

CYBER SECURITY MANAGEMENT SYSTEM AUDIT CHECKLIST (Version 1.0)

Notes:

Primatch grants a non-exclusive license at no cost to companies who wish to use this checklist to assist in assessing their own internal cyber security programs. The use of this checklist for other purposes is prohibited.

Primatch makes no warranties, express or implied, for this checklist and accepts no liabilities for its use.

This checklist is based on a management system that combines the requirements of ISO 17799, BS 7799:2 and ISA SP99 into a single management system using the ISO management system model (ISO 9000/14000/18000). In addition, the ISO model has been modified to integrate the management of all sureties within a single system. Improvements have also been made in the ISO model itself.

ISO 17799 is a code of practice for information security and focuses on controls. BS 7799:2 is a specification for an information security management system that incorporates requirements from ISO 17799. However, both documents have omissions and can be improved in a variety of ways. Modifications are also needed to extend their content to cyber security for manufacturing and control systems where cyber security must be defined more broadly than for business systems to include the range of malevents that could be perpetrated through access to a computer system. In order to encompass all types of threats, cyber security can be defined as the protection of computer systems from:

- C Cyber or physical attack by adversaries who wish to disable or manipulate them to cause harm.
- C Access by adversaries who want to obtain, corrupt, damage, destroy or prohibit access to valuable information (the confidentiality, integrity and availability of traditional IT security).

ISA SP99 overlaps with both BS 7799:2 and ISO 17799 (and references controls from ISO 17799). However, while it establishes a cyber security program for manufacturing and control systems, it does not utilize the framework of an ISO management system.

Each of these existing standards/practices contains areas not covered by the others (i.e. none of them is complete), and all of them have omissions from what is needed in a management system for cyber security. The improved management system used here remedies these problems.

The management system covers these stages in the life of the management system:

- C Establish
- C Implement
- C Operate
- C Maintain
- C Improve

Establishing the management system involves designing and developing it. Once developed it is ready for implementation. This stage includes working out bugs and smoothing its operation. Its normal operation follows. However, the management system will likely deteriorate if it is not maintained. It also needs to evolve with time and be continually improved.

The checklist below reflects requirements for each stage and element of this management system, including documents and records. Reviews and audits can be made against these requirements. For each element these questions should be asked:

- C Are the requirements met?
- C Are the documents prepared?
- C Are the records kept?

An enhanced annotated version of this checklist which includes objectives for each element, meanings and notes to enhance its usability and a correlation with other standards is available for a fee.

ESTABLISH THE MANAGEMENT SYSTEM

1.0 Leadership

1.1 Design and implementation team

Requirements:

- C Assemble a cross-organizational and cross-functional team of people with the capabilities and motivation to design and implement the MS.
- C Conduct design and implementation meetings.

Documents: List of design team members and their qualifications and roles.

Records:

- C Meeting attendance lists.
- C Meeting minutes.

1.2 Source of advice

Requirements: Identify and secure the services of one or more individuals who can provide specialist advice on the design, implementation and operation of the MS, as needed.

Documents: List of specialists and their contact information.

Records: None.

1.3 Business case

Requirements: Build a business case for the management system.

Documents: Business case.

Records: None.

1.4 Management forum

Requirements: Establish a forum of managers. Forum should:

- Review and approve the MS.
- Monitor and flag changes that may impact the MS.
- Conduct management reviews.
- Approve major initiatives to improve the MS.

Documents: List of forum members and their contact information.

Records:

- C Meeting attendance lists.
- C Meeting minutes.

1.5 Management commitment

Requirements: Evidence management commitment to managing MS sureties by:

- Ensuring a policy statement is developed.
- Ensuring all aspects of the MS life cycle are addressed.
- Ensuring roles and responsibilities are established.
- Communicating to the organization the importance of the management system.
- Providing sufficient resources for the proper execution of the management system throughout its life cycle.

- Conducting management reviews throughout the MS life cycle.

Documents: None.

Records: Records of communicating to the organization.

1.6 Ownership

Requirements:

- C Assign overall responsibility for the success of the MS throughout its life cycle to a single member of the executive management team.
- C Require regular reporting on the MS performance by the senior executive to the executive management team during management reviews.

Documents: None.

Records: Record of ownership.

2.0 Policy

2.1 Definitions of terms

Requirements: Provide definitions of key words and phrases to facilitate understanding of the MS. Provide definitions of the sureties addressed by the management system.

Documents: List of definitions.

Records: None.

2.2 Normative references

Requirements: List publications that are indispensable for the MS specifying publication dates and versions.

Documents: List of publications.

Records: None.

2.3 Informative references

Requirements: List publications that provide useful supporting information and include publication dates and versions.

Documents: List of publications.

Records: None.

2.4 Mandatory requirements

Requirements:

- C List applicable mandatory requirements according to the scope of the management system.
- C Identify modified or new mandatory requirements as they occur, update the list, and modify the MS, as appropriate.
- C Communicate relevant information to personnel and interested parties.

Documents: List of applicable mandatory requirements.

Records: None.

2.5 Expectations and views of stakeholders

Requirements: Identify the expectations and views of interested parties by consulting with them.

Documents: Summary of expectations and views.

Records: None.

2.6 Purpose and goals

Requirements:

- C Specify why the MS is needed and what it is intended to accomplish.
- C Address mandatory requirements and stakeholder expectations and views.

Documents: Statement of purpose and goals.

Records: None.

2.7 Scope

Requirements:

- C Specify the sureties, activities, locations, facilities, systems, equipment, etc. to be included.
- C Identify the processes to be included.
- C Determine the sequence and interaction of the processes.

Documents: Scope statement.

Records: None.

2.8 Overall policy statement

Requirements:

- C Define management intent and explain motivations.
- C State management commitment.
- C Incorporate the organization's values and the principles to which it subscribes.
- C Reflect the policy of any larger entity of which the organization is a part.
- C Address regulatory, legal, contractual and other mandatory requirements, and stakeholder expectations and views.
- C Include a commitment to continual improvement.
- C Define the organization's overall management system approach.
- C Require that the management system be developed in a risk management context.
- C Address balancing competing requirements in managing sureties, e.g. production versus safety, security, etc.
- C Set priorities for MS activities.
- C Specify an owner responsible for its review and maintenance.
- C Require periodic review and revision following a defined process to account for changing conditions and information, especially those that affect the basis of the previous risk assessment.
- C Provide references to supporting documents.
- C Approved by responsible management.
- C Endorsed by any larger entity of which the organization is a part.
- C Published in writing.
- C Communicated to appropriate personnel and interested parties in a form that is relevant, accessible and understandable.
- C Available to interested parties, as appropriate.

Documents: Policy statement.

Records: None.

2.9 Objectives and targets

Requirements:

- C Identify specific objectives and targets.
- C Consider mandatory requirements, stakeholder expectations and views, risks, technological options, and financial, operational and business requirements.
- C Be consistent with overall policy.

Documents: Statement of objectives and targets.

Records: None.

2.10 Roles and responsibilities

Requirements:

- C Define roles, responsibilities, authorities and accountabilities for achieving the objectives and targets with schedules.
- C Account for organizational interfaces when assigning roles and responsibilities.

Documents: Listing of roles and responsibilities and schedules.

Records: None.

2.11 Risk criteria

Requirements: Specify the risk acceptance criteria that will be used for the various types of risk covered by the MS.

Documents: Statement of risk criteria

Records: None.

2.12 Risk assessment approach

Requirements:

- C Identify a risk assessment method(s) that is suitable for the surety and the

- complexity of the processes involved.
- C Justify the selection of the method(s) considering the organization, activities and risks.
- C Use a risk assessment method that addresses:
- Proactive hazard identification.
 - Personnel required to conduct the risk assessment.
 - Identification of the study scope and includes:
 - Routine and non-routine activities.
 - Activities of all personnel in the workplace.
 - Facilities within the workplace, whether provided by the organization or others.
 - All stages in the life cycle of the organization's activities.
 - Equipment failures, failure of safeguards, human errors and human factors, utility failures, and external events.
 - Consistency with operating experience and the capabilities of risk control measures employed.
 - Consequences of incidents.
 - Identification of existing and needed risk control measures.
 - Classification and ranking of risks.
 - Documentation of the results and reports.
 - Establishing a system to promptly and effectively address findings and recommendations including:
 - Communicating with management on the risk results.
 - Resolving recommendations in a timely manner, documenting resolutions, and deciding on and documenting actions to be taken.
 - Communicating the rejection of recommendations by management to the risk assessors and resolving any responses.
 - Managing actions.
 - Considering interim measures when risks cannot be ameliorated promptly.
 - Communicating risk results and actions to be taken to affected personnel.
 - Retention of risk assessment results and resolutions of recommendations.
- C Provide guidelines for use in initial and periodic risk assessments.

Documents: Risk assessment guidelines.

Records: None.

3.0 Specification

3.1 Generic controls

3.1.1 Design and inherent surety

Requirements:

- C Incorporate security, safety, etc. controls into the design of new systems.
- C Incorporate inherent surety into designs.
- C Address facilities, processes, installations, equipment, the workplace
- C Address human factors in design.

Documents: Design documentation.

Records: None.

3.1.2 Personnel competency

3.1.2.1 Competencies needed to perform management system tasks

Requirements: Identify and document minimum competencies for all tasks performed as part of the management system.

Documents: List of competencies for tasks.

Records: None.

3.1.2.2 Screening personnel for competency

Requirements: Screen personnel to ensure personnel are selected who meet competency requirements.

Documents: None.

Records: Records of screening of personnel.

3.1.2.3 Personnel competency records

Requirements: Maintain records of education, training, skills, experience and qualifications of personnel who work are assigned responsibilities defined in the management system.

Documents: None.

Records: Competency records.

3.1.2.4 Initial training of personnel in management system tasks

Requirements: Establish a program to train personnel in tasks required by the management system before they perform the tasks that addresses:

- Identification of tasks and personnel for training.
- Identification of the subjects to be covered, and the goals and objectives of the training.
- Expression in clear, measurable terms of the learning goals or objectives.
- Basing the number of hours, frequency and content of training on the complexity of the operation, risks involved, and the experience and required skill level of the personnel
- Description of the important actions and conditions under which personnel will demonstrate competence or knowledge.
- Explanation of roles and responsibilities.
- Description of what is acceptable performance.
- Following procedures.
- Communicating the consequences of not following procedures and the importance and benefits of following them.
- Differing levels of responsibility, ability, literacy and risk.
- Using, if necessary, languages other than English for training.
- Development of methods for training evaluation.
- Periodic evaluation of the effectiveness of the training to see if personnel understand and implement the training.
- Modification of the content and frequency of training, and re-training of personnel, as needed, when training is found not to be effective.
- Consultation of both trainers and organization's personnel on training needs and how best to improve training.
- Modification of the training program as needed.
- Confirmation that all covered personnel have received and understood the training.
- Maintenance of records that contain the identities of the employee and trainer, the date of training, and the means used to verify that the employee understood the training.
- Use of training log and tracking system to manage personnel training.
- Inclusion of contractors and others who may be assigned management system responsibilities.

Documents:

- C Initial training program.
- C Initial training materials.

Records:

- C Initial training log.
- C Initial training records for personnel.
- C Initial qualification records for personnel.
- C Initial training evaluation records.
- C Personnel consultation records.
- C Training program evaluation records.
- C Records of modifications to the initial training program.

3.1.2.5 Refresher training of personnel in management system tasks

Requirements:

- C Establish a program to provide refresher training to personnel in tasks required by the management system that addresses the same items as initial training.
- C Base the frequency of refresher training on the likelihood and consequences of deviations from task requirements.
- C Consult personnel on frequency of refresher training.

Documents:

- C Refresher training program.
- C Refresher training materials.

Records:

- C Refresher training log.
- C Refresher training records for personnel.
- C Refresher qualification records for personnel.
- C Refresher training evaluation records.
- C Personnel consultation records.
- C Training program evaluation records.
- C Records of modifications to the refresher training program.

3.1.2.6 Personnel awareness

Requirements: Brief personnel on the management system, its requirements, the importance of conformance, and their role in ensuring its success.

Documents: Briefing materials.

Records: Briefing attendance lists.

3.1.3 Personnel management

3.1.3.1 Job responsibilities

Requirements:

- C Incorporate both general and specific management system responsibilities into job descriptions.
- C Communicate job responsibilities to personnel.

Documents: None

Records: Job descriptions.

3.1.3.2 Employment contracts

Requirements:

- C Specify personnel management system responsibilities in the terms and conditions of employment.
- C Address survivability of terms and conditions on termination and their applicability based on the location of work performance.

Documents: Specimen contract.

Records: Completed contracts.

3.1.3.3 Performance goals

Requirements: Set individual performance goals based on management system requirements.

Documents: None.

Records: Performance goals for individuals.

3.1.3.4 Supervision and accountability

Requirements: Provide supervision of personnel in executing their management system responsibilities and hold them accountable for performance according to their responsibilities and goals.

Documents: None.

Records: Performance evaluations.

3.1.3.5 Disciplinary process

Requirements:

- C Provide a formal process for appropriately disciplining personnel who violate management system requirements.
- C Comply with legal requirements and collective bargaining agreements.

Documents: None.

Records:

- C Notice of disciplinary action.
- C Record of disciplinary action.

3.1.4 Personnel involvement

Requirements: Establish a personnel involvement program that addresses:

- Consultation with personnel on the development and implementation of the management system.
- Involvement of personnel broadly and actively with the management system.
- Proactive communication of management system information to personnel.
- Provision of personnel with appropriate, prompt and ready access to information.
- Inclusion of third parties.

Documents: Personnel involvement program.

Records: Records of personnel participation.

3.1.5 Communications

Requirements:

- C Establish procedures for:
 - Internal communications and exchanges of management system information.
 - Receiving, documenting and responding to relevant communications and

- exchanges from external interested parties.
 - Necessary communications with public authorities on incident planning and response.
 - Informing personnel and interested parties of communications procedures.
- C Address:
- Communicating relevant procedures and requirements to suppliers, contractors and customers.

Documents: Communications procedures.

Records: Records of communications.

3.1.6 Information management

Requirements: Establish an information management program that addresses:

- Identification of information to be included.
- Levels of detail to be provided.
- How it is to be collected.
- Who is responsible for collection.
- Who is responsible for maintenance.
- Where it will be stored.
- Schedule for collection/updating.
- How it will be made available to personnel.
- Retention requirements.
- Provision of a tracking log that provides a description, the date last updated, and its location.
- Compilation of information before it is needed by the management system.

Documents: Information management program.

Records:

- C Tracking log.
- C Information records for the surety being managed.

3.1.7 Risk management

3.1.7.1 Periodic risk assessment

Requirements:

- C Periodically update and revalidate the risk assessment using a procedure that

addresses:

- Frequency or circumstances for updates and revalidations.
 - Risk assessment methods to be used.
 - Correcting omissions and deficiencies in the previous risk assessment.
 - Process changes.
 - Accuracy and completeness of information used.
- C Use the risk assessment results to provide input to the rest of the management system including operating and maintenance procedures, personnel training, facility requirements, etc.

Documents: Risk assessment revalidation and update procedure.

Records:

- C Log of risk assessments.
- C Completed updates and revalidations.
- C Records showing disposition of findings and recommendations.
- C Records showing the communication of risk results to management and affected personnel.

3.1.7.2 Siting

Requirements:

- C Identify locations that must be protected.
- C Prepare a checklist of threats.
- C Review locations to identify possible threats.
- C Identify suitable corrective actions.
- C Manage corrective actions.

Documents

- C List of locations that must be protected.
- C Checklist of threats.

Records:

- C Records of reviews
- C Corrective action records.

3.1.7.3 Environmental threats

Requirements:

- C Identify assets that must be protected.
- C Prepare a checklist of environmental factors.
- C Review assets to identify possible threats.
- C Identify suitable corrective actions.
- C Implement corrective actions.

Documents:

- C List of assets that must be protected.
- C Checklist of environmental factors.

Records:

- C Records of reviews.
- C Corrective action records.

3.1.7.4 Utilities

Requirements:

- C Identify utilities that must be protected.
- C Prepare a checklist of events that may compromise utilities.
- C Review utilities to identify possible ways they may be compromised.
- C Identify suitable corrective actions.
- C Implement corrective actions.

Documents:

- C List of utilities that must be protected.
- C Checklist of events that may compromise utilities.

Records:

- C Records of reviews.
- C Corrective action records.

3.1.8 Operations management

3.1.8.1 Procedures

Requirements:

- C Establish a procedures program that:
- Identifies tasks that require procedures.
 - Addresses the entire life cycle of the organization's activities.
 - Establishes a common format, structure, organization and content for all procedures of the same type.
 - Requires use of best practices for writing procedures.
 - Provides guidelines for writing procedures.
 - Ensures procedures are consistent with information used to support the management system.
 - Provides procedures in languages other than English, as needed.
 - Involves procedure users in their development.
 - Distributes and communicates procedures to all users.
 - Makes procedures readily accessible by users.
 - Ensures procedures are implemented and used.
 - Requires reviews of procedures as often as necessary to assure they reflect current operations and any significant changes that have occurred.
 - Ensures old procedures do not stay in use after updating.
 - Requires updating procedures before changes are made.
 - Requires formal approval of modifications to procedures.
 - Maintains a record of modifications including the nature of the change and date.
 - Alerts operating personnel to a modification in a procedure before it is made.
 - Requires annual certification that they are current and accurate.
 - Requires the use of procedures in training personnel.
- C Requires procedures to:
- Provide an overview of the activity covered.
 - Identify precautions to be taken.
 - Provide specific instructions on steps to be taken to perform tasks.
 - Identify data to be recorded and samples to be collected.
 - Identify operating criteria and conditions to be maintained.
 - Specify ranges and limits for operating parameters
 - Identify the consequences of deviating from the procedures.
 - Address steps needed to avoid deviations.
 - Identify pertinent alarms and instruments if an upset occurs.
 - Identify actions to be taken in the event of upset conditions.
 - Identify and describe the purpose and functions of safeguards.

Documents:

- C Procedures program.
- C Guidelines for writing procedures.
- C Operating, maintenance and other procedures for all modes of operation.

Records:

- C Records generated by the use of procedures, e.g. completed checklists.
- C Evidence of the involvement of personnel in preparing procedures.
- C Annual reviews and certifications.
- C Record of modifications.
- C Records of notification of changes to users.
- C Records of providing initial and updated procedures to users.
- C Records of use of procedures in training.

3.1.8.2 Operator logs

Requirements:

- C Identify operations for which logs will be required.
- C Require operators to maintain a log of their activities. The log should address:
 - Starting and finishing times.
 - Actions taken.
 - Problems encountered and corrective actions taken.
 - Name of person making the entry.

Documents: None.

Records: Logs.

3.1.8.3 Pre-startup review

Requirements:

- C Establish a procedure that confirms prior to startup:
 - Design specifications have been met.
 - Procedures are in place and are adequate.
 - Risk assessment is up-to-date and recommendations have been resolved and implemented before startup.
 - Modifications meet management of change requirements.
 - Training of personnel has been completed.
 - Requirements of other management system elements have been addressed.
- C Prepare a checklist or form to use in pre-startup reviews.
- C Apply the procedure to new facilities and ones that have been significantly modified.

Documents:

- C Pre-startup review procedure.
- C Specimen pre-startup review checklist or form

Records: Completed pre-startup review checklists or forms.

3.1.8.4 Systems integrity

Requirements: Establish a program to maintain the on-going integrity of the organization's systems that addresses:

- Design, construction, installation, operation and maintenance of systems to minimize the risk of risk events.
- Identification of items covered by the program.
- Setting priorities for which systems and items require closer scrutiny than others.
- Compliance with vendor recommended service procedures and intervals.
- Development of configuration, calibration and maintenance procedures per procedures program (see ____).
- Preventive maintenance (inspection and testing), as appropriate that:
 - Follows recognized and generally accepted good engineering practices.
 - Is performed at a frequency consistent with manufacturer's recommendations and more frequently if determined to be necessary by prior operating experience.
 - Corrects deficiencies outside acceptable limits before further use, or in a safe and timely manner, when necessary means are taken to ensure safe operation.
- Training of personnel responsible for maintaining systems integrity per training program (see ____).
- Use of qualified and authorized personnel.
- Accounting for the organization's failure experience.
- Quality assurance for fabrication, installation, and spare parts and materials that helps ensure:
 - Item as fabricated is suitable for the process application for which it will be used.
 - Item is installed properly and consistent with design specifications and the manufacturers' instructions using appropriate checks and inspections.
 - Maintenance materials, and spare parts and equipment are suitable for the process application for which they will be used.

Documents:

- C Systems integrity program.
- C List of items covered by the program.
- C Vendor manuals.
- C Engineering and design records.

- C Equipment files.
- C Codes and standards.
- C Configuration procedures.
- C Calibration procedures.
- C Maintenance procedures.
- C Test and inspection procedures including frequencies.
- C Acceptability criteria for tests and inspections.
- C Records of actions taken when deficiencies were found as a result of tests/inspections.
- C Quality assurance procedures.
- C Maintenance procedures

Records:

- C List of covered items.
- C Fabrication records.
- C Maintenance work orders.
- C Service records.
- C Configuration records.
- C Calibration records.
- C Records of installation checks and inspections.
- C Test and inspection records that include :
 - C Date.
 - C Name of person.
 - C Identification of item tested.
 - C Test/inspection description.
 - C Test/inspection results.
- C Records of actions taken when deficiencies were found as a result of tests/inspections.
- C Failure rate data.
- C Purchase orders.
- C Records on materials and spare parts: spec sheets, parts numbers, store room logs.
- C Records per personnel training element.
- C Records per procedures element.

3.1.8.5 Special work and permits

Requirements:

- C Establish special work procedures for tasks with particular impacts on surety that:
 - Convey the risks associated with the tasks and necessary precautions to those performing the actual tasks.
 - Ensure operating personnel are cognizant of any special work.

- Inform operating personnel of the risks of the tasks.
 - Assure that control over these activities remains with operating personnel.
 - Maintain communication among operating personnel and personnel performing the special work.
 - On completion of work, inform operating personnel to provide job closure.
 - Comply with the requirements for procedures (see _____).
- C Consider using a permit system for all special work and develop suitable permits.
- C Maintain records relating to the performance of special work, e.g. completed permits.
- C Apply to both employees and third parties.

Documents:

- C Special work procedures.
- C Special work permits.

Records: Completed special work permits.

3.1.8.6 Management of change

Requirements: Establish a procedure to manage changes that addresses:

- Types of changes covered.
- Technical basis for the change.
- Evaluation of the impact of the change using risk-based methods prior to their implementation.
- Establishing a system to promptly and effectively address findings and recommendations similar to the system described for the risk assessment element.
- Prompt notification to affected personnel of the changes.
- Ongoing supplemental training of personnel for changes prior to their implementation.
- Consideration of any adverse impacts that may occur as a result of the change process itself.
- Updating procedures as a result of the change.
- Updating information and documents as a result of the change.
- Updating the management system as a result of the change.
- Keeping records of modifications made to the management system in response to changes.
- Schedule for implementing the change.
- Management approval of the proposed change.
- Verification that the change has been implemented correctly.
- Determination that the system functions correctly after the change has been made.

- Maintenance of a log of the changes made.
- Briefing of personnel on the management of change procedure.
- Considering distinguishing between major and minor changes and adjusting practices accordingly.
- Consideration of both temporary and permanent changes, and emergency changes.
- Establishing and monitoring a time limit for temporary changes.
- Ensuring the process is returned to its original or designed conditions at the end of a temporary change.
- Integration with other change management programs, as appropriate.

Documents: Management of change (MOC) procedure.

Records:

- C Change requests.
- C Records that show a sound technical basis for each change.
- C MOC reviews.
- C Records that show how the impact of the change was evaluated.
- C Records showing notification of personnel of changes.
- C Records showing supplemental training of personnel for changes prior to their implementation.
- C Records showing briefing of personnel on the management of change procedure.
- C Records showing updates to procedures, training, information and other parts of the management system.
- C Records of modifications made to the management system in response to changes.
- C Log of changes.

3.1.8.7 Third-party involvement

Requirements:

- C Establish a program for the involvement of third parties in the management system that addresses:
 - Identification of third parties covered by the program.
 - Requirements for compliance with the management system.
 - Use of contracts to define responsibilities.
 - Screening and hiring of qualified third parties using appropriate criteria.
 - Periodic evaluation of the performance of third parties using appropriate criteria.
 - Informing third parties of possible risk events.
 - Explanation of incident response plans.
 - Training of third parties equivalent to that for employees per ____, as

- applicable.
 - Control of entrance, presence, and exit of third parties to sensitive facilities.
 - Compliance with facility rules.
 - Advising the organization of any unique potential risk events presented or found by the third party's work.
- C Consider using a permit or work authorization system for third parties.
 - C Prepare and administer a questionnaire for third-party selection.
 - C Prepare and administer a checklist and guidance for third-party performance evaluation.
 - C Prepare and provide third-party briefings.

Documents:

- C Third-party surety program.
- C Evaluation criteria that will be used to evaluate the performance of prospective third parties.
- C Specimen contracts.
- C Questionnaire for third-party selection.
- C Checklist and guidance for third-party performance evaluation.
- C Third-party briefings.

Records:

- C List of covered third parties.
- C Records that show the application of performance evaluation criteria to screen and select third parties.
- C Completed contracts.
- C Third-party training records.
- C Records showing documents and briefings provided to third parties.
- C Records that show third party entry to, presence in, and exit from sensitive facilities are controlled.
- C Records that show the periodic evaluation of third-party performance on the job.
- C Records that show the action taken when third-party performance was found to be nonconforming.

3.1.8.8 Protection of trade secrets and intellectual property

Requirements:

- C Provide personnel with information necessary to comply with the management system without regard to its proprietary status.
- C Require employees and third parties to enter into confidentiality agreements to protect confidential or secret information, and intellectual property, as

- appropriate.
- C Review agreements whenever there are changes that may impact them, e.g. termination of an employee.

Documents: Specimen confidentiality agreements.

Records:

- C Completed confidentiality agreements.
- C Records regarding requests for and the provision of proprietary information.

3.1.9 Incident management

3.1.9.1 Reporting and investigation

Requirements:

- C Establish an incident reporting and investigation program that addresses:
 - Definition of types of incidents covered.
 - Procedures for prompt reporting of incidents.
 - Recognition of incidents.
 - Response procedures including consequence mitigation.
 - Investigation requirements and procedures.
 - Requirements for maintaining an audit trail.
 - Prompt investigation.
 - Time period for initiating an investigation.
 - Documentation and reporting requirements.
 - Report retention requirements.
 - Establishing a system to promptly and effectively address findings and recommendations similar to that used for risk assessment recommendations.
 - Learning from incidents.
 - Providing feedback to personnel who report incidents and other affected personnel.
 - Ensuring employees and contractors have access to reports and documentation on recommendations.
 - Briefing of personnel on the procedures.
 - Using results in subsequent risk assessments.
 - Maintenance of a log of incidents.

Documents: Incident reporting and investigation program and procedures.

Records:

- C Records showing briefing of personnel on the procedures.
- C Log of incidents.
- C Incident investigation reports that address at a minimum:
 - Date of the incident.
 - Date investigation began.
 - Description of the incident.
 - Factors that contributed to the incident.
 - Any recommendations resulting from the investigation.
- C Corrective action records.
- C Records showing briefing of personnel on incidents.
- C Records showing personnel access to reports and documentation on recommendations and corrective actions.

3.1.9.2 Response plan

Requirements: Establish an incident response plan that addresses:

- Types of incidents covered based on a risk assessment.
- Identification of potential incidents to include in the plan.
- Conditions for activation of the plan.
- Alarm system.
- Remediating the consequences of the event.
- Use of response equipment.
- Qualification and authorization of response personnel.
- Actions required for response and recovery.
- Liaison with outside organizations.
- Communication with the media.
- Periodic testing of the plan, as feasible.
- Learning from activations and tests of the plan including updating the plan.
- Periodic reviews and updates of the plan, including when organizational changes occur.
- Briefing and training of personnel.
- Inspection, testing and maintenance of response equipment.

Documents: Incident response plan.

Records:

- C Reports on activations of the plan.
- C Records on updates to the plan.
- C Records on briefing and training personnel on the plan.

3.1.9.3 Business continuity management

Requirements: Establish a contingency plan to deal with the range of credible risk events addressed by the management system. The plan must address:

- Risk events covered and their risks based on a risk assessment.
- Conditions for activation of the plan.
- Remediating the consequences of the event.
- Strategy and plans for continuation of business.
- Prioritization of critical processes for the organization.
- Restoration of systems within acceptable time periods.
- Coordination of actions with involved parties.
- Liaison with outside organizations.
- Communication with the media.
- Testing the plan.
- Learning from activations and tests of the plan.
- Updating the plan
- Updating the plan when organizational changes occur.
- Briefing and training of personnel.
- Insurance coverages.

Documents: Business continuity plan.

Records:

- C Reports on activations of the plan.
- C Records on updates to the plan.
- C Records on briefing and training personnel on the plan.
- C Insurance policies.

3.1.10 Audits and inspections

3.1.10.1 Audits

Requirements:

- C Establish an audit program that addresses:
 - Activities and areas to be considered.
 - Responsibilities for managing and conducting audits.
 - Status and importance of the items to be audited.
 - Results of previous audits.
 - Audit methods and procedures.
 - Audit criteria and compliance requirements.
 - Preparation of protocols and checklists.
 - Scope.
 - Frequency and schedule.

- Planning of audits.
 - Selection of qualified auditors.
 - Conduct of audits.
 - Recording audit results.
 - Use of metrics to provide comparisons and monitor trends.
 - Audit reports and reporting results.
 - Prioritizing and categorizing audit findings.
 - Communication of audit results.
 - Ensuring personnel have access to reports and documentation on recommendations.
 - Retention of audit reports and records.
 - Follow-up on audit results.
 - Establishing a system to promptly and effectively address findings and recommendations similar to the risk assessment element.
 - Management of corrective actions.
- C Conduct management system audits at planned intervals.
- C Consider documenting not only areas that require corrective actions but also where the management system is effective.

Documents:

- C Audit program.
- C Audit protocols and checklists.

Records:

- C Completed audits.
- C Corrective action records.

3.1.10.2 Inspections

Requirements:

- C Establish an inspection program that addresses:
- Identification of inspections required.
 - Specification of inspection schedules.
 - Provision of inspection procedures.
 - Follow-up on inspection results.
 - Corrective action management.
- C Conduct inspections according to the program.

Documents: Inspection plan.

Records:

- C Inspection records.
- C Corrective action records.

3.1.11 Coordination with other organizations

Requirements:

- C Develop means to exchange information.
- C Conduct information exchanges on a regular basis.
- C Appropriately modify the management system as a result of information received.
- C Establish control mechanisms to ensure sensitive or confidential information is not provided to unauthorized personnel.

Documents: None.

Records: Files on information received and actions taken.

3.2 Specific technological controls

Specific technological controls are addressed in an addendum at the end of this document.

3.3 Performance considerations

Requirements: Establish a procedure to conduct performance impact reviews.

Documents: Performance impact review procedure.

Records: Performance impact reviews.

3.4 Capacity planning

Requirements:

- C Monitor and project capacity demands.
- C Evaluate their potential impact on the management system.
- C Take anticipatory actions.

Documents: None.

Records:

- C Capacity demand projections.
- C Evaluation records.
- C Anticipatory action records.

3.5 Outreach

Requirements:

- C Support education and research that will promote the management of sureties, as applicable.
- C Work with others to resolve past problems with managing sureties, as applicable.
- C Assist in the development of responsible standards, laws, and regulations that address the management of sureties.
- C Encourage others to practice responsible management of sureties.

Documents: None.

Records: Records generated from outreach activities.

3.6 Continual improvement

3.6.1 Review risk levels and criteria

Requirements: Review the level of residual risk and acceptable risk in light of changes to the organization, its objectives and processes, technology, risks, external factors, etc.

Documents: None.

Records: Revised risk levels and criteria.

3.6.2 Preventive action

Requirements:

- C Investigate potential nonconformances.
- C Identify preventive actions.
- C Manage preventive actions.

Documents: None.

Records:

- C List of potential nonconformances
- C Preventive action records.

3.6.3 Monitor the management system and measure performance

Requirements:

- C Establish a procedure to monitor use of the management system, measure performance, and determine if the management system is working as intended.
- C Use qualitative and quantitative performance measures, as appropriate.
- C Employ both proactive and reactive performance measures.
- C Record data and results of monitoring and measurement sufficient to facilitate corrective and preventive action analysis.
- C Identify actions.
- C Manage actions.
- C Calibrate and maintain monitoring equipment according to the requirements of the systems integrity management system element.

Documents:

- C MS monitoring procedure.

Records:

- C Records of nonconformances discovered.
- C Corrective action records.

3.6.4 Management review of the management system

3.6.4.1 Schedule reviews

Requirements: Set a time, date, location and frequency for reviews.

Documents: Schedule of meetings.

Records: None.

3.6.4.2 Collect information

Requirements: Collect information on the management system operation, trends,

adequacy of the management system design, technological developments, pending corrective actions and changes, and resource needs.

Documents: None.

Records: Records on management system operation, trends, adequacy of the management system design, technological developments, pending corrective actions and changes, and resource needs.

3.6.4.3 Review information

3.6.4.3.1 Management system experience

Requirements:

- C Review and assess the management system effectiveness using experience with its operation taking into account the results of audits, incident investigations, and concerns, suggestions and feedback from interested parties.
- C Include the experience of other parts of the organization and, where possible, other organizations.

Documents: None.

Records: Results of reviews and assessments.

3.6.4.3.2 Trend analysis

Requirements: Analyze trends in review results to identify issues that may merit special attention or require alternative approaches to correct.

Documents: None.

Records: Trend analyses.

3.6.4.3.3 Management system design

Requirements:

- C Review the management system design to assess its continuing suitability, adequacy and effectiveness in light of changing circumstances, activities, products, services, conditions, information, etc.
- C Ensure the management system scope is still applicable.

Documents: None.

Records: Results of reviews and assessments.

3.6.4.3.4 Management system developments

Requirements: Review the management system with regard to management system approaches, risk assessment methods, controls, and other aspects of a management system that have not previously been used or that are newly developed or available.

Documents: None.

Records: Reports on reviews.

3.6.4.3.5 Pending corrective actions

Requirements:

- C Identify any planned management system corrective actions including items from the previous management reviews.
- C Consult records of incident investigations, risk assessments, change reviews, audits, inspections, etc.

Documents: None.

Records: List of pending corrective actions.

3.6.4.3.6 Pending changes

Requirements: Identify any pending changes that may affect the management system.

Documents: None.

Records: List of pending changes.

3.6.4.3.7 Resource needs

Requirements: Periodically determine if existing resource allocations for the

management system are sufficient.

Documents: None.

Records: Records of resource needs.

3.6.4.4 Corrective actions

Requirements:

- C Identify actions needed to correct nonconformances or improve the management system.
- C Manage corrective actions.

Documents: None.

Records:

- C List of corrective actions.
- C Corrective action records.

3.6.4.5 Document management review

Requirements:

- C Establish a review meeting agenda.
- C Prepare review meeting minutes.

Documents: Management review meeting agenda.

Records: Management review meeting minutes.

3.6.4.6 Communicate the review results

Requirements: Report on management system performance to interested parties, as appropriate.

Documents: None.

Records: Records of reporting.

3.7 Management of preventive and corrective actions

3.7.1 Implement actions

Requirements:

- C Develop a procedure that addresses:
 - Ensuring the causes of nonconformances have been addressed in formulating corrective actions.
 - Ensuring actions are considered by the management of change program.
 - Description of actions and an explanation of their basis.
 - Developing a documented schedule for actions.
 - Definition of responsibility and authority for actions.
 - Approval of actions.
 - Implementation of corrective actions.
 - Completion of actions as soon as possible.
 - Monitoring progress of action implementation.
 - Capturing dates on which actions were taken.
 - Documentation that actions have been taken.
 - Verification that actions have been taken.

- C Prepare a Corrective/Preventive Action Form.

Documents: Specimen Preventive Action Form.

Records: Completed Corrective/Preventive Action Forms.

3.7.2 Communicate the results

Requirements: Communicate the results of the reviews and corrective actions taken to appropriate personnel.

Documents: None.

Records: Records of communications.

3.7.3 Review corrective actions taken

Requirements: Review results of corrective action implementation and compare them with expectations.

Documents: None.

Records:

- C Review records.
- C Modifications to corrective actions.

3.8 Control of documents and records

3.8.1 Control of documents

Requirements: Establish a procedure to:

- Create documents.
- Approve documents for adequacy prior to issue.
- Review and update documents as necessary and re-approve them.
- Ensure documents are dated and changes are identified with the current revision status.
- Ensure the most recent versions of documents are used.
- Prevent the use of obsolescent or draft documents at all points of issue and points of use.
- Mark obsolescent documents, if they must be retained, so they are readily identified and assured against unintended use.
- Suitably identify archival documents and data retained for legal, knowledge preservation, or other purposes.
- Distinguish draft and final documents.
- Ensure documents of external origin are so identified.
- Control the distribution of documents.
- Ensure documents are available at all locations where they are needed.
- Identify, store, maintain and retrieve documents.
- Protect documents against damage, deterioration or loss.
- Ensure documents remain legible, readily identifiable and retrievable, available and are kept in an orderly manner.
- Control access to documents
- Set, record and comply with retention requirements for documents.
- Address the disposition of documents.

Documents:

- C Procedure for document management.
- C List of documents with retention requirements.

Records: Records of document updates.

3.8.2 Control of records

Requirements: Establish a procedure to:

- Ensure records are traceable to the management system element or activity to which they relate.
- Identify, store, maintain and retrieve records.
- Protect records against damage, deterioration or loss.
- Ensure records remain legible, readily identifiable and retrievable, available, traceable to the activities involved, and are kept in an orderly manner.
- Control access to records.
- Set, record and comply with retention requirements for records.
- Address the disposition of records.

Documents:

- C Procedure for records management.
- C List of records with retention requirements.

Records: None.

4.0 Resource allocation

Requirements:

- C Identify the resources needed for the management system.
- C Provide the resources needed by the management system.

Documents: None.

Records: None.

5.0 Review, documentation and approval

5.1 Independent review

Requirements: Conduct an independent review of the management system.

Documents: None.

Records:

- C Records of the review.
- C Corrective action records.

5.2 Document the management system

Requirements:

- C Document all management system elements.
- C Apply document control to management system documentation.

Documents: None.

Records: management system documentation.

5.3 Management approval

Requirements: Obtain formal approval of the management system design from responsible management.

Documents: None.

Records: Original documents approved by signatures, or equivalent if electronic documents are used.

6.0 Implementation plan for the management system

Requirements:

- C Decide on actions, schedules, priorities and resources needed.
- C Assign roles and responsibilities for implementation.

Documents: None.

Records: Implementation plan.

IMPLEMENT THE MANAGEMENT SYSTEM

7.0 Communicate the management system to personnel

Requirements:

C Brief those personnel involved with or affected by the management system.

Documents: None.

Records: Records of briefings.

8.0 Gap analysis

8.1 Define existing system

Requirements: Review existing management system elements and identify those that meet requirements of the management system design.

Documents: None.

Records: List of existing management system elements that will meet the management system design requirements.

8.2 Identify gaps

Requirements: Compare the management system design with existing management system elements and identify missing requirements.

Documents: None.

Records: List of management system requirements that must be implemented.

9.0 Risk assessment

9.1 Prioritize risk assessments

Requirements:

C Establish a procedure for prioritizing systems based on their criticality to the organization, history, and potential impacts of risk events.

C Set priorities.

Documents: Prioritization procedure.

Records: List of prioritized systems with rationale for prioritization.

9.2 Conduct initial risk assessments

Requirements:

- C Identify and assess the risks using the method selected with the guidelines established (see ____).

Documents: None.

Records:

- C Log of risk assessments.
- C Risk assessment reports.
- C Records showing disposition of findings and recommendations.
- C Records showing the communication of risk results to management and affected personnel.

10.0 Risk controls

10.1 Select risk controls

Requirements:

- C Identify treatment options for the risks identified in the initial risk assessment.
- C Refine the requirements for the generic and surety-specific controls.
- C Consider the impact on the system of all the controls taken together to avoid adverse synergistic impacts.

Documents: None.

Records: List of treatment options and controls selected.

10.2 Statement of Applicability

Requirements: Document the controls selected to manage the risks identified and the reasons for their selection. Also document the exclusion of any controls identified in codes or standards included in the design of the management system with reasons for their exclusion.

Documents: None.

Records: Statement of Applicability (SOA).

10.3 Specifications for controls

Requirements: Provide information on the performance requirements for the controls selected, as appropriate.

Documents: None.

Records: Specifications for controls.

10.4 Test and acceptance program for controls

Requirements:

- C Develop a test and acceptance program that addresses:
 - Types of tests.
 - Degree of testing and assurance.
 - Methods and procedures used.
 - Schedule and timing.
 - Application to all modes of system operation.
 - Test conditions.
 - Individual versus integrated tests.
 - Sufficiency of testing.
 - Separating development, test and operational facilities.
 - Vendor and third-party versus organization testing.
 - Production testing.
 - Formal acceptance of controls.
 - Documentation of tests and acceptance that includes:
 - Controls tested.
 - Versions or models of controls tested.
 - Dates and times of tests.
 - Test results.
 - Recommendations for addressing any problems identified and modifying the implementation plan.

Documents: Test and acceptance program.

Records: Test and acceptance records.

10.5 Implementation plan for controls

Requirements:

- C Decide on actions, schedules, priorities and resources needed.
- C Assign roles and responsibilities for implementation.

Documents: None.

Records: Implementation plan.

11.0 Management approval

Requirements: Obtain formal approval from responsible management of the residual risks, the controls selected and the implementation plan.

Documents: None.

Records: Original documents approved by signatures, or equivalent if electronic documents are used.

12.0 Establish individual policies, procedures and guidelines for controls

Requirements: Develop individual policies, procedures and guidelines for each of the controls to be implemented, as applicable.

Documents: None.

Records: Policies, procedures and guidelines.

13.0 Implement controls

13.1 Install controls

Requirements: Implement controls according to the plan.

Documents: None.

Records: Implementation records.

13.2 Validate operation of the controls

Requirements:

- C Ensure the installed controls meet these criteria:
 - Installed correctly.
 - Configured correctly.
 - Meet the specifications.
 - Accomplish their intended purpose.
- C Correct deviations.
- C Modify the management system if needed.

Documents: None.

Records: Validation records.

14.0 Endorse the management system

Requirements:

- C Confirm the management system is appropriate in light of the validation of controls.

Documents: None.

Records:

- C Endorsement records.
- C Modification records.

OPERATE THE MANAGEMENT SYSTEM

Requirements: Operate all elements of the management system per individual elements.

Documents: Per individual elements.

Records: Per individual elements.

MAINTAIN THE MANAGEMENT SYSTEM

Requirements: Per individual elements.

Documents: Per individual elements.

Records: Per individual elements.

IMPROVE THE MANAGEMENT SYSTEM

Requirements:

- C Per individual elements.
- C Utilize source of special advice.

Documents: Per individual elements.

Records: Per individual elements.