

Information Security
Management Toolkit Download



Language: **English**

Show prices in: **Euro**

The Information Security Management Toolkit

Unit Price: EUR 97.12
Total: EUR 97.12
 Inc. price 19% sales tax/VAT is EUR 97.12; EUR 114.45
 EUR 115.57

Delivery: Download

File Size: Full version: 13.3 MB

Download Time: Full version
 • SSL: <1 min.
 • DSL/Cable (1.9/16MB): <2' <1' <1 min.

[Buy now!](#)

This toolkit provides a wide variety of resources to boost your understanding and ability to implement Information Security Management in your organization with 30 ready-to-use resources.

The toolkit is designed to provide a guiding hand to assist you in improving your knowledge and understanding of Information Security Management by offering easy to use templates, blueprints, and documents that can be adapted to your organization's requirements.

Buy with confidence, the Information Security Management toolkit has a 100% Satisfaction Guarantee & Free Returns.

List Price \$123.33 Get it now for just \$99.0! Save \$24.33 (20%)

Put together by The Art of Service's industry experts and providing ready to use documents, this valuable kit takes the reader beyond the theoretical to focus on the real benefits and deliverables of Information Security Management and how to apply them successfully within an organization.

This invaluable set of documents and ready-to-use templates will provide you with a head start for both learning and applying of a Information Security Management approach that meets today's standards. It is ideal for professionals who don't have the time or resources at hand to develop the required templates and structure for implementation.

The Complete Information Security Management Toolkit includes the following 30 resources:

1. File: Security Service Requirement.doc - Summary: Scope for the requirements document may be determined by the business, therefore covering only a select few of the Services provided by the IT department that are seen as critical to the support of the business processes. Wordcount: 1216
2. File: 02 Service Management Plan.doc - Summary: It is necessary to identify the service management processes developed to support service delivery, their purposes, and how they relate to each other and the other components (policies, tools, and controls) of the service management system. Wordcount: 2056
3. File: 04 Service Management Process Definitions and Interfaces.doc - Summary: Roles associated with requests for change to assess and manage the impact on services continuity and availability. Wordcount: 3140
4. File: 03 Availability Plan.doc - Summary: Accidental changes often occur when the machine is touched for legitimate reasons, like an update, but the machine is not left in a workable state, usually because the change has not been fully planned, tested, or the procedures for the change have not been completed as documented. Wordcount: 2324
5. File: 10 Incident Management Policy.doc - Summary: To empower you in the creation process, this document provides some background information regarding the subject area, including considerations to be addressed within the policy itself. However, this is a policy policy and should reflect the goals, objectives, and getting priorities of your organization. Wordcount: 2174
6. File: 01 Information Security Policy.doc - Summary: Contractual Documentation/Preparing Terms and Conditions of Employment Using Non-Disclosure Agreements (Staff and Third Party) Misuse of Organization Stationery Lending Keys to Secure Areas to Others Lending Money to Work Colleagues Complying with Information Security Policy Establishing Ownership of Intellectual Property Rights Employing/Contracting New Staff Contracting with External Suppliers/Other Service Providers Employee's Responsibility to Protect Confidentiality of Data/Confidential Personal Data/Respecting Privacy in the Workplace Handling Confidential Employee Information Caring Referring on Staff Checking Staff Security Clearance Sharing Employee Information with Other Employees Sharing Personal Salary Information/Personal Information Security Responsibilities/Use of Internet in an Acceptable Way Keeping Passwords/PIN Numbers Confidential Sharing Organization Information with Other Employees Signing for the Delivery of Goods Signing for Work done by Third Parties Ordering Goods and Services Verifying Financial Claims and Invoices Approving and Authorization of Expenditure Responding to Telephone Enquiries Sharing Confidential Information with Family Members Grouping and Distributing Information Spreading Information through the Office 'Crane View' Using E-Mail and Postal Mail Facilities for Personal Reasons Using Telephone Systems for Personal Reasons Using the Organization's Mobile Phones for Personal Use Using Organization's Credit Cards/Playing Games on Office Computers Using Office Computers for Personal Use/HR Management/Dealing with Qualified Staff Taking Official Notes of Employee Meetings/Staff Leaving Employment/Handling Staff Resignations Complying Procedures for Terminating Staff or Contractors Obligations of Staff Transferring to Competitor/HR Issues/Other/Recommending Professional Advisors. Wordcount: 3245
7. File: 02 Security Service Requirement.doc - Summary: The purpose of this document is to provide the client with a structure for gathering pertinent information regarding Security Requirements. Wordcount: 1577
8. File: 03 Security Audit Template.doc - Summary: Your use of this system constitutes your further agreement that you will not use the system in any way that would violate any law, or that would be inconsistent with any Company policy or standard including policies on Ethics, Harassment, Conflict of Interest, and standards for system security. Wordcount: 2211
9. File: 02 Service Desk Process.doc - Summary: For instance, if the Service Desk is required to provide the customer or end user with status on their existing incident/request and the record has been established to in-line support, updates from the technician are required. Wordcount: 2933
10. File: 00 Service Desk-Introduction.doc - Summary: Ability to match end user's concerns/request with similar/past concerns/requests. For incident/problems, the tool is commonly called a Known Error Database and will allow the Service Desk Analyst to search symptoms to identify pre-defined workarounds and resources to address the end users concerns. Wordcount: 2398
11. File: 00 General Improvement Practices.doc - Summary: A project may be halfway complete, a service may be available for half the desired customers, a process update may be in testing before it is published, an incident may be within 2 hours of its agreed resolution time, these are all examples of progress in meeting requirements. Wordcount: 2388
12. File: ISO 27000 Presentation.ppt - Summary: ISO/IEC 17799 is a code of practice, not a suitable basis for an Wordcount: 824
13. File: Roles and Responsibilities.doc - Summary: If Event Management activities are delegated to the Service Desk or IT Operations Management, Technical and Application Management must ensure that the staff are adequately trained and that they have access to the appropriate tools to enable them to perform these tasks. Wordcount: 1189
14. File: Service Desk Fact Sheet.doc - Summary: The Objective for ITSM is to support the overall Business Continuity Management process by ensuring that the required IT technical and services facilities (including computer systems, networks, applications, telecommunications, technical support and Service Desk) can be recovered within required, and agreed, business timescales. Wordcount: 4113
15. File: Service Operation Functions Fact Sheet.doc - Summary: As the custodian of technical knowledge and expertise related to managing the IT infrastructure, the Technical Management function provides detailed technical skills and resources needed to support the ongoing operation of the IT infrastructure. Wordcount: 1627
16. File: Service Operation Processes Fact Sheet.doc - Summary: As soon as the diagnosis is complete, and particularly where a workaround has been found (even though it may not be a permanent resolution), a Known Error Record must be raised and placed in the KEDB so if further incidents or problems arise, they can be identified and the service restored more quickly. Wordcount: 3945
17. File: TAGS ISO 27001 Fact Sheet.doc - Summary: The ISO 27000-series information security management standards align with other ISO management systems standard, such as those for ISO 9001 (quality management systems) and ISO 14001 (environmental management systems), both in terms of their general structure and in the nature of combining 'best practice' with certification standards. Wordcount: 829
18. File: TAGS ISO 20000 Fact Sheet.doc - Summary: JAS-ANZ AND the person is individually qualified as an authorized ISO auditor AND has passed the ISO 20000 certification exam that is sat at the end of an external auditors course in ISO 20000. Wordcount: 729
19. File: ITSM Tool Requirements Document.doc - Summary: The knowledge management database should be able to be updated with workaround and solution information that has been captured in the incident and Problem records. Wordcount: 9177
20. File: Service Catalogue Management.pdf - Summary: Document Technical Service Catalogue information Develop self-help capabilities for documentation within the Service Catalogue. Wordcount: 561
21. File: Information Security Management Presentation.ppt - Summary: Lack of commitment from the business to the ISM processes and procedures. Wordcount: 956
22. File: Security Management: Roles & Responsibilities.doc - Summary: Developing and maintaining the Information Security Policy and a supporting set of specific policies, ensuring appropriate authorization, commitment and endorsement from senior IT and business management. Wordcount: 243
23. File: Toolkit Introduction Presentation - Information Security Management.ppt - Summary: Aid your understanding of the important issues to be addressed when making Information Security Management decisions, as well as the factors to be considered in successfully implementing the Information Security Management process. Wordcount: 160
24. File: ISO 20000 FAQs.doc - Summary: ISO 9000 is applied and used by all organizations in different sectors and industries and whilst it has certain attributes and benefits it is not suitable to your existing commercial relationships, you should consider whether you will have a specific certificate for the IT Service Management (ITSM) component of your business. Wordcount: 3065
25. File: ISO IEC 20000 Presentation Chapters 6-10.ppt - Summary: All accounting practices used should be aligned to the wider accounting practices of the whole of the service provider's organization. Wordcount: 1080
26. File: Management Commitment & Co-ordination Presentation.ppt - Summary: A good report should include metrics that show the effectiveness, speed and predictability of a process to enable the audience to assess how well the process has been implemented. Wordcount: 2546
27. File: Process Summary - Information Security Management.doc - Summary: Arrangements that involve external organizations having access to information systems and services should be based on a formal agreement that defines all necessary security requirements. Wordcount: 350
28. File: 02 Help Desk Process.doc - Summary: The intent of investigation and diagnosis at the Help Desk as a practice is obtaining enough information about the situation to determine the cause of the incident and make a determination if the incident can be resolved at the Help Desk or should be escalated to an in-line support team. Wordcount: 2927
29. File: 00 Help Desk-Introduction.doc - Summary: Ability to resolve incidents or fulfil requests. From remote access to systems to password reset tool, the ability of the Help Desk to address the end users' concerns/requests are often dependent on the Help Desk's access to useful monitoring and management tools within the service environment. Wordcount: 2314
30. File: Service_Design_Capability_Assessment_Overview.doc - Summary: While the focal point of Capacity Management is to ensure adequate performance and capacity of IT services are being developed and already delivered, there are many supporting elements including IT components, product and software licenses, physical assets, human resources and third party products that will all need to be managed appropriately for the goal to be achieved. Wordcount: 8918

The toolkit includes a variety of electronic documents that provide a head start for the implementation, education and awareness for Information Security Management.

The kit is designed for those who need or are looking for awareness or skills, but simply don't have time to develop the necessary templates and structure for the implementation.

The kit serves to act as a starting point. It will give you a clear path to travel. It is designed to be a valuable source of information and activities.

The Information Security Management toolkit:

1. Contains 30 ready to use documents covering the Preparing, Planning, Designing, Implementing, Operating and Optimizing of Information Security Management
2. Is suitable in any size and type of project or organization
3. Provides blueprints, templates and documents - ready to download and apply
4. Saves you time and budget

Buy with confidence, the Information Security Management toolkit has a 100% Satisfaction Guarantee & Free Returns.

List Price \$123.33 Get it now for just \$99.0! Save \$24.33 (20%)

[Back](#)

Digital River GmbH (Share & Vice) is the seller of the products in your shopping cart and your contractual partner.

[Login/Notice](#) [Privacy Statement](#) [Cookies](#) [Terms and Conditions](#)

Copyright © 2018 Share & Vice



Verified Security Certificate

Management Toolkit

This toolkit provides a wide variety of resources to boost your understanding and ability to implement Information Security Management in your organization with 30 ready-to-use resources.

This toolkit is designed to provide a guiding hand to assist you in improving your knowledge and understanding of Information Security Management by offering easy to use templates, blueprints, and documents that can be adapted to your organization's requirements.

Buy with confidence, the Information Security Management toolkit has a 100% Satisfaction Guarantee & Free Returns.

List Price \$183.33 Get it now for just \$99.0 ! Save \$84.33 (46%)

Put together by The Art of Service's industry experts and providing ready to use documents, this valuable kit takes the reader beyond the theoretical to focus on the real benefits and deliverables of Information Security Management and how to apply them successfully within an organization.

This innovative set of documents and ready-to-use templates will provide you with a head start for both learning and applying of a Information Security Management approach that meets today's standards. It is tailor-fit for professionals who don't have the time or resources at hand to develop the required templates and structure for implementation.

The Complete Information Security Management Toolkit Includes the following 30 resources:

1.File: Security Service Requirement.doc – Summary: Scope for the requirements document may be determined by the business, therefore covering only a select few of the Services provided by the IT department that are seen as critical to the support of the business processes. Wordcount: 1216

2.File: 02 Service Management Plan.doc – Summary: It is necessary to identify the service management processes developed to support service delivery, their purposes, and how they relate to each other and the other components (policies,

tools, and controls) of the service management system.

Wordcount: 2056

3.File: 04 Service Management Process Definitions and Interfaces.doc – Summary: □Risks associated with requests for change: to assess and manage the impact on service continuity and availability Wordcount: 3140

4.File: 03 Availability Plan.doc – Summary: Accidental changes often occur when the machine is touched for legitimate reasons, like an update, but the machine is not kept in a workable state; usually because the change has not be fully planned, tested, or the procedures for the change have not been completed as documented. Wordcount: 2324

5.File: 10 Incident Management Policy.doc – Summary: To empower you in the creation process, this document provides some background information regarding the subject area, including considerations to be addressed within the policy itself; however, this is your policy and should reflect the goals, objectives, and guiding principles of your organization. Wordcount: 2374

6.File: 01 Information Security Policy.doc – Summary: □
Contractual Documentation Preparing Terms and Conditions of Employment Using Non-Disclosure Agreements (Staff and Third Party) Misuse of Organization Stationery Lending Keys to Secure Areas to Others Lending Money to Work Colleagues Complying with Information Security Policy Establishing Ownership of Intellectual Property Rights Employing/Contracting New Staff Contracting with External Suppliers/other Service Providers Employees' Responsibility to Protect Confidentiality of Data Confidential Personnel Data Respecting Privacy in the Workplace Handling Confidential Employee Information Giving References on Staff Checking Staff Security Clearance Sharing Employee Information with Other Employees Sharing Personal Salary Information Personnel Information Security Responsibilities Using the Internet in an Acceptable Way Keeping Passwords/PIN Numbers Confidential Sharing Organization Information with Other Employees Signing for the Delivery of Goods Signing for Work done by Third

Parties Ordering Goods and Services Verifying Financial Claims and Invoices Approving and Authorization of Expenditure Responding to Telephone Enquiries Sharing Confidential Information with Family Members Gossiping and Disclosing Information Spreading Information through the Office 'Grape Vine' Using E-Mail and Postal Mail Facilities for Personal Reasons Using Telephone Systems for Personal Reasons Using the Organization's Mobile Phones for Personal Use Using Organization Credit Cards Playing Games on Office Computers Using Office Computers for Personal Use HR Management Dealing with Disaffected Staff Taking Official Notes of Employee Meetings Staff Leaving Employment Handling Staff Resignations Completing Procedures for Terminating Staff or Contractors Obligations of Staff Transferring to Competitors HR Issues Other Recommending Professional Advisors Wordcount: 3245

7.File: 02 Security Service Requirement.doc – Summary: The purpose of this document is to provide the <> with a structure for gathering pertinent information regarding Security Requirements.Wordcount: 1577

8.File: 03 Security Audit Template.doc – Summary: Your use of this system constitutes your further agreement that you will not use the system in any way that would violate any law, or that would be inconsistent with any Company policy or standard including policies on Ethics, Harassment, Conflict of Interest, and standards for system security. Wordcount: 3211

9.File: 02 Service Desk-Process.doc – Summary: For instance, if the Service Desk is required to provide the customer or end user with status on their existing incident/request and the record has been escalated to n-line support, updates from the technician are required. Wordcount: 2933

10.File: 00 Service Desk-Introduction.docx – Summary: Ability to match end user's concern/request with similar/past concerns/requests For incident/problems, the tool is commonly called a Known Error Database and will allow the Service Desk analyst to search symptoms to identify pre-defined workarounds and resolutions to address the end users concerns. Wordcount: 2384

11.File: 09 General Improvement Plan.docx – Summary: A project may be halfway complete, a service may be available for half the desired customers, a process update may be in editing before it is published, an incident may be within 2 hours of its agreed resolution time. These are all examples of progress in meeting requirements. Wordcount: 2388

12.File: ISO 27000 Presentation.ppt – Summary: ISO/IEC 17799 is a code of practice, not a suitable basis for an Wordcount: 824

13.File: Roles and Responsibilities.doc – Summary: If Event Management activities are delegated to the Service Desk or IT Operations Management, Technical and Application Management must ensure that the staff are adequately trained and that they have access to the appropriate tools to enable them to perform these tasks. Wordcount: 1189

14.File: Service Design Fact Sheet.doc – Summary: The Objective for ITSCM is to support the overall Business Continuity Management process by ensuring that the required IT technical and services facilities (including computer systems, networks, applications, telecommunications, technical support and Service Desk) can be recovered within required, and agreed, business timescales. Wordcount: 4113

15.File: Service Operation Functions Fact Sheet.doc – Summary: As the custodian of technical knowledge and expertise related to managing the IT Infrastructure, the Technical Management function provides detailed technical skills and resources needed to support the ongoing operation of the IT Infrastructure. Wordcount: 1627

16.File: Service Operation Processes Fact Sheet.doc – Summary: As soon as the diagnosis is complete, and particularly where a workaround has been found (even though it may not be a permanent resolution), a Known Error Record must be raised and placed in the KEDB. So if further incidents or problems arise, they can be identified and the service restored more quickly. Wordcount: 3946

17.File: TA05 ISO 27001 Fact Sheet.doc – Summary: The ISO 27000-series information security management standards align

with other ISO management systems standard, such as those for ISO 9001 (quality management systems) and ISO 14001 (environmental management systems), both in terms of their general structure and in the nature of combining best practice with certification standards. Wordcount: 829

18.File: TAOS i ISO 20000 Fact Sheet.doc – Summary: JAS- ANZ) AND the person is individually qualified as an authorized ISO auditor AND has passed the ISO 20000 certification exam that is sat at the end of an external auditors course in ISO 20000. Wordcount: 729

19.File: ITSM Tool Requirements Document.doc – Summary: □The knowledge management database should be able to be updated with work around and solution information that has been captured in the Incident and Problem records. Wordcount: 9177

20.File: Service Catalogue Management.pdf – Summary: Document Technical Service Catalogue information Develop self-help capabilities for documentation within the Service Catalogue Wordcount: 561

21.File: Information Security Management Presentation.ppt – Summary: Lack of commitment from the business to the ISM processes and procedures Wordcount: 956

22.File: Security Management- Roles & Responsibilities.doc – Summary: Developing and maintaining the Information Security Policy and a supporting set of specific policies, ensuring appropriate authorization, commitment and endorsement from senior IT and business management. Wordcount: 283

23.File: Toolkit Introduction Presentation – Information Security Management.ppt – Summary: Aid your understanding of the important issues to be addressed when making Information Security Management decisions, as well as the factors to be considered in successfully implementing the Information Security Management process. Wordcount: 160

24.File: ISO 20000 FAQ's.doc – Summary: ISO 9000 is applied and used by all organisations in different sectors and industries and whilst it has certain attributes and benefits that are valuable to your existing commercial relationship, you should consider whether you wish to have a specific

certification for the IT Service Management (ITSM) component of your business. Wordcount: 3065

25.File: ISO IEC 20000 Presentation Chapters 6-10.ppt – Summary: All accounting practices used should be aligned to the wider accountancy practices of the whole of the service provider's organization. Wordcount: 1080

26.File: Management Commitment & Co-ordination Presentation.ppt – Summary: A good report should include metrics that show the effectiveness, speed and predictability of a process to enable the audience to assess how well the process has been implemented. Wordcount: 2546

27.File: Process Summary – Information Security Management.doc – Summary: Arrangements that involve external organizations having access to information systems and services shall be based on a formal agreement that defines all necessary security requirements. Wordcount: 350

28.File: 02 Help Desk-Process.doc – Summary: The intent of investigation and diagnosis at the Help Desk as a practice is obtaining enough information about the situation to determine the cause of the incident and make a determination if the incident can be resolved at the Help Desk or should be escalated to an n-line support team. Wordcount: 2927

29.File: 00 Help Desk-Introduction.doc – Summary: Ability to resolve incidents or fulfill requests From remote access to systems to password reset tools, the ability of the Help Desk to address the end users' concerns/requests are often dependent on the Help Desk's access to useful monitoring and management tools within the service environment. Wordcount: 2384

30.File:

Service_Design_Capability_Assessment_Questionnaire.docx – Summary: While the focal point of Capacity Management is to ensure adequate performance and capacity of IT services are being developed and already delivered, there are many supporting elements including IT components, product and software licenses, physical sites, human resources and third party products that will all need to be managed appropriately

for this goal to be achieved. Wordcount: 8816

This toolkit includes a variety of electronic documents that provide a head start for the implementation, education and awareness for Information Security Management.

The kit is designed for those who need or are looking for awareness or skills, but simply don't have time to develop the necessary templates and structure for the implementation.

The kit serves to act as a starting point. It will give you a clear path to travel. It is designed to be a valuable source of information and activities.

The Information Security Management toolkit:

1. Contains 30 ready to use documents covering the Preparing, Planning, Designing, Implementing, Operating and Optimizing of Information Security Management
2. Is scalable to any size and type of project or organization
3. Provides blueprints, templates and documents – ready to download and apply
4. Saves you time and budget

Buy with confidence, the Information Security Management toolkit has a 100% Satisfaction Guarantee & Free Returns.

List Price \$183.33 Get it now for just \$99.0 ! Save \$84.33 (46%)

Unit Price: EUR 97.12

Total: EUR 97.12

Info plus 19% sales tax/VAT to EUR 97.12: EUR 18.45

EUR 115.57

Delivery: Download

File Size: Full version: 13.3 MB

Download Time: Full version

56k: ~31 min.

DSL/Cable (1/8/16Mbit): ~2 / <1 / <1 min.

[Click Here To Get It Now >>](#)

Tags: [information security management](#), [security management toolkit](#), [Information Security Policy](#), [Security Service Requirement.doc](#), [service management](#), [Wordcount](#), [Summary](#), [Security Management approach](#), [Service Management Process](#), [Information Personnel Information](#), [Complete Information Security](#), [Information Spreading Information](#), [Service Management Plan.doc](#), [Information Security Policy.doc](#), [Security Management process](#), [Service Desk](#), [security management standards](#), [Security Management Presentation.ppt](#), [Service Catalogue information](#), [Information Security Management.ppt](#), [Security Management- Roles](#), [Security Management decisions](#), [Information Security Management.doc](#), [Service Catalogue Wordcount](#), [ISO management systems](#), [Sharing Organization Information](#), [Incident Management Policy.doc](#), [Fact Sheet.doc](#), [Sharing Employee Information](#), [Staff Security Clearance](#), [Sharing Confidential Information](#), [Continuity Management process](#), [Technical Management function](#), [Confidential Employee Information](#), [quality management systems](#), [environmental management systems](#), [HR Management Dealing](#), [Event Management activities](#), [Security Policy Establishing](#), [knowledge management database](#), [Service Desk analyst](#), [Service Providers Employees](#), [Service Design Fact](#), [Service Operation Processes](#), [Professional Advisors Wordcount](#), [Security Audit Template.doc](#), [Service Operation Functions](#), [necessary security requirements](#), [Service Catalogue Management.pdf](#)