL MANAGEMENT

**GENRAL REQUIREMENTS**

* Has the company[[1]](#footnote-1) established, documented, maintained, and continually improved an environmental management system in accordance with the requirements of an approved environmental management system (EMS) and determined how it will fulfill these requirements?

ENVIRONMENTAL POLICY

* Is there a written environmental policy in existence?
* Was the policy written, distributed and supported by top management?
* Is the environmental policy appropriate to the nature, scale, and environmental impacts of all its activities, products and services?
* Does it include a commitment to continuous improvement and prevention of pollution?
* Does the policy support a commitment to comply with applicable legal requirements and the requirements to which the organization subscribes which relate to its environmental aspects?
* Is there a framework for setting and reviewing environmental objectives and targets?
* Is there a framework for monitoring environmental objectives and targets?
* Has the policy been documented, implemented, maintained, and communicated to all employees?
* Is the policy available to the public?

|  |
| --- |
| **ENVIRONMENTAL PLANNING**   * Does the company have a procedure for identifying the environmental aspects of its activities, products, and services? * Does the company determine those aspects that can have significant environmental impacts (i.e., significant environmental aspects) * Do the environmental objectives of the company match the level of risks related to the list of environmental aspects? * Is the list of environmental aspects and objectives up-to-date? * Is there a procedure to identify and access the legal environmental considerations related to the company’s environmental aspects? * Does each significant level of the company have environmental objectives and targets at appropriate locations? * Are all environmental objectives and targets consistent with environmental policy? * Are specific responsibilities documented at every level in the organization for each environmental objective and target? Does this include the means and time frame for completion? * Are new products or processes and their development included in the Environmental Management System?   **IMPLEMENTATION & OPERATION**   * Has management ensured the availability of resources essential to establish, implement, maintain, and improve the EMS, including human resources with specialized skills, operational infrastructure, technology and financial resources? * Does an organizational chart exist showing roles, responsibilities, and authorities of all the EMS personnel? * Has a management representative been appointed? * Is there written evidence that the Management Representative is able to assure the establishment, implementation, and maintenance of requirements related to the Environmental Management System? * Does the Management Representative report regularly on the performance of the Environmental Management System to top management? * Are training needs identified? * Are personnel involved with environmental impacts required to attend appropriate training? Is there a written report of such training? Is there a training schedule? * Does training emphasize the importance of conformity with the EMS? * Are employees aware of the significant environmental aspects and related actual or potential impacts associated with their work, and the environmental aspects of improved personal performance, and the potential consequences of departure from specified procedures? * Is emergency preparedness and response part of the required training? Are personnel aware of the consequences of departures from established environmental procedures? * Are there job descriptions outlining the education, training, and experience required for performing tasks that can cause significant environmental impacts? * Is there a procedure for internal communications between various levels and functions? * Is there a written procedure for receiving, documenting, and responding to relevant communications from external parties concerning environmental matters? * Does this procedure for document control specify where controlled documents can be located; that the documents are periodically reviewed for adequacy; that the current version of a document is in the appropriate location; that obsolete documents are immediately removed from the system; and that some obsolete documents be retained for legal or reference purposes? * Looking at a sample of controlled documents, are they legible, correctly dated, readily identifiable, maintained in an orderly manner, and retained for the designated period? * Are the procedures and responsibilities for the establishment of maintenance of new or revised documents established? * Is there a documented list of operations and activities directly related to the environmental impacts identified by the Company? Do these operations and activities fall within the scope of the Company’s environmental policy, objectives, and targets? * Are these operations and activities planned and maintained with procedures and work instructions to ensure that there are no deviations from the environmental policies, objectives, and targets? Are there stipulated operating criteria in the written procedures and work instructions for operations? * Has the Company identified situations where there is a potential for accidents or emergency situations that have significant environmental impacts? Are there written procedures for emergency preparedness and response? * Are these emergency procedures routinely tested where practicable?   **CHECKING**   * Has the company established procedures to monitor and measure, on a regular basis, the key characteristics of operations that can have a significant environmental impact? * Do the procedures include documenting of information to monitor performance and conformity with environmental objectives and targets? * Does the organization ensure that calibrated or verified monitoring and measurement equipment is used and maintained and are associated records maintained? * Has the organization established procedures to periodically evaluate compliance with legal requirements, and are there records of these periodic evaluations? * Does the Company have a written procedure for monitoring and measuring key characteristics that have significant impacts on the environment? Are the measurements recorded and compared to objectives and targets? * Is the monitoring equipment maintained and calibrated? Are records kept for equipment maintenance and calibration? * Is there a procedure for evaluating compliance with relevant environmental regulations? * Is there a procedure for investigating nonconformance and taking action to mitigate the environmental impacts that could result? Has a single job title been identified as the ultimate authority for this procedure? * Are corrective and preventive actions taken appropriate to the size of the problem and the level of risk involved? Are there written records of the corrective and preventive actions? * Does the Company change its procedures and processes based on corrective and preventive recommendations? Are these changes documented? * Is there a written procedure for the identification, maintenance, and disposal of environmental records? Are the environmental records legible, identifiable, and traceable to their related activity, product, or service? Are the environmental records stored to prevent deterioration or loss? Is there an established retention time? * Is there a written procedure to establish and maintain a system of internal auditing of the Environmental Management System? Does the procedure establish an internal auditing system to assure that the Environmental Management System conforms to planned activities, has been properly implemented, is properly maintained, and is these findings reported to top management? * Is there a written audit schedule to which the company conforms completely? * Does the internal audit procedure document the method for establishing the audit scope, audit frequency, methodologies to use, how to report results, and responsibilities of the audit team?   **MANAGEMENT REVIEW**   * Does the Company’s management regularly review the entire Environmental Management System? Is the Environmental Management System checked for its suitability, adequacy, and effectiveness? * Is the management review documented? Did previous management reviews consider changes in its policies or objectives based on audit results, changing circumstances, or the need for continuous improvement? * Does input to the management reviews include:   + Results of internal audits and evaluations of compliance with legal requirements and other requirements to which the organization subscribes   + Communications from external interested parties, including complaints   + The environmental performance of the organization   + The extent to which environmental objectives and targets have been met   + Status of corrective or preventive actions   + Follow-up actions from previous management reviews   + Changing circumstances, including developments in legal and other requirements related to its environmental aspects   + Recommendations for improvement? |
|  |

## 

## APPENDIX TWO: CORPORATE SECURITY MANAGEMENT

GENRAL REQUIREMENTS

* Has the organization established, documented, maintained, and continually improved an effective security management system for identifying security threats, assessing risks, and controlling/mitigating their consequences?
* Has the organization defined the scope of its security management system, including control of outsourced processes that affect the conformity with these requirements?

SECURITY MANAGEMENT POLICY

* Has top management developed a written security policy, and is it:
  + Consistent with other organizational policies
  + Providing framework for specific security objectives, targets, and programs to be produced
  + Consistent with the organization’s overall security threat and risk management framework
  + Appropriate to the threats to the organization and the nature and scale of its operations
  + Clear in its statement of overall/broad security management objectives
  + Committed to compliance with current applicable legislation, regulatory and statutory requirements and with other requirements to which the organization subscribes
  + Visibly endorsed by top management
  + Documented, implemented, and maintained
  + Communicated to all relevant employees and third parties including contractors and visitors with the intent that these persons are made aware of their individual security-related obligations
  + Available to stakeholders where appropriate
  + Provided for review in case of acquisition or merger, or other change to the business scope, which may affect the relevance of the security management system?

|  |
| --- |
| **SECURITY RISK ASSESSMENT PLANNING**   * Has the organization established and maintained procedures for ongoing identification and assessment of security threats and security management-related threats and risks, and the identification and implementation of necessary management control measures? * Are threats and risk identification, assessment, and control methods appropriate to the nature and scale of the operations? * Does the risk assessment include:   1. Physical failure threats and risks, such as functional failure, incidental damage, malicious damage or terrorist or criminal action   2. Operational threats and risks, including the control of security, human factors, and other activities that affect the organization’s performance, condition, or safety   3. Natural environmental events which may render security measures and equipment ineffective   4. Factors outside of the organization’s control such as failures in externally supplied equipment and services   5. Stakeholder threats and risks, such as failure to meet regulatory requirements or damaged reputation   6. Design and installation of security equipment including replacement, maintenance, etc.   7. Information and data management and communications   8. A threat to the continuity of operations? * Are the results of these assessments considered and do they provide input into:   1. Security management objectives and targets   2. Security management programs   3. The determination of requirements for the design, specification, and installation   4. Identification of adequate resources including staffing levels   5. Identification of training needs and skills   6. Development of operational controls   7. The organization’s overall threat and risk management framework? * Is the organization’s methodology for risk identification and assessment:   1. Defined with respect to its scope, nature, and timing, to ensure that it is proactive rather than reactive   2. Include a collection of information related to security threats and risks   3. Provide for the classification of threats and risks and identification of those that are to be avoided, eliminated, or controlled   4. Provide for the monitoring of actions to ensure effectiveness and the timeliness of their implementation? * Has the organization established, implemented, and maintained a procedure:   1. To identify and have access to the applicable legal requirements and other requirements to which the organization subscribes related to its security threat and risks   2. To determine how these requirements apply to its security threats and risks? * Does the organization have documented security management objectives, and do they take into account:   1. Legal, statutory, and other security regulatory requirements   2. Security-related threats and risks   3. Technological and other options   4. Financial, operational, and business requirements   5. Views of appropriate stakeholders? * Are the security objectives:   1. Consistent with the organization’s commitment to continual improvement   2. Quantified (where practicable)   3. Communicated to all relevant employees and third parties, including contractors, with the intent that these persons are made aware of their personal obligations   4. Reviewed periodically to ensure that they remain relevant and consistent with the security management policy. Where necessary the security management objectives shall be amended accordingly. * Are security management targets established, implemented, and maintained, and are they:   1. To an appropriate level of detail   2. Specific, measurable, achievable, relevant and time-based (where practicable)   3. Communicated to all relevant employees and third parties including contractors with the intent that these persons are made aware of their individual obligations   4. Reviewed periodically to ensure that they remain relevant and consistent with the security management objectives, and amended accordingly? * Are there security management programs established for achieving the organization’s objectives and targets, and are they optimized and prioritized, and do they describe:   1. Designated authority and responsibility for achieving objectives and targets   2. The means and time scale by which the objectives and targets will be achieved, and are they reviewed/amended periodically to ensure that they remain effective?   **IMPLEMENTATION & OPERATION**  **Structure, authority, and responsibility for security management**   * Has the organization established and maintained an organizational structure of roles, responsibilities, and authorities, consistent with the achievement of its security management policy, objectives, targets, and programs, and are these defined, documented, and communicated to responsible individuals? * Does top management provide evidence of its commitment to development of the security management system and improving its effectiveness by: * Appointing a member of top management who, irrespective of other responsibilities is responsible for the design, maintenance, documentation and improvement of the security management system * Appointing members of management with the necessary authority to ensure that the objectives and targets are implemented * Identifying and monitoring the requirements and expectations of the organization’s stakeholders and taking appropriate action to manage these expectations * Ensuring the availability of adequate resources * Communicating to the organization the importance of meeting its security management requirements in order to comply with its policy * Ensuring any security programs generated from other parts of the organization complement the security management system * Communicating to the organization the importance of meeting its security management requirements in order to comply with its policy * Ensuring security-related threats and risks are evaluated and included in organizational threat and risk assessments as appropriate * Ensuring the viability of the security management objectives, targets, and programs?   **Competence, training, and awareness**   * Does the organization ensure that personnel responsible for the design, operation, and management of security equipment and processes are suitably qualified in terms of education, training and/or experience, and has the organization established and maintained procedures for making persons working for it or on its behalf aware of:  1. The importance of compliance with the security management policy and procedures, and to the requirements of the security management system 2. Their roles and responsibilities in achieving compliance with the security management policy and procedures and with the requirements of the security management system, including emergency preparedness and response requirements 3. The potential consequences to the organization’s security by departing from specified operating procedures?   **Communication**   * Does the organization have procedures for ensuring that pertinent security management information is communicated to and from relevant employees, contractors, and stakeholders? * Is proper consideration given to the sensitivity of security-related information?   **Documentation**   * Has the organization established a security management documentation system that includes but is not limited to the following:  1. The security policy, objectives, and targets 2. Description of the security management system scope 3. Description of the main elements of the security management system and their interaction, and reference to related documents 4. Documents, including records, required by this International Standard 5. Documents including records determined by the organization to be necessary to ensure the effective planning, operation and control of processes that relate to its significant security threats and risks   **Document and data control**   * Has the organization established and maintained procedures for controlling all documents, data, and information required by Clause 4 of this International Standard to ensure that:  1. These documents, data and information can be located and accessed only by authorized individuals 2. These documents, data, and information are periodically reviewed, revised as necessary, and approved for adequacy by authorized personnel 3. Current versions of relevant documents, data, and information are available at all locations where operations essential to the effective functioning of the security management system are performed 4. Obsolete documents, data, and information are promptly removed from all points of issue and points of use, or otherwise assured against unintended use 5. Archival documents, data, and information retained for legal or knowledge preservation purposes or both are suitably identified 6. These documents, data, and information are secure, and if in electronic form are adequately backed up and can be recovered?   **Operational control**   * Has the organization identified operations that are necessary for achieving:  1. Its security management policy 2. The control of activities and mitigation of threats identified as having significant risk 3. Compliance with legal, statutory and other regulatory security requirements 4. The security management objectives 5. The delivery of its security management programs 6. The required level of supply chain security 7. Has the organization ensured that these operations and activities are carried out under specified conditions by:  * Establishing, implementing, and maintaining documented procedures to control situations where their absence could lead to failure to achieve the operations and activities listed above * Evaluating any threats posed from upstream supply chain activities and applying controls to mitigate these impacts to the organization and other downstream supply chain operators * Establishing and maintaining the requirements for goods or services which impact on security and communicating these to suppliers and contractors? * Where existing designs, installations, operations, etc., are revised, do the revisions include:   1. Revised organizational structure, roles or responsibilities   2. Revised security management policy, objectives, targets, or programs   3. Revised processes or procedures   4. The introduction of new infrastructure, security equipment or technology, which may include hardware and/or software   5. The introduction of new contractors, suppliers or personnel, as appropriate?   **Emergency preparedness, response and security recovery**   * Has the organization established, implemented, and maintained appropriate plans and procedures to identify the potential for and responses to, security incidents and emergency situations, and for preventing and mitigating the likely consequences associated with them? * Do the plans and procedures include information on the provision of maintenance of any identified, facilities or services that can be required during or after incidents or emergency situations? * Does the organization periodically review the effectiveness of its emergency preparedness, response and security recovery plans and procedures, in particular after the occurrence of incidents or emergency situations caused by security breaches and threats, and are these procedures periodically tested (as applicable)?   CHECKING AND CORRECTIVE ACTION  **Security performance measurement and monitoring**   * Has the organization established and maintained procedures to monitor and measure the performance of its security management system, and does it consider associated threats, risks, including potential deterioration of mechanisms and their consequences, and do these procedures provide for:  1. Both qualitative and quantitative measurements, appropriate to the needs of the organization 2. Monitoring the extent to which the organization’s security management policy, objectives, and targets are met 3. Proactive measures of performance that monitor compliance with the security management programs, operational control criteria and applicable legislation, statutory and other security regulatory requirements 4. Reactive measures of performance to monitor security-related deteriorations, failures, incidents, non-conformances and other historical evidence of deficient security management system performance 5. Recording data and results of monitoring and measurement sufficient to facilitate subsequent corrective and preventive action analysis, and if monitoring equipment is needed are there maintenance and calibration procedures, and are records of calibration kept?   **System evaluation**   * Does the organization evaluate security management plans, procedures, and capabilities through periodic reviews, testing, post-incident reports, lessons learned, performance evaluations, and exercises, and are significant changes in these factors reflected immediately in the procedures? * Does the organization periodically evaluate compliance with relevant legislation and regulations, industry best practices, and conformance with its own policy and objectives? * Are records kept of the results of these periodic evaluations?   **Security-related failures, incidents, non-conformance and corrective and preventive actions**   * Has the organization established, implemented, and maintained procedures for defining responsibility and authority for:   1. Evaluating and initiating preventive actions to identify potential failures of security in order that they may be prevented from occurring   2. The investigation of security-related      + 1. Failures, including near misses and false alarms        2. Incidents and emergency situations        3. Non-conformances   3. Taking action to mitigate any consequences arising from such failures, incidents, and non-conformances   4. The initiation and completion of corrective actions   5. The confirmation of the effectiveness of corrective actions taken? * Are all proposed corrective and preventive actions reviewed through the security threat and risk assessment process prior to implementation? * Are corrective and preventive actions taken appropriate for the magnitude of the problems and commensurate with the security management-related risks and threats likely to be encountered?   **Control of records**   * Has the organization established and maintained records as necessary to demonstrate conformity to the requirements of its security management system and of this International Standard, and the results achieved? * Has the organization established, implemented, and maintained procedures for the identification, storage, protection, retrieval, retention, and disposal of records? * Are the records legible, identifiable, and traceable? * Are electronic and digital documentation rendered tamper-proof, securely backed-up, and accessible only by authorized personnel?   **Audit**   * Has the organization established, implemented, and maintained a security management audit program and does it ensure that audits of the security management system are carried out at planned intervals, in order to:   1. Determine whether or not the security management system:      1. Conforms to planned arrangements for security management including the requirements of the whole of Clause 4 of this specification      2. Has been properly implemented and maintained      3. Is effective in meeting the organization’s security management policies and objectives   2. Review the results of previous audits and the actions taken to rectify non-conformances   3. Provide information on the results of audits to management   4. Verify that the security equipment and personnel are appropriately deployed? * Is the audit schedule based on the results of threat and risk assessments of the organization’s activities, and the results of previous audits, and do the audit procedures cover the scope frequency, methodologies, and competencies, as well as the responsibilities and requirements for conducting audits and reporting results, and are audits, where possible, conducted by personnel independent of those having direct responsibility for the activity being examined?   **MANAGEMENT REVIEW AND CONTINUAL IMPROVEMENT**   * Does top management review the organization’s security management system at planned intervals, to ensure its continuing suitability, adequacy, and effectiveness, and do reviews include assessing opportunities for improvement and the need for changes to the security management system, including security policy and security objectives and threats and risks. Records of the management reviews shall be retained. * Do inputs to management reviews include:   1. Results of audits and evaluations of compliance with legal requirements and with other requirements to which the organization subscribes   2. Communication from external interested parties, including complaints   3. The security performance of the organization   4. The extent to which objectives and targets have been met   5. Status of corrective and preventive actions   6. Follow-up actions from previous management reviews   7. Changing circumstances, including developments in legal and other requirements related to its security aspects   8. Recommendations for improvement? * Do outputs from management reviews include any decisions and actions related to possible changes to security policy, objectives, targets, and other elements of the security management system, consistent with the commitment to continual improvement?   **Notes:**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |

## APPENDIX THREE: CORPORATE RESPONSIBILITY MANAGEMENT

**1. CORPORATE RESPONSIBILITY SYSTEM REQUIREMENTS**

**1.1** **General**

* Has the organization developed, documented, and implemented a Corporate Responsibility Management System (CRMS) that will:
* Identify all processes and interactions
* Determine the interaction between these various processes and interactions,
* Determine the (ethics-based) effectiveness criteria for the implementation and monitoring of these processes,
* Show the availability of resources and information relevant to the processes,
* Monitor, measure, and analyze the processes
* Take necessary actions to:
* Achieve the planned objectives,
* Implement corrective and preventive action, and
* Continuously improve the processes?
  1. **Policy and Procedural Requirements**
     1. **General**
* Does the CRMS include a manual, containing documented explanations of policies and objectives, and procedures required by this International Standard?

**4.2.2 Corporate Responsibility Management System Manual**

* Does the organization maintain an Corporate Responsibility Management System manual that includes:
  + The scope of the Corporate Responsibility Management System,
  + The documented procedures established for the system or reference to them, and
  + A description of the interaction between the processes of the Corporate Responsibility Management System.

**5. Management INVOLVEMENT**

* 1. **Involvement of Management**
* Does management demonstrate its social and ethical involvement with society, the governing board, other stakeholders, and own personnel by:
  + Developing, implementing, and continuously improving the Corporate Responsibility Management System,
  + Communicating to all levels in the organization the importance of satisfying the requirements, standards, and values used by the organization to carry out its business,
  + Communicating to all levels in the organization the importance of satisfying statutory and regulatory requirements in the practice of company ethics,
  + Developing and implementing the company’s ethics policies and objectives,
  + Carrying out a program or internal audits, and
  + Making resources available?

**5.2 Corporate Responsibility Management** **Policy**

* Has management determined a policy and ensured that the policy:
  + Is suitable and contiguous with the needs of the organization,
  + Is consistent with statutory and regulatory requirements,
  + Provides for continuous improvement of the CRMS
  + Provides the framework for development of measurable objectives,
  + Is communicated to, and understood by, the whole organization,
  + Is periodically assessed for its suitability?

**5.3 Administration and Management**

* Has management ensured that all responsibilities and authorities are documented and communicated through the organization, be establishing:
  + The tasks, responsibilities, and authorities of all employees with respect to carrying out the formulated ethics policy.
  + The tasks, responsibilities, and authorities of assigned supporting contractors, as applicable?

**5.3.1 Oversight Officer**

* Has management appointed an oversight officer, who will be responsible for the development, implementation, and maintenance of the Corporate Responsibility Management System?
* Does the Management Representative work directly for the President and periodically report on the performance of the Corporate Responsibility Management System and identify potential improvements?
  + 1. **Internal Communication**
* Has management provided a structure to inform personnel about the Corporate Responsibility Management System, in which ethics management is regularly reviewed within the organization and communication takes place at all levels and functions regarding the effectiveness of the Corporate Responsibility Management System?

**5.4 Management Oversight**

* Does management periodically review the effectiveness of the Corporate Responsibility Management System?
* During each review, does management determine:
  + If the Corporate Responsibility Management System has to be modified,
  + If policies have to be modified, or objectives amended,
  + The need for (or status of) corrective and corrective actions?

1. **HUMAN resourceS**

**6.1 General**

* Are personnel trained on the Corporate Responsibility Management System and how it applies to their positions and functions?

**6.1.2 Ethics Awareness Training**

* Has management:
  + Developed and scheduled ethics awareness training for all personnel,
  + Evaluated and measured the effectiveness of the training, and
  + Record all relevant training conducted?
    1. **Complaints Procedure**
* Has management provided employees with a process for communicating instances of unacceptable behavior, to include:
* The complaint submission procedure
* Responsibilities for complaints procedure administration,
* Confidentiality of complaints
* Appeal rights of personnel accused?

**6.1.4 Personnel Representation**

* Has management created a consultative body within the organization:
  + To monitor the ethical functioning of the organization and the interests of all the employees,
  + To define objectives, tasks, responsibilities, authorities, and procedures in the operation of the Corporate Responsibility Management System,
  + To review instances of reported violations of the Corporate Responsibility Management System, and
  + To administer the organization’s system of sanctions (see 6.3)?

**6.2**  **Sanctions**

* Has management developed a system of sanctions to include:
  + Definition and description undesirable ethical behavior in the organization,
  + The manner in which unacceptable ethical conduct is reported,
  + The manner in which corrective action will be taken, and
  + The manner in which personal information is documented and recorded?

**6.3 Code of Ethics and Standards of Conduct**.

* Has management created a *Code of Ethics and Standards of Conduct*, to include:
  + The Corporate Responsibility Management System,
  + Statutory and regulatory requirements,
  + Formal standards of performance and expectations,,
  + The organization’s moral values with respect to personnel, customers, competitors, suppliers, and society,
  + Unacceptable ethical behavior as it applies to the organization,
  + Legal obligations of the organization and its members,
  + Intellectual property,
  + Physical and environmental security,
  + Access control,
  + Communications and operations management,
  + Use of company property,
  + Internet usage,
  + Timesheet and travel claim preparation,
  + Working from home,
  + Internal auditing processes?

7 MANAGING THE CORPORATE RESPONSIBILITY MANAGEMENT SYSTEM

**7.1 Communication and Participation**

* Does management involve all levels of the organization in the operation of the Corporate Responsibility Management System?
  + Do committees will ensure that meetings are recorded , and
  + Is sufficient time and resources are allocated?

**7.2 Integrity and Disclosure**

* Has the organization will defined (as applicable) processes for:
* Financial integrity and accurate disclosure
* Key performance indicators and reporting of deviations
* Management responsibilities and oversight
* Safeguards (e.g., periodic inventories, reconciliations,)
* Record keeping and retention
* Recording and disbursement of funds
* Risk analysis and mitigation
* Conflicts of interests, outside interests, and related transactions
* Timesheet and travel claim preparation, to include:
  + Time recording
  + Labor charging/rate determination
  + Customer billing
* Copyrighted or licensed materials
* Accurate representation of data and credentials
* Reporting adverse personnel information.

**7.3 Personnel Recruitment and Selection**

* Has the organization developed ethically responsible procedures for the recruitment and selection of personnel so as to positively influence and reinforce company culture?
* Has the organization maintained the following as applicable:
  + A policy statement precluding discrimination on grounds of ethnic origin, handicap or gender or other discrimination,
  + A signed agreement by prospective employees adhering to the Statement of Ethics Policy,
  + A documented selection procedure for employment agencies servicing the organization,
  + Criteria for evaluation of the ethics of employment agencies doing business with the organization,
  + Recording the results of the measures?

**7.4 Contracts of Employment**

* Does the organization reflect the *Code of Ethics and Standards of Conduct* in its employment contracts?
  1. **Performance Review**
* Does management ensure that scheduled personnel performance reviews cover adherence to the policies and practices of the Corporate Responsibility Management System? Specifically:
  + Does the organization describe the procedures for carrying out the above-mentioned appraisal/performance?
  + Does discussion cover all areas and issues that can affect the work and the performance of the employee?
  + Are employees to be appraised informed about what is required of them in the function that they are carrying out?
  + Does the organization have a standard appraisal form for use by reporting seniors in the organization?
  + Is there an appeals procedure?

**7.6 Requirements for Suppliers**

* Does the organization ensure that suppliers are aware of the applicable sections of the *Code of Ethics and Standards of Conduct* and the expectations of suppliers in accordance with the *Code of Ethics and Standards of Conduct*?

**7.7 Community Responsibility**

* Is there a policy defining the organization’s responsibility to the community (i.e., district, town/city, and region)?

**7.8 Quality of Life**

* Does the organization monitor its effect on the quality of life of:
  + Employees and their families,
  + Major suppliers and subcontractors
  + The geographical area in which it operates and has potential to impact positively or negatively?

**7.9 Competition**

* Does the organization conform to applicable statutory and regulatory requirements with regard to:
  + The development and maintenance of pricing structures
  + Delivery terms and conditions
  + Exclusion of supply to particular customers
  + The use of different prices for the same level of performance
  + Doing business with organizations that use restrictive competitive practices
  + The fixing of prices
  + Dividing of markets
  + Restrictive production or supply practices?

**7.10 Accident Reporting**

* Has the organization developed procedures for directly reporting safety or environmental accidents to proper authority?

**7.11 Hazardous Materials**

* Has the organization developed (as applicable) procedures to prevent or reduce the environmental risks related to the storage, transfer and transport of dangerous materials? Specifically:
  + Adherence to National laws and regulations, guidelines, decisions, and permits,
  + Responsibilities for carrying out formulated policy,
  + Procedures for the storage, transfer and transport of dangerous materials,
  + Training and qualifications of users?

**7.12 Pollution Prevention**

* Has the organization developed (as applicable) pollution prevention procedures to include:
  + Identification of all potential sources of pollution, wastes, and emissions,
  + Identification of all applicable statutory and regulatory requirements.
  + Reduction measures
  + Recycling opportunities?
* Does the organization discuss the operation of the pollution prevention procedures at scheduled Management Reviews and record discussions, nonconformities, and corrective and preventive actions?

**7.13 Energy Conservation**

* Has the organization developed an Energy Conservation Program, to include:
  + An energy conservation policy,
  + Recognition of all applicable environmental laws and regulations and the conditions that are stipulated in the environmental license as applicable),
  + A survey identifying all sources of energy expenditure and the technical and economic feasibility of implementing specific energy conservation measures.
  + Periodic evaluation of the system during the internal audits and management reviews?

**7.14 Environmental Assessment**

* Does the organization carry out, or have carried out a survey into the environmental aspects of the activities, and into alternatives for those activities which constitute a potential burden on the environment?

**7.14.1 Environmental Aspects**

* Has the organization identified all relevant environmental aspects of products and services, to include:
  + - * + A purchasing policy reflecting for products and services with potential environmental impact,
        + Criteria and selection of the most suitable suppliers?

**4.15 Competence, Experience, and Training**

* Has the organization established requirements with regard to the education and instruction of all personnel and set standards for competence, experience, and training in the following areas related to the Corporate Responsibility Management System? Specifically:
  + - * + Occupational Safety and Health,
        + Energy conservation
        + Hazardous Material Control and Management
        + Pollution prevention, and
        + Recycling.
        + Contracting,
        + Procurement,
        + Internal auditing, and
        + Finance and accounting?

**7.16 Risk Assessment and Minimization**

* Has the organization implemented risk assessment and minimization procedures for all activities and components, in order to:
  + Determine a relative ranking of potential risks, and determine the likely frequencies and consequences of those risks,
  + Recognize opportunities as well as risks, and
  + Formalize and document knowledge for more precise decision-making?

**7.17 Emergency Preparedness and Response**

* Has the organization developed an emergency response plan covering:
  + Identification of potential disasters or emergencies in the organization
  + Preplanned responses
  + Emergency evacuation, aid, and assistance,
  + Safeguarding organization personnel
  + Consequence management (including drills or exercises)
  + Disaster prevention,
  + Cooperation with external aid and assistance organizations
  + Employee awareness training
  + Emergency reporting?

**7.18 Absence Due to Illness**

* Does the organization have documented procedures with regard to work related absenteeism and incapacity through illness, to include:
  + The definition of work related absenteeism and incapacity through illness.
  + Social and medical counseling of employees who are ill or incapacitated. or who are returning to the workplace,
  + Information and training for managers regarding absenteeism, and ways to address employee illness, absence, and return,
  + Maintenance of absenteeism statistics, and
  + Work related health investigation?

**7.19 Safety and Health**

* Does the organization have a published safety and health promotion policy, to include:
  + Occupational safety,
  + Accident prevention and safe human behavior,
  + Workplace cleanliness and sanitation (including ventilation systems),
  + Exercise and nutrition,
  + Transportation safety?

**7.20 Working hours**

* Does the organization have written policies regarding working hours, to include:
  + Applicable statutory and regulatory requirements,
  + Core working hours,
  + Employee categories,
  + Emergency recalls,
  + Working from home,
  + Overtime, and
  + Charge number usage (if appropriate)?

**8. METRICS ESTABLISHMENT**

#### 8.1 General

* Does the organization have documented procedures to monitor and measure, the key characteristics of its operations and activities that can have significant impact on the professional and business ethics of the organization?

**8.1.1 Personnel, Customer, and Stakeholder Satisfaction**

* Does the organization have a research methodology for periodic measurement of personnel, board, and stakeholders’ satisfaction, to include:
  + Effectiveness of the Corporate Responsibility Management System,
  + Effectiveness of the Code of Ethics and Standards of Conduct,
  + Personnel, customer, and stakeholder feedback?

**8.1.2****Internal Reviews**

* Does the organization will conduct periodic internal reviews to determine the effectiveness of the Corporate Responsibility Management System, in order to:
  + Determine whether or not the Corporate Responsibility Management System conforms to the organization’s requirements and to statutory and regulatory requirements
* Has the internal audit system been properly implemented and maintained?
* Are the results of reviews provided to management?

**8.2 Nonconformance and Corrective and Preventive Action**

* Does the organization have procedures for defining responsibility and authority for ethical nonconformities, taking action to mitigate any impacts caused and for initiating and completing corrective and preventive action?
* Are corrective or preventive actions taken to eliminate the cause of actual or potential nonconformities appropriate for the magnitude of the problem and commensurate with actual or potential impact?

**8.3 Continual Improvement**

* Does the organization continually improve the effectiveness of the Corporate Responsibility Management System by using policy, objectives, audit results, data analysis, research into personnel, customer, and stakeholders’ satisfaction, corrective and preventive measures and management review meetings?
* When shortcomings are detected from audit results, data analyses, satisfaction surveys, or management reviews, does the organization ensure that timely corrective and preventive measures are taken?
* Is the effectiveness of measures taken documented?

## APPENDIX FOUR: BUSINESS CONTINUITY MANAGEMENT

**The Business Continuity Management System**

* Has the Organization developed, implemented, maintained, and continually improved a documented BCMS in accordance with the Standard?
* Has the Organization defined the scope of the BCMS and set objectives with due regard to:
  1. Requirements for business continuity
  2. Organizational objectives and obligations
  3. Acceptable level of risk
  4. Statutory, regulatory, and contractual duties; and
  5. Interests of its key stakeholders?
* Has the organization identified the key products and services within the scope of the BCMS?

**BCM Policy**

* Has top management established and demonstrated commitment to a business continuity management policy?
* Does the policy include or make reference to:
  + - 1. The Organization’s business continuity objectives
      2. The scope of business continuity, including limitations and exclusions?
    - Is the policy:

1. Approved by top management
2. Communicated to all persons working for and on behalf on the organization; and
3. Reviewed at planned intervals and when significant changes occur?

**Provision of Resources**

* Has the Organization determined and provided the resources needed to establish, implement, operate, and maintain the BCMS?
* Are BCMS roles, responsibilities, competencies, and authorities defined and documented?
* Has Top Management:

1. Appointed or nominated a person with appropriate seniority and authority to be accountable for BSM policy and implementation; and
2. Appointed one or more persons who, irrespective of other responsibilities, implemented and maintained the BCMS?

**Competency of BCM Personnel**

* Are all personnel assigned business continuity responsibilities competent to perform required tasks by:

1. Determining the necessary competencies for such personnel;
2. Conducting training needs analysis on personnel being assigned BCM roles and responsibilities:
3. Providing training;
4. Ensuring that the necessary competence has been achieved; and
5. Maintaining records of education, training, skills, experience, and qualifications.

**Embedding BCM in the Organization’s Culture**

* To ensure that BCM has become part of its core values and effective management, has the Organization:

1. Raised, enhanced, and maintained awareness through an ongoing BCM education and information program for all employees and establishing a process for evaluating the effectiveness of the BM awareness and delivery; and
2. Communicated to all employees the importance of:
   1. Meeting business continuity management objectives;
   2. Conforming to the business continuity policy; and
   3. Continual improvement; and
3. Ensure that all employees are aware of how they contribute to the achievement of the Organization’s business continuity objectives.

**BCMS Documentation and Records**

**General**

* Does the Organization have documentation covering the following aspects of the BCMS:

1. The scope and objectives of the BCMS and procedures
2. The BCM policy
3. The provision of resources
4. The competency of BCM personnel and associated training records
5. The business impact analysis
6. The risk assessment
7. The business continuity strategy
8. The incident response structure
9. Business continuity plans and incident management plans
10. BCM exercising
11. The maintenance and review of BCM arrangements
12. Internal audit
13. Management review of the BCMS
14. Preventive and corrective actions
15. Continual improvement

* Are records established, maintained, and controlled to provide evidence of the effective operation of the BCMS?
* Are there documented procedures established in order to identify the controls over BCMS documentation and records?

**Control of BCMS Records**

* Are controls established over BCMS records in order to:

1. Ensure that they remain legible, readily identifiable, and retrievable; and
2. Provide for their identification, storage, protection, and retrievable?

**Control of BCMS Documentation**

* Are controls established over the BCMS documentation to ensure that:

1. Documents are approved for adequacy prior to use;
2. Documents are reviewed and updated as necessary and re-approved;
3. Changes and the current revision status of documents are identified;
4. Relevant versions of applicable documents are available at points of use;
5. Documents of external origin are identified and their distribution controlled; and
6. The unintended use of obsolete documents is prevented and that such documents are suitably identified if they are retained for any purpose?

**Implementing and Operating the BCMS**

**Understanding the Organization**

* Is there a defined, documented, and appropriate for determining the impact of any disruption of the activities that support the organization’s key products and services?

**Business Impact Analysis**

* Does the Organization:

1. Identify activities that support its key products and services;
2. Identify impacts resulting from the disruption to these activities, and determine how these vary over time;
3. Establish the maximum tolerable period of disruption for each activity by identifying:
4. The maximum time period after the start of a disruption within which each activity needs to be resumed;
5. The minimum level at which each activity needs to be performed upon resumption; and
6. The length of time within which normal levels of operation need to be resumed?
7. Categorize its activities according to their priority for recovery and identify its critical activities;
8. Identify all dependencies relevant to the critical activities, including suppliers and outsourcing partners;
9. For suppliers and outsourced partners on whom critical activities depend, determine what BCM arrangements are in place for the relevant products and services that they provide;
10. Set recovery time objectives for resumption of critical activities within their maximum tolerable period of disruption; and
11. Estimate the resources that each critical activity will require for resumption?

**Risk Assessment**

* Has the Organization defined, documented, an appropriate method for risk assessment that will enable the organization to understand the threats and vulnerabilities of its critical activities and supporting resources, including those provided by suppliers and outsource partners?
* Does the Organization understand the impact that would arise if an identified threat became an incident and caused a business disruption?

**Determining Choices**

* For each of its critical activities, has the Organization identified available risk treatments that:

1. Reduce the likelihood of a disruption;
2. Shorten the period of disruption;
3. Limit the impact of a disruption on the Organization’s key products and services?

* Has the Organization chosen and implemented appropriate risk treatments for each critical activity in accordance with its level of risk acceptance?

**Determining the Business Continuity Strategy**

* Does the Organization:

1. Define a fit-for-purpose, predefined and documented incident response structure that will enable an effective response and recovery from disruptions;
2. Determine how it will recover each critical activity within its recovery time objective and the BCM arrangements, including the resources required for resumption and products and services provided by suppliers and outsource partners; and
3. Determine how it will manage relationships with its key stakeholders and external parties involved in the recovery?

**Developing and Implementing a BCM Response**

* Does the Organization use the outputs developed above to implement appropriate plans and arrangements to ensure continuity of critical activities and the management of an incident?
* Has the Organization nominated incident response personnel with the necessary responsibility, authority, and competence to manage an incident?
* Does the incident response structure provide sufficient personnel to:

1. Confirm the nature and extent of the incident
2. Trigger an appropriate business continuity response
3. Have plans, processes, and procedures for the activation, operation, coordination, and communication of the incident response
4. Have resources available to support the plans, processes, and procedures to manage an incident; and
5. Communicate with stakeholders?

* Does the Organization have documented plans that detail how it will manage an incident and how it will recover or maintain its activities to a predetermined level in the event of a disruption?
* Does the plan:

1. Have a defined purpose and scope
2. Have accessibility and is it understood by the users
3. Have ownership and responsibility for review, update, and approval specified
4. Have alignment with other relevant contingency arrangements external to the Organization?

* Does the plan correctly contain:

1. Identified lines of communication
2. Key tasks and reference information
3. Defined roles and responsibilities for people and teams having authority during and following an incident
4. Guidelines and criteria regarding which individuals have the authority to invoke each plan and under what circumstances
5. A method by which each plan is invoked
6. Meeting locations with alternatives, and up-to-date contact and mobilization details for any relevant agencies, organizations, and resources that might be required to support the response
7. A process for standing down once the incident is over
8. A reference to the essential contact details for all key stakeholders
9. Details to manage the immediate consequences of a business disruption giving due regard to:
   1. The welfare of individuals
   2. Strategic and operational options for responding to the disruption; and
   3. Prevention of further loss or unavailability of critical activities;
10. Details for managing the incident, including:
    1. Provision for managing issues during the incident; and
    2. Processes to enable continuity and recovery of critical activities;
11. Details on how and under what circumstances the Organization will communicate with employees and their relatives, key stakeholders, and emergency contacts;
12. Details on the Organization’s media response following an incident, including:
    1. The incident communications strategy
    2. Preferred interface with the media
    3. Guideline or template for drafting a statement for the media; and
    4. Appropriate spokespeople
13. A method for recording key information about the incident, actions taken, and decisions made
14. Details of actions and tasks that need to be performed
15. Details of the resources required for business continuity and business recovery at different points in time; and
16. Prioritized objectives in terms of the critical activities to be recovered, the timescales in which they are to be recovered, and the recovery levels needed for each critical activity?

**Exercising, maintaining, and reviewing BCM arrangements**

* Does the Organization ensure that BCM arrangements are validated by exercise and review, and are kept up-to-date?
* Does the Organization:

1. Develop exercises that are consistent with the scope of the BCMS
2. Have a program approved by top management to ensure that exercises are carried out at planned intervals and when significant changes occur
3. Carry out a range of different exercises that, taken together, validate the whole of the business continuity arrangements
4. Plan exercises so that the risk of an incident occurring as a direct result of the exercise is minimized
5. Define the goals and objectives of the exercise
6. Conduct a post-exercise review of each exercise that will assess the achievement of the goals and objectives of the exercise
7. Produce a written report of the exercise, outcome, and feedback, including required actions?

* Does the Organization, at defined intervals, review its BCM arrangements to ensure their continuing suitability, adequacy, and effectiveness?
* Does the Organization ensure that its business continuity capability and appropriateness is reviewed at planned intervals and when significant changes occur, to ensure its continuing suitability, adequacy, and effectiveness?
* Are BCM arrangements reviewed regularly by self-assessment or audit?
* In the event of an incident that results in exercising the BCM, is a post-incident review conducted to determine:

1. The cause and the nature of the incident
2. The adequacy of the response
3. The effectiveness of the organization in meeting its recovery time objectives
4. The effectiveness of the organization in preparing the employees
5. Improvements that can be made in the BCM arrangements?

**Monitoring and Reviewing the BCMS**

* 1. **Internal Audit**
* Does the Organization conduct internal audits at prescribed intervals to determine whether the BCMS:

1. Conforms to planned arrangements for BCM, including the requirements of the BCM Standard
2. Is properly implemented and maintained
3. Is effective in meeting the Organization’s BCM policy and objective?

* Is information on the results of the audits provided to management?
* Does the internal audit program reflect risk assessment and control and mitigation measures and the results of previous audits?
* Does the internal audit procedure address:

1. The responsibilities, competencies, and requirements for planning and conducting audits, reporting results and retaining associated records
2. The determination of audit criteria, scope, frequency, and methods?

* Do the selection of auditors and the conduct of audits ensure objectivity and impartiality in the audit process?

* 1. **Management Review of the BCMS**
* Does management review the Organization’s BCMS at planned intervals and when significant changes occur, to ensure its continuing suitability, adequacy, and effectiveness?
* Does the review include assessing opportunities for improvement and the need for changes to the BCMS, including business continuity management policy and objectives?
* Are the results of the reviews clearly documented and maintained?

**Review Input**

* Does input to management reviews include:

1. Results of BCMS audits and reviews, including those of key suppliers and outsource partners
2. Feedback from interested parties, including independent observations
3. Techniques, products, and procedures, which could be used to improve BCMS performance and effectiveness
4. Status of preventive and corrective actions
5. Level of residual risk and acceptable risk
6. Vulnerabilities or threats not adequately addressed in the previous risk assessment
7. Follow up actions from previous management reviews
8. External or internal changes that could affect the BCMS
9. Recommendations for improvements
10. Exercise results
11. Emerging good practice and guidance
12. Lessons learned from incidents
13. Results of education and awareness training programs?

**Review Output**

* Does output from management reviews include decisions and actions related to:

1. Varying the scope of the BCMS
2. Improving the effectiveness of the BCMS
3. Resource needs
4. Funding and budgeting requirements
5. Modification of the BCM strategy and procedures, including changes to:

* Business requirements
* Resilience requirements
* Business processes affecting the existing business requirements
* Statutory, regulatory, and contractual requirements
* Levels of risk and/or levels of risk acceptance?

**Maintaining and Improving the BCMS**

**Preventive and Corrective Actions - General**

* Does the Organization continue to improve the BCMS through application of preventive and corrective actions?
* Are preventive and corrective actions taken appropriate to the magnitude of the problems and commensurate with the BCMS and the Organization’s policies and objectives?
* Are changes arising from preventive and corrective actions reflected in BCMS documentation?

**Preventive Action**

* Does the Organization take action to guard against potential nonconformities in order to prevent their occurrence and is it appropriate to the potential impact of the nonconformity?
* Is there a documented procedure for preventive action that defines the requirements for:
  + - 1. Identifying potential nonconformities and their causes
      2. Determining and implementing the action needed
      3. Recording the results of action taken
      4. Reviewing the preventive action taken
      5. Identifying changed risks and ensuring that attention is focused on significantly changed risks?
      6. Ensuring that all those who need to know are informed of the nonconformity and the preventive action put in place
      7. The priority of preventive actions based on the results of the risk assessment?

**Corrective Action**

* Does the Organization take action to eliminate the cause of nonconformities associated with the implementation and operation of the BCMS, in order to prevent their recurrence?
* Is the procedure documented and do the procedures for corrective action define the requirements for:

1. Identifying any nonconformities
2. Determining the causes of the nonconformities
3. Evaluating the need for actions to ensure that nonconformities do not recur
4. Determining and implementing the corrective action needed
5. Recording the results of the action taken
6. Reviewing the corrective action taken?

**Continual Improvement**

* Does the Organization continually improve the effectiveness of the BCMS through the review of:

1. Business continuity policy and objectives
2. Audit results
3. Analysis of monitored events
4. Preventive and corrective actions
5. Management review?

**Notes:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## APPENDIX FIVE: ISO 28000/C-TPAT Checklist

ITEM 4.1 GENRAL REQUIREMENTS

* Has the organization established, documented, maintained, and continually improved an effective security management system for identifying security threats, assessing risks, and controlling/mitigating their consequences?
* Has the organization defined the scope of its security management system, including control of outsourced processes that affect the conformity with these requirements?

ITEM: 4.2 SECURITY MANAGEMENT POLICY

* Has top management developed a written security policy, and is it:
  + Consistent with other organizational policies
  + Providing framework for specific security objectives, targets, and programs to be produced
  + Consistent with the organization’s overall security threat and risk management framework
  + Appropriate to the threats to the organization and the nature and scale of its operations
  + Clear in its statement of overall/broad security management objectives
  + Committed to compliance with current applicable legislation, regulatory and statutory requirements and with other requirements to which the organization subscribes
  + Visibly endorsed by top management
  + Documented, implemented, and maintained
  + Communicated to all relevant employees and third parties including contractors and visitors with the intent that these persons are made aware of their individual security-related obligations
  + Available to stakeholders where appropriate
  + Provided for review in case of acquisition or merger, or other change to the business scope, which may affect the relevance of the security management system?

## OBSERVATION: YES/NO FINDING: YES/NO

***AUDITOR COMMENTS (If Any) (Attach additional pages if required)***

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |
| --- |
| **ITEM 4.3: SECURITY RISK ASSESSMENT PLANNING**   * Has the organization established and maintained procedures for ongoing identification and assessment of security threats and security management-related threats and risks, and the identification and implementation of necessary management control measures? * Are threats and risk identification, assessment, and control methods appropriate to the nature and scale of the operations? * Does the risk assessment include:   1. Physical failure threats and risks, such as functional failure, incidental damage, malicious damage or terrorist or criminal action   2. Operational threats and risks, including the control of security, human factors, and other activities that affect the organization’s performance, condition, or safety   3. Natural environmental events which may render security measures and equipment ineffective   4. Factors outside of the organization’s control such as failures in externally supplied equipment and services   5. Stakeholder threats and risks, such as failure to meet regulatory requirements or damaged reputation   6. Design and installation of security equipment including replacement, maintenance, etc.   7. Information and data management and communications   8. A threat to the continuity of operations? * Are the results of these assessments considered and do they provide input into:   1. Security management objectives and targets   2. Security management programs   3. The determination of requirements for the design, specification, and installation   4. Identification of adequate resources including staffing levels   5. Identification of training needs and skills   6. Development of operational controls   7. The organization’s overall threat and risk management framework? * Is the organization’s methodology for risk identification and assessment:   1. Defined with respect to its scope, nature, and timing, to ensure that it is proactive rather than reactive   2. Include a collection of information related to security threats and risks   3. Provide for the classification of threats and risks and identification of those that are to be avoided, eliminated, or controlled   4. Provide for the monitoring of actions to ensure effectiveness and the timeliness of their implementation? * Has the organization established, implemented, and maintained a procedure:   1. To identify and have access to the applicable legal requirements and other requirements to which the organization subscribes related to its security threat and risks   2. To determine how these requirements apply to its security threats and risks? * Does the organization have documented security management objectives, and do they take into account:   1. Legal, statutory, and other security regulatory requirements   2. Security-related threats and risks   3. Technological and other options   4. Financial, operational, and business requirements   5. Views of appropriate stakeholders? * Are the security objectives:   1. Consistent with the organization’s commitment to continual improvement   2. Quantified (where practicable)   3. Communicated to all relevant employees and third parties, including contractors, with the intent that these persons are made aware of their personal obligations   4. Reviewed periodically to ensure that they remain relevant and consistent with the security management policy. Where necessary the security management objectives shall be amended accordingly. * Are security management targets established, implemented, and maintained, and are they:   1. To an appropriate level of detail   2. Specific, measurable, achievable, relevant and time-based (where practicable)   3. Communicated to all relevant employees and third parties including contractors with the intent that these persons are made aware of their individual obligations   4. Reviewed periodically to ensure that they remain relevant and consistent with the security management objectives, and amended accordingly? * Are there security management programs established for achieving the organization’s objectives and targets, and are they optimized and prioritized, and do they describe:   1. Designated authority and responsibility for achieving objectives and targets   2. The means and time scale by which the objectives and targets will be achieved, and are they reviewed/amended periodically to ensure that they remain effective?  OBSERVATION: YES/NO FINDING: YES/NO ***AUDITOR COMMENTS (If Any) (Attach additional pages if required)***  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **ITEM 4.4: IMPLEMENTATION & OPERATION**  **4.4.1 Structure, authority, and responsibility for security management**   * Has the organization established and maintained an organizational structure of roles, responsibilities, and authorities, consistent with the achievement of its security management policy, objectives, targets, and programs, and are these defined, documented, and communicated to responsible individuals? * Does top management provide evidence of its commitment to development of the security management system and improving its effectiveness by:  1. Appointing a member of top management who, irrespective of other responsibilities is responsible for the design, maintenance, documentation and improvement of the security management system 2. Appointing members of management with the necessary authority to ensure that the objectives and targets are implemented 3. Identifying and monitoring the requirements and expectations of the organization’s stakeholders and taking appropriate action to manage these expectations 4. Ensuring the availability of adequate resources 5. Communicating to the organization the importance of meeting its security management requirements in order to comply with its policy 6. Ensuring any security programs generated from other parts of the organization complement the security management system 7. Communicating to the organization the importance of meeting its security management requirements in order to comply with its policy 8. Ensuring security-related threats and risks are evaluated and included in organizational threat and risk assessments as appropriate 9. Ensuring the viability of the security management objectives, targets, and programs?  OBSERVATION: YES/NO FINDING: YES/NO ***AUDITOR COMMENTS (If Any) (Attach additional pages if required)***  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **4.4.2 Competence, training, and awareness**   * Does the organization ensure that personnel responsible for the design, operation, and management of security equipment and processes are suitably qualified in terms of education, training and/or experience, and has the organization established and maintained procedures for making persons working for it or on its behalf aware of:   1. The importance of compliance with the security management policy and procedures, and to the requirements of the security management system   2. Their roles and responsibilities in achieving compliance with the security management policy and procedures and with the requirements of the security management system, including emergency preparedness and response requirements   3. The potential consequences to the organization’s security by departing from specified operating procedures?      1. **Communication** * Does the organization have procedures for ensuring that pertinent security management information is communicated to and from relevant employees, contractors, and stakeholders? * Is proper consideration given to the sensitivity of security-related information?   **4.4.4 Documentation**   * Has the organization established a security management documentation system that includes but is not limited to the following:  1. The security policy, objectives, and targets 2. Description of the security management system scope 3. Description of the main elements of the security management system and their interaction, and reference to related documents 4. Documents, including records, required by this International Standard 5. Documents including records determined by the organization to be necessary to ensure the effective planning, operation and control of processes that relate to its significant security threats and risks    * 1. **Document and data control**  * Has the organization established and maintained procedures for controlling all documents, data, and information required by Clause 4 of this International Standard to ensure that:  1. These documents, data and information can be located and accessed only by authorized individuals 2. These documents, data, and information are periodically reviewed, revised as necessary, and approved for adequacy by authorized personnel 3. Current versions of relevant documents, data, and information are available at all locations where operations essential to the effective functioning of the security management system are performed 4. Obsolete documents, data, and information are promptly removed from all points of issue and points of use, or otherwise assured against unintended use 5. Archival documents, data, and information retained for legal or knowledge preservation purposes or both are suitably identified 6. These documents, data, and information are secure, and if in electronic form are adequately backed up and can be recovered?  OBSERVATION: YES/NO FINDING: YES/NO ***AUDITOR COMMENTS (If Any) (Attach additional pages if required)***  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**   * + 1. **Operational control** * Has the organization identified operations that are necessary for achieving:  1. Its security management policy 2. The control of activities and mitigation of threats identified as having significant risk 3. Compliance with legal, statutory and other regulatory security requirements 4. The security management objectives 5. The delivery of its security management programs 6. The required level of supply chain security  * Has the organization ensured that these operations and activities are carried out under specified conditions by:  1. Establishing, implementing, and maintaining documented procedures to control situations where their absence could lead to failure to achieve the operations and activities listed above 2. Evaluating any threats posed from upstream supply chain activities and applying controls to mitigate these impacts to the organization and other downstream supply chain operators 3. Establishing and maintaining the requirements for goods or services which impact on security and communicating these to suppliers and contractors?  * Where existing designs, installations, operations, etc., are revised, do the revisions include:   1. Revised organizational structure, roles or responsibilities   2. Revised security management policy, objectives, targets, or programs   3. Revised processes or procedures   4. The introduction of new infrastructure, security equipment or technology, which may include hardware and/or software   5. The introduction of new contractors, suppliers or personnel, as appropriate?      1. **Emergency preparedness, response and security recovery** * Has the organization established, implemented, and maintained appropriate plans and procedures to identify the potential for and responses to, security incidents and emergency situations, and for preventing and mitigating the likely consequences associated with them? * Do the plans and procedures include information on the provision of maintenance of any identified, facilities or services that can be required during or after incidents or emergency situations? * Does the organization periodically review the effectiveness of its emergency preparedness, response and security recovery plans and procedures, in particular after the occurrence of incidents or emergency situations caused by security breaches and threats, and are these procedures periodically tested (as applicable)?  OBSERVATION: YES/NO FINDING: YES/NO ***AUDITOR COMMENTS (If Any) (Attach additional pages if required)***  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **4.5: CHECKING AND CORRECTIVE ACTION**   * + 1. **Security performance measurement and monitoring** * Has the organization established and maintained procedures to monitor and measure the performance of its security management system, and does it consider associated threats, risks, including potential deterioration of mechanisms and their consequences, and do these procedures provide for:   1. Both qualitative and quantitative measurements, appropriate to the needs of the organization   2. Monitoring the extent to which the organization’s security management policy, objectives, and targets are met   3. Proactive measures of performance that monitor compliance with the security management programs, operational control criteria and applicable legislation, statutory and other security regulatory requirements   4. Reactive measures of performance to monitor security-related deteriorations, failures, incidents, non-conformances and other historical evidence of deficient security management system performance   5. Recording data and results of monitoring and measurement sufficient to facilitate subsequent corrective and preventive action analysis, and if monitoring equipment is needed are there maintenance and calibration procedures, and are records of calibration kept?      1. **System evaluation** * Does the organization evaluate security management plans, procedures, and capabilities through periodic reviews, testing, post-incident reports, lessons learned, performance evaluations, and exercises, and are significant changes in these factors reflected immediately in the procedures? * Does the organization periodically evaluate compliance with relevant legislation and regulations, industry best practices, and conformance with its own policy and objectives? * Are records kept of the results of these periodic evaluations?   **4.5.3 Security-related failures, incidents, non-conformance and corrective and preventive actions**   * Has the organization established, implemented, and maintained procedures for defining responsibility and authority for:   1. Evaluating and initiating preventive actions to identify potential failures of security in order that they may be prevented from occurring   2. The investigation of security-related      + 1. Failures, including near misses and false alarms        2. Incidents and emergency situations        3. Non-conformances   3. Taking action to mitigate any consequences arising from such failures, incidents, and non-conformances   4. The initiation and completion of corrective actions   5. The confirmation of the effectiveness of corrective actions taken? * Are all proposed corrective and preventive actions reviewed through the security threat and risk assessment process prior to implementation? * Are corrective and preventive actions taken appropriate for the magnitude of the problems and commensurate with the security management-related risks and threats likely to be encountered?   + 1. **Control of records** * Has the organization established and maintained records as necessary to demonstrate conformity to the requirements of its security management system and of this International Standard, and the results achieved? * Has the organization established, implemented, and maintained procedures for the identification, storage, protection, retrieval, retention, and disposal of records? * Are the records legible, identifiable, and traceable? * Are electronic and digital documentation rendered tamper-proof, securely backed-up, and accessible only by authorized personnel?   **4.5. 5 Audit**   * Has the organization established, implemented, and maintained a security management audit program and does it ensure that audits of the security management system are carried out at planned intervals, in order to:   1. Determine whether or not the security management system:      1. Conforms to planned arrangements for security management including the requirements of the whole of Clause 4 of this specification      2. Has been properly implemented and maintained      3. Is effective in meeting the organization’s security management policies and objectives   2. Review the results of previous audits and the actions taken to rectify non-conformances   3. Provide information on the results of audits to management   4. Verify that the security equipment and personnel are appropriately deployed? * Is the audit schedule based on the results of threat and risk assessments of the organization’s activities, and the results of previous audits, and do the audit procedures cover the scope frequency, methodologies, and competencies, as well as the responsibilities and requirements for conducting audits and reporting results, and are audits, where possible, conducted by personnel independent of those having direct responsibility for the activity being examined?  OBSERVATION: YES/NO FINDING: YES/NO ***AUDITOR COMMENTS (If Any) (Attach additional pages if required)***  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **ITEM 4.6: MANAGEMENT REVIEW AND CONTINUAL IMPROVEMENT**   * Does top management review the organization’s security management system at planned intervals, to ensure its continuing suitability, adequacy, and effectiveness, and do reviews include assessing opportunities for improvement and the need for changes to the security management system, including security policy and security objectives and threats and risks. Records of the management reviews shall be retained. * Do inputs to management reviews include:   1. Results of audits and evaluations of compliance with legal requirements and with other requirements to which the organization subscribes   2. Communication from external interested parties, including complaints   3. The security performance of the organization   4. The extent to which objectives and targets have been met   5. Status of corrective and preventive actions   6. Follow-up actions from previous management reviews   7. Changing circumstances, including developments in legal and other requirements related to its security aspects   8. Recommendations for improvement? * Do outputs from management reviews include any decisions and actions related to possible changes to security policy, objectives, targets, and other elements of the security management system, consistent with the commitment to continual improvement?   , OBSERVATION: YES/NO FINDING: YES/NO ***AUDITOR COMMENTS (If Any) (Attach additional pages if required)***  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
|  |

**RECOMMENDATIONS & REQUIRED ACTION**

Lead Auditor: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Responsible Manager: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Responsible Head of Department: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Org. Development: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Management Review: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Required Action(s): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Completion Time: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Implementation Follow-up:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Auditor:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## APPENDIX SIX: SUMMARY OF KEY PERFORMANCE INDICATORS

Here are additional metrics from which to build an effective program of internal auditing, and, in turn, benchmarking, gap analysis, and risk management.

**Operational metrics**

* Throughput
* Throughput as a percent of capacity
* Defects as a percent of throughput
* Number of order deliveries past due
* Rush order percent
* On-time delivery percent
* Customer satisfaction rating
* Number of complaints
* Number of complaints to revenue
* Returns as a percent of units delivered
* Number of manual journal vouchers/entries per employee
* Ration of support staff to number of employees
* Days of inventory outstanding
* Inventory turns
* Market share
* Number of outstanding audit issues
* Book to bill ration
* Days sales outstanding
* Overtime percent
* Days without workplace injury
* Number of hours that production is off-line
* Personnel/material requisitions open past threshold or benchmark

**Exception Reporting**

* Audit reports
* Assets assigned to employees in excess of threshold or benchmark
* Unauthorized system access attempts
* General ledger accounts without assigned owners
* Assets without assigned owners
* Un-reconciled accounts
* Inventory aged over threshold
* Wires/checks issued over $ threshold
* Deliveries overdue/past-due over threshold
* Sales to unapproved customers
* Sales to customers over established limits
* Was or suspense accounts (or other accounts that should have a zero balance) that still have a balance
* Unavailable materials report
* Inventory count differences
* Purchase orders aged over threshold
* Unmatched receipts
* Unsigned management representation of financial results

**Financial Metrics**

* Cost per unit
* Revenue per full time equivalent
* Employee expenses headcount
* Accounts receivable turnover
* Write-offs as a percent of sales
* Reserves as a percent of assets
* Reserves as a percent of accounts receivable over 90 days past due
* Budget to actual variances
* Value at risk
* Market value to contract value of financial interests
* Un-reconciled accounts exposure
* Accounts payable aging
* Financial costs as a percent of revenue
* Margin percent
* Regulatory capital charges
* Working capital
* Interest coverage
* Sales, general and administrative expenses as a percent of revenue
* Earnings per share
* Risk-adjusted return on capital
* Debt/equity trend

**Monitoring**

* Internal threat analysis of competitor-controlled incidents
* Evaluation of proposed or pending legislation effects on current operations
* Periodic threat analysis of extremist groups on current operations
* Camera surveillance of key areas to identify illegal activity.

**NOTES:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

***About the Author***

******

***Eugene A. (Gene) Razzetti retired from the U.S. Navy as a Captain in 1992. Since then, he has been an international management consultant, project manager, and auditor, working with Quality, Environmental, and Security Management Systems, primarily in the maritime industries.***

***For six years after 9-11, he was a Military Analyst. He co-authored MVO 8000, the Corporate Responsibility Management Standard that is contained in his first book.***

***He is published in a number of professional journals dealing with ethics, auditing, and strategic planning, and is an adjunct lecturer in Management at the undergraduate and graduate levels with two universities.***

1. The terms “company” and “organization” are synonymous for the purposes of this checklist. [↑](#footnote-ref-1)