ISO/IEC 27001
Information Security
Management System

Self-assessment questionnaire

How ready are you for ISO/IEC 27001:2005?

This document has been designed to assess your company's readiness for an ISO/IEC 27001 Information Security Management System. By completing this questionnaire your results will allow you to self-assess your organization and identify where you are in the ISO/IEC 27001 process. If you would like us to do this analysis for you, please complete the questionnaire (including your contact details), save and email it to us at info.indonesia@bsigroup.com

Information provided will not be disclosed and will be destroyed immediately after use. Please mark your answers ✓ **for Yes** and **leave blank for No**. To order a copy of ISO/IEC 27001:2005 please visit www.bsigroup.com/en-ID/

Contact: .... Job title: ....

Company: .... No. of employees: ....

Address: .... Town: ....

County: .... Postcode: ....

Telephone (*inc. dialing code*): .... Email: ....

1. Planning

Has the scope and boundaries of the Information Security Management System (ISMS) been defined, justifying any exclusions from this scope?

Is there an approved information security policy that includes a framework for setting objectives, takes into account contractual, legal and regulatory requirements, aligns with the information security risks to the business and establishes the criteria for risk evaluation?

Has an appropriate and repeatable risk assessment method and the acceptable levels of risk been defined and documented?

Have the assets within the scope of the ISMS and their owners been defined? Have the threats and vulnerabilities, along with the resulting impacts for the loss of confidentiality, integrity and availability to the assets been identified?

Has the business impact for loss of confidentiality, integrity and availability, and the likelihood of security failures, been analysed and evaluated, taking into account security controls that are currently implemented?

Have the levels of risk been estimated and determined as being within the acceptable level or requiring risk treatment?

Have options for risk treatment been identified and evaluated?

Have security controls been determined and implemented to meet the requirements identified in the risk assessment and risk treatment processes (see section 7)?

Has management approval been given for the implementation of the ISMS and for the residual risk levels?

Is there a Statement of Applicability showing which controls from ISO/IEC 27001 Annex A have been selected, the reasons for selection or non-selection, and the status of implementation?

Continued >>

bsi.

...making excellence a habit.™

2. Implementation and operation

Is there a risk treatment plan that identifies actions, resources and funding, as well as responsibilities and priorities for managing information security risks?

Has the risk treatment plan and the identified security controls been implemented?

Have the measures been defined for the effectiveness of controls?

Has a training and awareness programme been implemented?

Is the operation of the ISMS and the required resources being managed?

Have controls that enable prompt detection and response to security events been implemented?

3. Monitor and review

Are there monitoring and reviewing activities or processes to detect processing errors, attempted or successful security breaches, performance of people and/or technology, prevention of security events and to determine whether actions taken are effective?

Are regular reviews of effectiveness undertaken using the results of audits, incidents, measurements and feedback from interested parties?

Are risk assessments, residual risks and acceptable levels of risk reviewed at planned intervals, taking into account any changes to the organization or its business activities, the threats and vulnerabilities it faces and external events such as legal or contractual changes?

Are internal ISMS audits conducted at planned intervals according to defined schedules and procedures, and are results reported and timely effective action taken to resolve identified findings?

Are management reviews of the ISMS undertaken at planned intervals to determine its continued suitability and effectiveness?

4. Maintain and improve

Are improvements identified, implemented and evaluated to ensure they meet the intended objectives?

Are appropriate corrective and preventive actions identified and implemented, applying the lessons learned from both internal and external sources?

5. Documents and records

Are the documents and records related to the management system managed and controlled according to defined procedures?

6. Management commitment

Is there evidence that management provide commitment to the ISMS, such as establishing its policy and objectives and communicating the importance of meeting these objectives to the organization?

Are the required resources to establish, implement, operate, monitor, review and improve the ISMS determined and provided, and are responsibilities defined?

Do personnel with assigned ISMS responsibilities have the required competence and training to perform their duties?

Are all relevant personnel aware of their information security activities and how these contribute to meeting the objectives?

7. Security control examples

This section lists examples of security controls that you may have selected as applicable during your risk assessment and risk treatment processes.

Do you have confidentiality and/or non-disclosure agreements within your conditions of employment and contracts with suppliers?

Do you have contact with external authorities, special interest groups and/or any independent review of your information security arrangements?

Have you identified information security risks from external parties and are security requirements addressed in contracts or agreements?

Do you have an inventory of your organizational assets, with defined ownership and rules for acceptable use?

Do you have information classification guidelines and procedures for labelling and handling based on the classification scheme?

Do you perform background verification checks of all candidates for employment – in accordance with relevant regulations and in proportion to business requirements?

Is there a disciplinary process for employees who have committed a security breach?

Are responsibilities for performing employment changes or termination clearly defined, and are assets returned and access rights removed or adjusted?

Is there a secure physical security perimeter and entry controls on facilities, offices and security sensitive areas, including delivery and loading access points?

Have you implemented protection against external and environmental threats and is equipment sited to reduce associated risks?

Is equipment protected against failure of supporting utilities and are cables protected from damage or interception?

Is equipment adequately maintained and tested to ensure continued availability and integrity of operation?

Is security applied to equipment being removed from or operated off premises, and is equipment subject to secure disposal or re-use?

Do you have documented operating procedures and are changes controlled?

Have you implemented segregation of duties for tasks that may have security implications?

Are development, test and operational facilities separated to reduce the risk of unauthorised access to operational systems?

Are the security requirements for services delivered by third parties covered by a formal agreement and are they monitored, reviewed and under appropriate change management based on the levels of risk?

Is capacity management in place to enable forecasts of future requirements and to ensure system performance?

Are acceptance criteria defined for new and changed systems and are tests carried out during development and prior to acceptance?

Have you implemented controls to detect, prevent and recover from malicious code, and implemented associated awareness procedures?

Do you take regular backups of information and software, and are backups tested regularly in accordance with an agreed backup policy?

Continued >>

Are networks managed and controlled in order to protect from threats and maintain security for systems and application, and is there an agreement in place to maintain these security requirements?

Is removable media managed according to procedures which include handling, transport and storage?

Are formal exchange policies in place for any exchange of information and software with third parties?

Are procedures in place to protect information associated with interconnecting business systems, including electronic messaging?

Are controls implemented to protect electronic commerce, online transactions and publicly available information?

Are audit logs of user activities, system events and system administration activities produced, retained and protected against tampering?

Are fault logs and systems monitored, regularly reviewed and actions taken?

Is there an access control policy based on business and security requirements?

Is there a formal user registration procedure, and management of privileges and passwords and a regular review of access rights?

Are users required to follow good security practice for passwords and unattended equipment and facilities?

Is there a policy on the use of network services and has good practice been implemented to protect networks and connection of equipment?

Is access to operating systems controlled by secure log on procedures, are users uniquely identified and is use of system utilities restricted?

Is there a formal policy, security measures and procedures covering mobile computing and/or teleworking?

Are security requirements for new and changed information systems formally defined?

Is the correct processing of applications assured by validation of data input and output, processing controls and integrity checks?

Is there a policy for use of cryptographic controls and is cryptographic key management in place?

Are there controls in place for the installation of software and is system test data carefully selected and controlled?

Are change control procedures in place for application software and is source code protected?

Is there a technical review of business critical applications following upgrades to operating systems?

Is outsourced software development supervised and monitored?

Are security events and weaknesses reported and recorded to enable an orderly response and subsequent learning to be identified and implemented?

Have the security aspects of business continuity been considered and are there tested and up to date plans for maintaining and restoring operations and availability of information?

Have all relevant legal, statutory and contractual requirements been identified and the approach to maintaining currency and continued compliance defined?

Is compliance with security policies, standards and technical compliance of information systems subject to regular checks, and is access to any information system audit tools restricted and controlled?

For BSI to complete the analysis on your behalf, please click the submit button below or email a saved copy of your completed questionnaire to:
certification.sales@bsigroup.com

Save Submit

+6221 8379 3174 - 77
bsigroup.com/en-ID/

ISO/IEC 27001 Information Security Management