

## ISO IEC 27002 2005 (17799 2005) INFORMATION SECURITY AUDIT TOOL

7. ORGANIZATIONAL ASSET MANAGEMENT AUDIT	RESPONSES	NOTES AND COMMENTS
--	-----------	--------------------

7.1 ESTABLISH RESPONSIBILITY FOR ASSETS						
1	GOAL	Do you protect your organization's assets?	YES	NO	N/A	
2	GOAL	Do you use controls to protect your assets?	YES	NO	N/A	
3	GOAL	Do you account for your organization's assets?	YES	NO	N/A	
4	GOAL	Do you nominate owners for all organizational assets?	YES	NO	N/A	
5	GOAL	Do you make nominated owners responsible for protecting your organization's assets?	YES	NO	N/A	
6	GOAL	Do you assign responsibility for the maintenance of your organization's asset controls?	YES	NO	N/A	
7	GOAL	Do you make your asset owners responsible for protecting your organization's assets even though owners may have delegated the responsibility for implementing controls?	YES	NO	N/A	
7.1.1 COMPILE AN INVENTORY OF ORGANIZATIONAL ASSETS						
8	CTRL	Have you identified all organizational assets?	YES	NO	N/A	
9	CTRL	Have you compiled an inventory of all important assets?	YES	NO	N/A	
10	CTRL	Do you maintain an inventory of all important assets?	YES	NO	N/A	
11	GUIDE	Can your asset inventory be used to help your organization recover from disasters?	YES	NO	N/A	
12	GUIDE	Does your asset inventory gather all essential information about each of your assets?	YES	NO	N/A	
13	GUIDE	Does your asset inventory document the importance of each of your assets?	YES	NO	N/A	
14	GUIDE	Does your asset inventory assign a business value to each of your assets?	YES	NO	N/A	
15	GUIDE	Does your inventory identify asset types?	YES	NO	N/A	
16	GUIDE	Does your inventory specify asset formats?	YES	NO	N/A	
17	GUIDE	Does your inventory specify asset locations?	YES	NO	N/A	

ORGANIZATION:	YOUR LOCATION:	
COMPLETED BY:	DATE COMPLETED:	
REVIEWED BY:	DATE REVIEWED:	
SEPT 2007	COPYRIGHT © 2007 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.	EDITION 4.0
<b>PART 7</b>	<b>ORGANIZATIONAL ASSET MANAGEMENT AUDIT</b>	<b>PAGE 54</b>

## ISO IEC 27002 2005 (17799 2005) INFORMATION SECURITY AUDIT TOOL

7. ORGANIZATIONAL ASSET MANAGEMENT AUDIT	RESPONSES	NOTES AND COMMENTS
--	-----------	--------------------

18	GUIDE	Does your inventory provide license information?	YES	NO	N/A	
19	GUIDE	Does your inventory provide backup information?	YES	NO	N/A	
20	GUIDE	Does your inventory identify an owner for each asset ("owners" do not actually "own" the asset)?	YES	NO	N/A	
21	GUIDE	Does your asset inventory assign a security classification to each asset?	YES	NO	N/A	
22	GUIDE	Have you identified levels of protection for your assets?	YES	NO	N/A	
23	GUIDE	Have you assigned a level of protection to each asset?	YES	NO	N/A	
24	GUIDE	Do you provide a higher level of protection for your organization's most valuable and important assets?	YES	NO	N/A	
25	GUIDE	Do you provide a higher level of protection for assets that have a higher security classification?	YES	NO	N/A	
26	NOTE	Have you compiled an inventory of all information assets?	YES	NO	N/A	
27	NOTE	Have you compiled an inventory of databases and data files?	YES	NO	N/A	
28	NOTE	Have you compiled an inventory of contracts and agreements?	YES	NO	N/A	
29	NOTE	Have you compiled an inventory of system documentation?	YES	NO	N/A	
30	NOTE	Have you compiled an inventory of research information?	YES	NO	N/A	
31	NOTE	Have you compiled an inventory of training materials?	YES	NO	N/A	
32	NOTE	Have you compiled an inventory of user manuals?	YES	NO	N/A	
33	NOTE	Have you compiled an inventory of procedures?	YES	NO	N/A	
34	NOTE	Have you compiled an inventory of audit trails?	YES	NO	N/A	
35	NOTE	Have you compiled an inventory of business continuity plans?	YES	NO	N/A	
36	NOTE	Have you compiled an inventory of fallback arrangements?	YES	NO	N/A	
37	NOTE	Have you compiled an inventory of archived information?	YES	NO	N/A	
38	NOTE	Have you compiled an inventory of software assets?	YES	NO	N/A	

ORGANIZATION:	YOUR LOCATION:	
COMPLETED BY:	DATE COMPLETED:	
REVIEWED BY:	DATE REVIEWED:	
SEPT 2007	COPYRIGHT © 2007 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.	EDITION 4.0
<b>PART 7</b>	<b>ORGANIZATIONAL ASSET MANAGEMENT AUDIT</b>	<b>PAGE 55</b>

## ISO IEC 27002 2005 (17799 2005) INFORMATION SECURITY AUDIT TOOL

7. ORGANIZATIONAL ASSET MANAGEMENT AUDIT	RESPONSES	NOTES AND COMMENTS
--	-----------	--------------------

39	NOTE	Have you compiled an inventory of application software?	YES	NO	N/A	
40	NOTE	Have you compiled an inventory of system software?	YES	NO	N/A	
41	NOTE	Have you compiled an inventory of development tools?	YES	NO	N/A	
42	NOTE	Have you compiled an inventory of software utilities?	YES	NO	N/A	
43	NOTE	Have you compiled an inventory of physical assets?	YES	NO	N/A	
44	NOTE	Have you compiled an inventory of computer equipment?	YES	NO	N/A	
45	NOTE	Have you compiled an inventory of communications equipment?	YES	NO	N/A	
46	NOTE	Have you compiled an inventory of removable media?	YES	NO	N/A	
47	NOTE	Have you compiled an inventory of services?	YES	NO	N/A	
48	NOTE	Have you compiled an inventory of computing services?	YES	NO	N/A	
49	NOTE	Have you compiled an inventory of communication services?	YES	NO	N/A	
50	NOTE	Have you compiled an inventory of general utility services?	YES	NO	N/A	
51	NOTE	Have you compiled an inventory of heating services?	YES	NO	N/A	
52	NOTE	Have you compiled an inventory of lighting services?	YES	NO	N/A	
53	NOTE	Have you compiled an inventory of power services?	YES	NO	N/A	
54	NOTE	Have you compiled an inventory of air-conditioning services?	YES	NO	N/A	
55	NOTE	Have you compiled an inventory of personnel?	YES	NO	N/A	
56	NOTE	Does your personnel inventory list qualifications?	YES	NO	N/A	
57	NOTE	Does your personnel inventory list experience?	YES	NO	N/A	
58	NOTE	Does your personnel inventory list skills?	YES	NO	N/A	
59	NOTE	Have you compiled an inventory of intangible assets?	YES	NO	N/A	
60	NOTE	Do you use your asset inventories to support health and safety programs?	YES	NO	N/A	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	
SEPT 2007	COPYRIGHT © 2007 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.		EDITION 4.0
<b>PART 7</b>	<b>ORGANIZATIONAL ASSET MANAGEMENT AUDIT</b>		<b>PAGE 56</b>

## ISO IEC 27002 2005 (17799 2005) INFORMATION SECURITY AUDIT TOOL

7. ORGANIZATIONAL ASSET MANAGEMENT AUDIT	RESPONSES	NOTES AND COMMENTS
--	-----------	--------------------

61	NOTE	Do you use your asset inventories to support your organization's insurance programs?	YES	NO	N/A	
62	NOTE	Do you use your asset inventories to support your financial management activities?	YES	NO	N/A	
63	NOTE	Do you use your asset inventories to support your risk management activities?	YES	NO	N/A	

### 7.1.2 SELECT OWNERS FOR YOUR INFORMATION AND ASSETS

64	CTRL	Have you selected <i>owners</i> for your information assets (these "owners" do not legally "own" these assets)?	YES	NO	N/A	
65	CTRL	Have you selected <i>owners</i> for assets that are part of your organization's information processing facilities?	YES	NO	N/A	
66	CTRL	Are your asset owners formally responsible for controlling the production, development, maintenance, security, and use of the assets they officially "own"?	YES	NO	N/A	
67	GUIDE	Are your asset owners responsible for ensuring that information associated with information processing facilities is properly classified?	YES	NO	N/A	
68	GUIDE	Are your asset owners responsible for ensuring that assets associated with information processing facilities are properly classified?	YES	NO	N/A	
69	GUIDE	Are your asset owners responsible for defining access restrictions and ensuring that these restrictions are consistent with access control policies?	YES	NO	N/A	
70	GUIDE	Are your asset owners responsible for reviewing access restrictions and ensuring that these restrictions are consistent with access control policies?	YES	NO	N/A	
71	GUIDE	Are your asset owners responsible for defining access classifications and ensuring that these classifications are consistent with access control policies?	YES	NO	N/A	
72	GUIDE	Are your asset owners responsible for reviewing access classifications and ensuring that these classifications are consistent with access control policies?	YES	NO	N/A	
73	GUIDE	Have you assigned asset owners to business processes?	YES	NO	N/A	

ORGANIZATION:	YOUR LOCATION:	
COMPLETED BY:	DATE COMPLETED:	
REVIEWED BY:	DATE REVIEWED:	
SEPT 2007	COPYRIGHT © 2007 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.	EDITION 4.0
<b>PART 7</b>	<b>ORGANIZATIONAL ASSET MANAGEMENT AUDIT</b>	<b>PAGE 57</b>

## ISO IEC 27002 2005 (17799 2005) INFORMATION SECURITY AUDIT TOOL

7. ORGANIZATIONAL ASSET MANAGEMENT AUDIT	RESPONSES	NOTES AND COMMENTS
--	-----------	--------------------

74	GUIDE	Have you assigned asset owners to defined sets of activities?	YES	NO	N/A	
75	GUIDE	Have you assigned asset owners to specific applications?	YES	NO	N/A	
76	GUIDE	Have you assigned asset owners to defined sets of data?	YES	NO	N/A	
77	NOTE	Do asset owners retain responsibility for their assets even though others use these assets in their work?	YES	NO	N/A	
78	NOTE	Do service providers assume ownership of and are responsible for all of the assets used to deliver service?	YES	NO	N/A	

### 7.1.3 ESTABLISH ACCEPTABLE USE RULES FOR INFORMATION AND ASSETS

79	CTRL	Have you identified rules that define the acceptable use of information?	YES	NO	N/A	
80	CTRL	Have you documented rules that define the acceptable use of information?	YES	NO	N/A	
81	CTRL	Have you implemented rules that define the acceptable use of information?	YES	NO	N/A	
82	CTRL	Have you identified rules that define the acceptable use of assets associated with your information processing facilities?	YES	NO	N/A	
83	CTRL	Have you documented rules that define the acceptable use of assets associated with information processing facilities?	YES	NO	N/A	
84	CTRL	Have you implemented rules that define the acceptable use of assets associated with information processing facilities?	YES	NO	N/A	
85	GUIDE	Do all employees follow your acceptable use rules?	YES	NO	N/A	
86	GUIDE	Do all contractors follow your acceptable use rules?	YES	NO	N/A	
87	GUIDE	Do all third parties follow your acceptable use rules?	YES	NO	N/A	
88	GUIDE	Does everyone follow the rules that define how electronic mail should be used?	YES	NO	N/A	
89	GUIDE	Does everyone follow the rules that define how the Internet should be used?	YES	NO	N/A	
90	GUIDE	Does everyone follow the rules that define how mobile devices should be used?	YES	NO	N/A	

ORGANIZATION:	YOUR LOCATION:	
COMPLETED BY:	DATE COMPLETED:	
REVIEWED BY:	DATE REVIEWED:	
SEPT 2007	COPYRIGHT © 2007 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.	EDITION 4.0
<b>PART 7</b>	<b>ORGANIZATIONAL ASSET MANAGEMENT AUDIT</b>	<b>PAGE 58</b>

## ISO IEC 27002 2005 (17799 2005) INFORMATION SECURITY AUDIT TOOL

7. ORGANIZATIONAL ASSET MANAGEMENT AUDIT	RESPONSES	NOTES AND COMMENTS
--	-----------	--------------------

91	GUIDE	Does everyone follow the rules that define how mobile devices should be used outside of your premises?	YES	NO	N/A	
92	GUIDE	Do your organization's managers provide specific acceptable use guidance and advice?	YES	NO	N/A	
93	GUIDE	Are all employees aware of your organization's acceptable use rules, guidelines, and limits?	YES	NO	N/A	
94	GUIDE	Are all contractors aware of your organization's acceptable use rules, guidelines, and limits?	YES	NO	N/A	
95	GUIDE	Are all third-party users aware of your organization's acceptable use rules, guidelines, and limits?	YES	NO	N/A	
96	GUIDE	Are all employees responsible for their use of your organization's information processing resources?	YES	NO	N/A	
97	GUIDE	Are all contractors responsible for their use of your organization's information processing resources?	YES	NO	N/A	
98	GUIDE	Are all third parties responsible for their use of your organization's information processing resources?	YES	NO	N/A	

### 7.2 USE AN INFORMATION CLASSIFICATION SYSTEM

99	GOAL	Do you provide an appropriate level of protection for your organization's information?	YES	NO	N/A	
100	GOAL	Have you established an information classification system for your organization?	YES	NO	N/A	
101	GOAL	Do you use your classification system to define security levels?	YES	NO	N/A	
102	GOAL	Have you specified how much protection is expected at each level?	YES	NO	N/A	
103	GOAL	Have you assigned a security priority to each information security level?	YES	NO	N/A	
104	GOAL	Do you use your information classification system to specify how information should be protected at each level?	YES	NO	N/A	
105	GOAL	Do you use your information classification system to specify how information should be handled at each level?	YES	NO	N/A	

ORGANIZATION:	YOUR LOCATION:	
COMPLETED BY:	DATE COMPLETED:	
REVIEWED BY:	DATE REVIEWED:	
SEPT 2007	COPYRIGHT © 2007 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.	EDITION 4.0
<b>PART 7</b>	<b>ORGANIZATIONAL ASSET MANAGEMENT AUDIT</b>	<b>PAGE 59</b>

## ISO IEC 27002 2005 (17799 2005) INFORMATION SECURITY AUDIT TOOL

7. ORGANIZATIONAL ASSET MANAGEMENT AUDIT	RESPONSES	NOTES AND COMMENTS
--	-----------	--------------------

7.2.1 DEVELOP INFORMATION CLASSIFICATION GUIDELINES						
106	CTRL	Have you established information classification guidelines?	YES	NO	N/A	
107	CTRL	Do you classify information according to how sensitive it is?	YES	NO	N/A	
108	CTRL	Do you classify information according to how critical it is?	YES	NO	N/A	
109	CTRL	Do you classify your information according to how valuable it is to your organization?	YES	NO	N/A	
110	CTRL	Do you classify your information according to the kinds of legal requirements that must be met?	YES	NO	N/A	
111	GUIDE	Do your information classifications allow you to meet your business need to share information?	YES	NO	N/A	
112	GUIDE	Do your information classifications allow you to meet your business need to restrict access to information?	YES	NO	N/A	
113	GUIDE	Do your protective control methods allow you to meet your business need to share information?	YES	NO	N/A	
114	GUIDE	Do your protective control methods allow you to meet your business need to restrict access to information?	YES	NO	N/A	
115	GUIDE	Do your information classification guidelines specify how information should be classified initially?	YES	NO	N/A	
116	GUIDE	Do your information classification guidelines specify how information should be reclassified over time?	YES	NO	N/A	
117	GUIDE	Are your information classification guidelines consistent with your access control policy?	YES	NO	N/A	
118	GUIDE	Do you avoid the use of complex, cumbersome, and costly multicategory information classification systems?	YES	NO	N/A	
119	GUIDE	Have you given the responsibility for classifying information to the owner of that information?	YES	NO	N/A	
120	GUIDE	Are information owners responsible for ensuring that information is classified at the right level?	YES	NO	N/A	
121	GUIDE	Have you given the responsibility for periodically reviewing classifications to information owners?	YES	NO	N/A	

ORGANIZATION:	YOUR LOCATION:	
COMPLETED BY:	DATE COMPLETED:	
REVIEWED BY:	DATE REVIEWED:	
SEPT 2007	COPYRIGHT © 2007 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.	EDITION 4.0
<b>PART 7</b>	<b>ORGANIZATIONAL ASSET MANAGEMENT AUDIT</b>	<b>PAGE 60</b>

## ISO IEC 27002 2005 (17799 2005) INFORMATION SECURITY AUDIT TOOL

7. ORGANIZATIONAL ASSET MANAGEMENT AUDIT	RESPONSES	NOTES AND COMMENTS
--	-----------	--------------------

122	GUIDE	Are information owners responsible for ensuring that information classifications are up-to-date?	YES	NO	N/A	
123	GUIDE	Have you considered the possibility that information may become more sensitive and require more protection once large quantities are accumulated (aka the <i>aggregation effect</i> )?	YES	NO	N/A	
124	NOTE	Have you considered the possibility that information may become less sensitive or critical and require less protection over time?	YES	NO	N/A	
125	NOTE	Have you figured out what level of protection a piece of information must have by examining its confidentiality requirements?	YES	NO	N/A	
126	NOTE	Have you figured out what level of protection a piece of information must have by examining its availability requirements?	YES	NO	N/A	
127	NOTE	Have you figured out what level of protection a piece of information must have by examining its integrity requirements?	YES	NO	N/A	
128	NOTE	Have you figured out what level of protection documents must have by grouping documents with similar security requirements?	YES	NO	N/A	
129	NOTE	Do your information classifications specify how information should be handled and protected?	YES	NO	N/A	
<b>7.2.2 USE INFORMATION HANDLING AND LABELING PROCEDURES</b>						
130	CTRL	Have you developed information handling procedures for each of your information security classifications?	YES	NO	N/A	
131	CTRL	Have you developed information labeling procedures for each of your information security classifications?	YES	NO	N/A	
132	CTRL	Have you implemented your information handling procedures?	YES	NO	N/A	
133	CTRL	Have you implemented your information labeling procedures?	YES	NO	N/A	
134	GUIDE	Do your organization's information labeling procedures cover physical information assets?	YES	NO	N/A	
135	GUIDE	Do your organization's information labeling procedures cover electronic information assets?	YES	NO	N/A	

ORGANIZATION:	YOUR LOCATION:	
COMPLETED BY:	DATE COMPLETED:	
REVIEWED BY:	DATE REVIEWED:	
SEPT 2007	COPYRIGHT © 2007 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.	EDITION 4.0
<b>PART 7</b>	<b>ORGANIZATIONAL ASSET MANAGEMENT AUDIT</b>	<b>PAGE 61</b>



## ISO IEC 27002 2005 (17799 2005) INFORMATION SECURITY AUDIT TOOL

7. ORGANIZATIONAL ASSET MANAGEMENT AUDIT	RESPONSES	NOTES AND COMMENTS
--	-----------	--------------------

136	GUIDE	Does information system output, which is classified as sensitive or critical, receive a security label that makes it clear that the output is sensitive or critical?	YES	NO	N/A	
137	GUIDE	Does your security labeling system meet your information classification guidelines?	YES	NO	N/A	
138	GUIDE	Do your information security labeling procedures tell you how to label printed reports?	YES	NO	N/A	
139	GUIDE	Do your security labeling procedures tell you how to label screen displays?	YES	NO	N/A	
140	GUIDE	Do your security labeling procedures tell you how to label recorded media (e.g., CDs, tapes, disks)?	YES	NO	N/A	
141	GUIDE	Do your security labeling procedures tell you how to label electronic messages?	YES	NO	N/A	
142	GUIDE	Do your security labeling procedures tell you how to label file transfers?	YES	NO	N/A	
143	GUIDE	Do your information handling procedures define how information should be processed at each security classification level?	YES	NO	N/A	
144	GUIDE	Do your information handling procedures define how information should be stored at each security classification level?	YES	NO	N/A	
145	GUIDE	Do your information handling procedures define how information should be transmitted at each security classification level?	YES	NO	N/A	
146	GUIDE	Do your information handling procedures define how information should be declassified at each security classification level?	YES	NO	N/A	
147	GUIDE	Do your information handling procedures define how information should be destroyed at each security classification level?	YES	NO	N/A	
148	GUIDE	Do your information handling procedures define the chain of custody for each security level?	YES	NO	N/A	

ORGANIZATION:	YOUR LOCATION:	
COMPLETED BY:	DATE COMPLETED:	
REVIEWED BY:	DATE REVIEWED:	
SEPT 2007	COPYRIGHT © 2007 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.	EDITION 4.0
<b>PART 7</b>	<b>ORGANIZATIONAL ASSET MANAGEMENT AUDIT</b>	<b>PAGE 62</b>

