

ISO IEC 27002 2013 INFORMATION SECURITY AUDIT TOOL

15. SUPPLIER RELATIONSHIP MANAGEMENT AUDIT

15.1 ESTABLISH SECURITY AGREEMENTS WITH SUPPLIERS

15.1.1 EXPECT SUPPLIERS TO COMPLY WITH RISK MITIGATION AGREEMENTS

1	CTRL	Do you clarify the information security risks that exist whenever your suppliers have access to your organization's assets?	Y	N	X	
2	CTRL	Do you clarify your risk mitigation requirements and the risk mitigation expectations that your organization's suppliers must comply with?	Y	N	X	
3	CTRL	Do you establish security risk mitigation agreements with suppliers?	Y	N	X	
4	CTRL	Do you document your security risk mitigation agreements?	Y	N	X	
5	GUIDE	Did you establish a policy to control supplier access to your information?	Y	N	X	
6	GUIDE	Do you use your supplier access policy to document your access controls?	Y	N	X	
7	GUIDE	Do you establish control by developing processes and procedures?	Y	N	X	
8	GUIDE	Do you develop processes and procedures that you must apply?	Y	N	X	
9	GUIDE	Do you develop processes and procedures that suppliers must use?	Y	N	X	
10	GUIDE	Did you establish controls to restrict supplier access to your information?	Y	N	X	
11	GUIDE	Did you identify the types of suppliers that will be allowed to have access?	Y	N	X	
12	GUIDE	Did you describe the information that each type of supplier may access?	Y	N	X	
13	GUIDE	Did you describe specific access controls for each type of supplier?	Y	N	X	
14	GUIDE	Did you define security requirements for each type of information?	Y	N	X	
15	GUIDE	Did you specify access controls for each type of information?	Y	N	X	
16	GUIDE	Did you describe monitoring methods for each type of supplier?	Y	N	X	
17	GUIDE	Do you create information accuracy and completeness controls?	Y	N	X	
18	GUIDE	Do you use your controls to ensure the integrity of information?	Y	N	X	
19	GUIDE	Do you use them to ensure the integrity of information processing?	Y	N	X	
20	GUIDE	Do you clarify suppliers' information security duties and obligations?	Y	N	X	

ORGANIZATION:

YOUR LOCATION:

COMPLETED BY:

DATE COMPLETED:

REVIEWED BY:

DATE REVIEWED:

APR 2014

PLAIN ENGLISH INFORMATION SECURITY AUDIT TOOL

EDITION 1.0

PART 15

COPYRIGHT © 2014 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.

PAGE 121

ISO IEC 27002 2013 INFORMATION SECURITY AUDIT TOOL

15. SUPPLIER RELATIONSHIP MANAGEMENT AUDIT

21	GUIDE	Did you develop a typical supplier relationship management process?	Y	N	X	
22	GUIDE	Did you develop a typical supplier relationship management lifecycle?	Y	N	X	
23	GUIDE	Do you prepare information security agreements for each supplier (15.1.2)?	Y	N	X	
24	GUIDE	Do you define your minimum information security requirements?	Y	N	X	
25	GUIDE	Do you consider the type of information each supplier may access?	Y	N	X	
26	GUIDE	Do you consider your unique risk profile and business needs?	Y	N	X	
27	GUIDE	Do you define access controls for each type of information?	Y	N	X	
28	GUIDE	Do you describe how transitions should be managed and controlled?	Y	N	X	
29	GUIDE	Do you clarify how information will be moved safely and securely?	Y	N	X	
30	GUIDE	Do you clarify how information processing facilities are protected?	Y	N	X	
31	GUIDE	Do you assign responsibility for handling information security incidents?	Y	N	X	
32	GUIDE	Do you allocate responsibilities to both you and your suppliers?	Y	N	X	
33	GUIDE	Do you clarify your resilience and recovery needs and requirements?	Y	N	X	
34	GUIDE	Do you clarify your suppliers' resilience and recovery obligations?	Y	N	X	
35	GUIDE	Do you establish joint resilience and recovery arrangements?	Y	N	X	
36	GUIDE	Do you document all information security requirements and controls?	Y	N	X	
37	GUIDE	Do you monitor compliance with information security requirements?	Y	N	X	
38	GUIDE	Did you establish supplier monitoring processes and procedures?	Y	N	X	
39	GUIDE	Did you establish processes and procedures for each type of supplier?	Y	N	X	
40	GUIDE	Did you establish processes and procedures for each type of access?	Y	N	X	
41	GUIDE	Do you review compliance with information security requirements?	Y	N	X	
42	GUIDE	Did you establish third party review processes and procedures?	Y	N	X	
43	GUIDE	Did you establish product validation processes and procedures?	Y	N	X	

ORGANIZATION:

YOUR LOCATION:

COMPLETED BY:

DATE COMPLETED:

REVIEWED BY:

DATE REVIEWED:

APR 2014

PLAIN ENGLISH INFORMATION SECURITY AUDIT TOOL

EDITION 1.0

PART 15

COPYRIGHT © 2014 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.

PAGE 122

ISO IEC 27002 2013 INFORMATION SECURITY AUDIT TOOL

15. SUPPLIER RELATIONSHIP MANAGEMENT AUDIT

44	GUIDE	Did you establish an awareness program to talk about supplier security?	Y	N	X	
45	GUIDE	Do you make your personnel aware of your supplier access controls?	Y	N	X	
46	GUIDE	Do you teach buyers about your policies, processes and procedures?	Y	N	X	
47	GUIDE	Do you explain how your personnel should interact with suppliers?	Y	N	X	
48	GUIDE	Do you distinguish between types of suppliers and types of access?	Y	N	X	
49	GUIDE	Do you clarify the access that suppliers may be allowed to have?	Y	N	X	
15.1.2 EXPECT SUPPLIERS TO COMPLY WITH INFORMATION SECURITY AGREEMENTS						
50	CTRL	Have you identified all of the information security requirements that you expect suppliers to comply with?	Y	N	X	
51	CTRL	Do you clarify information security requirements whenever suppliers must <i>access</i> your organization's information?	Y	N	X	
52	CTRL	Do you clarify information security requirements whenever suppliers must <i>process</i> your organization's information?	Y	N	X	
53	CTRL	Do you clarify information security requirements whenever suppliers must <i>store</i> your organization's information?	Y	N	X	
54	CTRL	Do you clarify information security requirements whenever suppliers must <i>communicate</i> using your organization's information?	Y	N	X	
55	CTRL	Do you clarify information security requirements whenever your suppliers must <i>provide IT infrastructure components</i> ?	Y	N	X	
56	CTRL	Have you established information security agreements with each supplier?	Y	N	X	
57	GUIDE	Did you develop information security agreements for each supplier?	Y	N	X	
58	GUIDE	Do you describe relevant information security policies for each contract?	Y	N	X	
59	GUIDE	Do you describe the type of information that may be provided or accessed?	Y	N	X	
60	GUIDE	Do you describe the methods that may be used to provide information?	Y	N	X	
61	GUIDE	Do you describe the methods that may be used to access information?	Y	N	X	

ORGANIZATION:

YOUR LOCATION:

COMPLETED BY:

DATE COMPLETED:

REVIEWED BY:

DATE REVIEWED:

APR 2014

PLAIN ENGLISH INFORMATION SECURITY AUDIT TOOL

EDITION 1.0

PART 15

COPYRIGHT © 2014 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.

PAGE 123

ISO IEC 27002 2013 INFORMATION SECURITY AUDIT TOOL

15. SUPPLIER RELATIONSHIP MANAGEMENT AUDIT

62	GUIDE	Do you describe the information classification scheme that will be used?	Y	N	X	
63	GUIDE	Do you map your organization's scheme (8.2) against each supplier's?	Y	N	X	
64	GUIDE	Do you describe all relevant legal and regulatory requirements?	Y	N	X	
65	GUIDE	Do you explain how legal and regulatory requirements must be met?	Y	N	X	
66	GUIDE	Do you describe data protection obligations and requirements?	Y	N	X	
67	GUIDE	Do you describe intellectual property rights and requirements?	Y	N	X	
68	GUIDE	Do you describe the controls that each party must implement?	Y	N	X	
69	GUIDE	Do you describe the access controls that must be established?	Y	N	X	
70	GUIDE	Do you describe acceptable and unacceptable uses of information?	Y	N	X	
71	GUIDE	Do you describe how appropriate supplier personnel will be selected?	Y	N	X	
72	GUIDE	Do you specify personnel screening requirements and responsibilities?	Y	N	X	
73	GUIDE	Do you establish notification procedures that screeners must use?	Y	N	X	
74	GUIDE	Do you ask suppliers to notify you if they uncover security issues?	Y	N	X	
75	GUIDE	Do you ask suppliers to notify you if they fail to screen personnel?	Y	N	X	
76	GUIDE	Do you describe how authorized persons will be assigned and removed?	Y	N	X	
77	GUIDE	Do you describe how and when access authorizations will be assigned?	Y	N	X	
78	GUIDE	Do you consider creating explicit lists of authorized personnel?	Y	N	X	
79	GUIDE	Do you consider establishing supplier authorization procedures?	Y	N	X	
80	GUIDE	Do you consider defining supplier authorization conditions?	Y	N	X	
81	GUIDE	Do you describe how and why access authorizations would be revoked?	Y	N	X	
82	GUIDE	Do you describe rules to control the use of subcontractors by suppliers?	Y	N	X	

ORGANIZATION:

YOUR LOCATION:

COMPLETED BY:

DATE COMPLETED:

REVIEWED BY:

DATE REVIEWED:

APR 2014

PLAIN ENGLISH INFORMATION SECURITY AUDIT TOOL

EDITION 1.0

PART 15

COPYRIGHT © 2014 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.

PAGE 124

ISO IEC 27002 2013 INFORMATION SECURITY AUDIT TOOL

15. SUPPLIER RELATIONSHIP MANAGEMENT AUDIT

83	GUIDE	Do you describe controls suppliers must use to manage subcontractors?	Y	N	X	
84	GUIDE	Do you describe your organization's incident management requirements?	Y	N	X	
85	GUIDE	Do you describe your organization's incident management procedures?	Y	N	X	
86	GUIDE	Do you describe your notification and collaboration procedures?	Y	N	X	
87	GUIDE	Do you explain how people will work together if incidents occur?	Y	N	X	
88	GUIDE	Do you describe your security training and awareness requirements?	Y	N	X	
89	GUIDE	Do you expect suppliers to explain incident response procedures?	Y	N	X	
90	GUIDE	Do you expect suppliers to explain access authorization procedures?	Y	N	X	
91	GUIDE	Do you describe how you plan to communicate with each supplier?	Y	N	X	
92	GUIDE	Do you identify contacts for each information security agreement?	Y	N	X	
93	GUIDE	Do you describe how you plan to monitor supplier performance?	Y	N	X	
94	GUIDE	Do you describe your right to audit suppliers' processes and controls?	Y	N	X	
95	GUIDE	Do you describe the supplier audits that you plan to carry out?	Y	N	X	
96	GUIDE	Do you describe how you plan to review the performance of suppliers?	Y	N	X	
97	GUIDE	Do you describe suppliers' reporting obligations and responsibilities?	Y	N	X	
98	GUIDE	Do you ask suppliers to submit regular independent security reports?	Y	N	X	
99	GUIDE	Do you ask suppliers to report on the effectiveness of their controls?	Y	N	X	
100	GUIDE	Do you ask suppliers to explain how security issues were resolved?	Y	N	X	
101	GUIDE	Do you describe defect resolution and conflict resolution processes?	Y	N	X	
102	GUIDE	Do you document the security agreements you have with each supplier?	Y	N	X	
103	GUIDE	Do you expect your suppliers to comply with all security requirements?	Y	N	X	
104	GUIDE	Do you document the security obligations that your suppliers have?	Y	N	X	

ORGANIZATION:

YOUR LOCATION:

COMPLETED BY:

DATE COMPLETED:

REVIEWED BY:

DATE REVIEWED:

APR 2014

PLAIN ENGLISH INFORMATION SECURITY AUDIT TOOL

EDITION 1.0

PART 15

COPYRIGHT © 2014 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.

PAGE 125

ISO IEC 27002 2013 INFORMATION SECURITY AUDIT TOOL

15. SUPPLIER RELATIONSHIP MANAGEMENT AUDIT

15.1.3 EXPECT SUPPLIERS TO DEAL WITH THEIR OWN SUPPLY CHAIN SECURITY RISKS

105	CTRL	Do you expect your suppliers to address the information security risks connected with their use of information and communications technology services and product supply chains?	Y	N	X
106	CTRL	Do you include information security risk management requirements in the agreements you have with your organization's suppliers?	Y	N	X
107	GUIDE	Do you expect your suppliers to control their own supply chain risks?	Y	N	X
108	GUIDE	Do you prepare supply chain security agreements with your suppliers?	Y	N	X
109	GUIDE	Do you define the security requirements that suppliers must meet?	Y	N	X
110	GUIDE	Do you define security requirements that apply to your suppliers?	Y	N	X
111	GUIDE	Do you expect them to ensure that products meet requirements?	Y	N	X
112	GUIDE	Do you expect them to ensure that services meet requirements?	Y	N	X
113	GUIDE	Do you define the requirements that apply to suppliers' purchases?	Y	N	X
114	GUIDE	Do you clarify requirements for information products and services?	Y	N	X
115	GUIDE	Do you clarify requirements for communications technologies?	Y	N	X
116	GUIDE	Do you ask suppliers to create a process to identify critical components?	Y	N	X
117	GUIDE	Do you ask them to identify critical product and service components?	Y	N	X
118	GUIDE	Do you ask them to pay special attention to critical components?	Y	N	X
119	GUIDE	Do you ask them to monitor critical outsourced components?	Y	N	X
120	GUIDE	Do you ask them to ensure that the origin of items can be traced?	Y	N	X
121	GUIDE	Do you ask them to ensure that critical components work as expected?	Y	N	X
122	GUIDE	Do you clarify the requirements that your suppliers' suppliers must meet?	Y	N	X
123	GUIDE	Do you ask suppliers to implement security throughout supply chains?	Y	N	X
124	GUIDE	Do you ask them to protect the technologies that you depend upon?	Y	N	X
125	GUIDE	Do you ask them to protect IT and communication technologies?	Y	N	X

ORGANIZATION:

YOUR LOCATION:

COMPLETED BY:

DATE COMPLETED:

REVIEWED BY:

DATE REVIEWED:

APR 2014

PLAIN ENGLISH INFORMATION SECURITY AUDIT TOOL

EDITION 1.0

PART 15

COPYRIGHT © 2014 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.

PAGE 126

ISO IEC 27002 2013 INFORMATION SECURITY AUDIT TOOL

15. SUPPLIER RELATIONSHIP MANAGEMENT AUDIT

126	GUIDE	Do you ask them to safeguard the services that they subcontract?	Y	N	X	
127	GUIDE	Do you ask suppliers to propagate required security practices?	Y	N	X	
128	GUIDE	Do you ask them to safeguard the components that they buy?	Y	N	X	
129	GUIDE	Do you ask suppliers to propagate security requirements?	Y	N	X	
130	GUIDE	Do you expect suppliers to establish a supplier monitoring process?	Y	N	X	
131	GUIDE	Do you expect them to validate technology products and services?	Y	N	X	
132	GUIDE	Do you expect them to see if products meet security requirements?	Y	N	X	
133	GUIDE	Do you expect them to see if services meet security requirements?	Y	N	X	
134	GUIDE	Do you expect them to share information about their supply chains?	Y	N	X	
135	GUIDE	Do you ask them to share information about potential problems?	Y	N	X	
136	GUIDE	Do you ask them to share information about component lifecycles?	Y	N	X	
137	GUIDE	Do you ask them to tell you if items may no longer be available?	Y	N	X	
138	GUIDE	Do you ask suppliers to help you manage related security risks?	Y	N	X	

15.2 MANAGE SUPPLIER SECURITY AND SERVICE DELIVERY

15.2.1 MANAGE SUPPLIER SERVICES AND SUPPLIER SECURITY

139	CTRL	Do you monitor supplier service delivery and information security?	Y	N	X	
140	CTRL	Do you review supplier service delivery and information security?	Y	N	X	
141	CTRL	Do you audit supplier service delivery and information security?	Y	N	X	
142	GUIDE	Have you established a process to manage your relationship with suppliers?	Y	N	X	
143	GUIDE	Did you assign responsibility for managing your supplier relationships?	Y	N	X	
144	GUIDE	Did you assign this job to an individual or service management team?	Y	N	X	
145	GUIDE	Do you ask suppliers to assign someone to manage service agreements?	Y	N	X	
146	GUIDE	Do you ask them to enforce agreements and to review compliance?	Y	N	X	
147	GUIDE	Did you implement your supplier relationship management process?	Y	N	X	

ORGANIZATION:

YOUR LOCATION:

COMPLETED BY:

DATE COMPLETED:

REVIEWED BY:

DATE REVIEWED:

APR 2014

PLAIN ENGLISH INFORMATION SECURITY AUDIT TOOL

EDITION 1.0

PART 15

COPYRIGHT © 2014 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.

PAGE 127

ISO IEC 27002 2013 INFORMATION SECURITY AUDIT TOOL

15. SUPPLIER RELATIONSHIP MANAGEMENT AUDIT

148	GUIDE	Do you use your process to ensure that suppliers can provide services?	Y	N	X	
149	GUIDE	Do you verify that suppliers are capable of maintaining service levels?	Y	N	X	
150	GUIDE	Do you verify that suppliers have workable service continuity plans?	Y	N	X	
151	GUIDE	Do you verify that services can be provided after big disasters (17)?	Y	N	X	
152	GUIDE	Do you verify that acceptable service levels can be maintained?	Y	N	X	
153	GUIDE	Do you use your process to monitor supplier service and compliance?	Y	N	X	
154	GUIDE	Do you check compliance with information security agreements?	Y	N	X	
155	GUIDE	Do you monitor suppliers' service delivery performance levels?	Y	N	X	
156	GUIDE	Do you support monitoring by providing needed skills and resources?	Y	N	X	
157	GUIDE	Do you verify that security incidents and issues are well managed?	Y	N	X	
158	GUIDE	Do you take action whenever incidents occur and service suffers?	Y	N	X	
159	GUIDE	Do you use your process to coordinate and control critical suppliers?	Y	N	X	
160	GUIDE	Do you control suppliers who manage or provide critical services?	Y	N	X	
161	GUIDE	Do you retain control over how these suppliers manage security?	Y	N	X	
162	GUIDE	Do you control how suppliers protect your critical facilities?	Y	N	X	
163	GUIDE	Do you monitor how critical suppliers manage your security?	Y	N	X	
164	GUIDE	Do you monitor how critical suppliers identify vulnerabilities?	Y	N	X	
165	GUIDE	Do you monitor how critical suppliers respond to incidents?	Y	N	X	
166	GUIDE	Do you monitor how critical suppliers manage changes?	Y	N	X	
167	GUIDE	Do you monitor how critical suppliers report incidents?	Y	N	X	
168	GUIDE	Did you establish a security incident reporting process?	Y	N	X	
169	GUIDE	Do you control how suppliers protect sensitive information?	Y	N	X	
170	GUIDE	Do you control how suppliers access sensitive information?	Y	N	X	
171	GUIDE	Do you monitor how suppliers protect sensitive information?	Y	N	X	

ORGANIZATION:

YOUR LOCATION:

COMPLETED BY:

DATE COMPLETED:

REVIEWED BY:

DATE REVIEWED:

APR 2014

PLAIN ENGLISH INFORMATION SECURITY AUDIT TOOL

EDITION 1.0

PART 15

COPYRIGHT © 2014 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.

PAGE 128

ISO IEC 27002 2013 INFORMATION SECURITY AUDIT TOOL

15. SUPPLIER RELATIONSHIP MANAGEMENT AUDIT

172	GUIDE	Do you control how suppliers process sensitive information?	Y	N	X
173	GUIDE	Do you monitor how suppliers process sensitive information?	Y	N	X
174	GUIDE	Do you use your process to share information about security incidents?	Y	N	X
175	GUIDE	Do you evaluate supplier service delivery and compliance (15.1.3)?	Y	N	X
176	GUIDE	Do you audit supplier compliance with your supplier agreements?	Y	N	X
177	GUIDE	Do you study reports produced by independent auditors (if available)?	Y	N	X
178	GUIDE	Do you follow up on compliance and performance problems?	Y	N	X
179	GUIDE	Do you review supplier compliance with your supplier agreements?	Y	N	X
180	GUIDE	Do you review service delivery reports generated by your suppliers?	Y	N	X
181	GUIDE	Do you arrange regular progress meetings (to verify compliance)?	Y	N	X
182	GUIDE	Do you review how well security incidents are being handled?	Y	N	X
183	GUIDE	Do you review supplier audit trails and records of security events?	Y	N	X
184	GUIDE	Do you review operational problems, failures, faults, and disruptions?	Y	N	X
185	GUIDE	Do you resolve identified problems, failures, faults, and disruptions?	Y	N	X
186	GUIDE	Do you review the relationship suppliers have with their own suppliers?	Y	N	X
187	GUIDE	Do you review the information security aspects of this relationship?	Y	N	X
188	GUIDE	Do you review information security incidents with your suppliers?	Y	N	X

15.2.2 MANAGE CHANGES TO SERVICES PROVIDED BY SUPPLIERS

189	CTRL	Do you evaluate changes to services provided by your suppliers?	Y	N	X
190	CTRL	Do you think about how critical your business information is and how important your systems and processes are whenever you evaluate changes to supplier services?	Y	N	X
191	CTRL	Do you re-assess your organization's information security risks whenever changes to supplier services are being considered?	Y	N	X
192	CTRL	Do you manage changes to services provided by suppliers?	Y	N	X
193	CTRL	Do you manage changes in information security policies?	Y	N	X

ORGANIZATION:

YOUR LOCATION:

COMPLETED BY:

DATE COMPLETED:

REVIEWED BY:

DATE REVIEWED:

APR 2014

PLAIN ENGLISH INFORMATION SECURITY AUDIT TOOL

EDITION 1.0

PART 15

COPYRIGHT © 2014 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.

PAGE 129

ISO IEC 27002 2013 INFORMATION SECURITY AUDIT TOOL

15. SUPPLIER RELATIONSHIP MANAGEMENT AUDIT

194	CTRL	Do you manage changes in information security controls?	Y	N	X	
195	CTRL	Do you manage changes in information security procedures?	Y	N	X	
196	GUIDE	Do you manage changes to supplier agreements (15.1.2, 15.1.3)?	Y	N	X	
197	GUIDE	Do you manage the changes that you make to supplier services?	Y	N	X	
198	GUIDE	Do you manage and control changes in policies and procedures?	Y	N	X	
199	GUIDE	Do you manage and control enhancements to current services?	Y	N	X	
200	GUIDE	Do you manage and control the development of new applications?	Y	N	X	
201	GUIDE	Do you manage and control the development of new systems?	Y	N	X	
202	GUIDE	Do you manage and control changes in information security controls?	Y	N	X	
203	GUIDE	Do you manage and control how security incidents are resolved?	Y	N	X	
204	GUIDE	Do you manage and control all attempts to improve security?	Y	N	X	
205	GUIDE	Do you manage the changes that suppliers make to their services?	Y	N	X	
206	GUIDE	Do you manage and control changes and enhancements to networks?	Y	N	X	
207	GUIDE	Do you manage and control the use of new technologies and techniques?	Y	N	X	
208	GUIDE	Do you manage and control the use of new products and new versions?	Y	N	X	
209	GUIDE	Do you manage and control the use of new development environments?	Y	N	X	
210	GUIDE	Do you manage and control the use of new development tools?	Y	N	X	
211	GUIDE	Do you manage and control changes in location or service facilities?	Y	N	X	
212	GUIDE	Do you manage and control changes in suppliers and contractors?	Y	N	X	
213	GUIDE	Do you manage and control changes in the use of subcontractors?	Y	N	X	
214	GUIDE	Do you control how suppliers subcontract to another supplier?	Y	N	X	

Answer each of the above questions. Three answers are possible: Y (yes), N (no), and X (eXclude). Y means you're in compliance, N means you're not in compliance, while X means that this question can be excluded because it's not applicable in your situation. Y answers and X answers require no further action, while N answers point to security practices that need to be followed and security controls that need to be implemented. Also, please use the column on the right to record your notes, and in the spaces below, enter the name and location of your organization, who completed this page, who reviewed it, and the dates.

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	
APR 2014	PLAIN ENGLISH INFORMATION SECURITY AUDIT TOOL		EDITION 1.0
PART 15	COPYRIGHT © 2014 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.		PAGE 130