ISO IEC 27002 2013 INFORMATION SECURITY AUDIT TOOL

7. PERSONNEL SECURITY MANAGEMENT AUDIT

7.1 EMPHASIZE SECURITY PRIOR TO EMPLOYMENT

7.1.1 VERIFY THE BACKGROUNDS OF ALL NEW PERSONNEL

1	CTRL	Do you check the backgrounds of all candidates for employment?	Y	N	X	
2	CTRL	Do you make sure that background verifications comply with all relevant laws and regulations and with all relevant ethical standards?	Y	N	X	
3	CTRL	Do you make sure that background verifications take your unique security risks and requirements into consideration?	Y	N	X	
4	CTRL	Do you perform more rigorous background verification checks whenever the perceived security risk is greater?	Y	N	X	
5	CTRL	Do you perform more rigorous background checks on people who will be handling sensitive information?	Y	N	X	
6	GUIDE	Do you respect all relevant legislation when you do background checks?	Y	N	X	
7	GUIDE	Do you consider privacy legislation when verifications are done?	Y	N	X	
8	GUIDE	Do you protect all relevant personally identifiable information?	Y	N	X	
9	GUIDE	Do you inform candidates beforehand when legally required?	Y	N	X	
10	GUIDE	Do you consider employment legislation when verifications are done?	Y	N	X	
11	GUIDE	Have you established personnel background verification procedures?	Y	N	X	
12	GUIDE	Did you define how background verifications should be performed?	Y	N	X	
13	GUIDE	Did you define background verification criteria and clarify limitations?	Y	N	X	
14	GUIDE	Did you clarify who is allowed to do background verifications?	Y	N	X	
15	GUIDE	Did you clarify when background verifications should be done?	Y	N	X	
16	GUIDE	Did you clarify why background verifications are important?	Y	N	X	
17	GUIDE	Have you established a process for screening contractors?	Y	N	X	
18	GUIDE	Do you use agreements to ensure that screening takes place?	Y	N	X	
19	GUIDE	Do you specify contractor screening duties and responsibilities?	Y	N	X	
20	GUIDE	Do you create notification procedures to address screening issues?	Y	N	X	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

21	GUIDE	Do you clarify what must be done when problems are discovered?	Y	N	X	
22	GUIDE	Do you clarify what must be done when screening isn't completed?	Y	N	X	
23	GUIDE	Do you check the personal history of all candidates?	Y	N	X	
24	GUIDE	Do you check the candidate's personal identity?	Y	N	X	
25	GUIDE	Do you check the candidate's character references?	Y	N	X	
26	GUIDE	Do you check the candidate's financial credit history?	Y	N	X	
27	GUIDE	Do you check to see if candidate has a criminal record?	Y	N	X	
28	GUIDE	Do you verify the professional history of all candidates?	Y	N	X	
29	GUIDE	Do you verify the candidate's curriculum vitae (résumé)?	Y	N	X	
30	GUIDE	Do you verify its completeness and accuracy?	Y	N	X	
31	GUIDE	Do you verify the candidate's qualifications?	Y	N	X	
32	GUIDE	Do you verify the candidate's occupational qualifications?	Y	N	X	
33	GUIDE	Do you verify the candidate's academic qualifications?	Y	N	X	
34	GUIDE	Do you determine the suitability of all information security candidates?	Y	N	X	
35	GUIDE	Do you verify the competence of information security candidates?	Y	N	X	
36	GUIDE	Do you verify the trustworthiness of information security candidates?	Y	N	X	
37	GUIDE	Do you do more checks if candidates will handle confidential information?	Y	N	X	
38	GUIDE	Do you do more detailed checks for both new hires and promotions?	Y	N	X	
39	GUIDE	Do you check more if information processing facilities will be accessed?	Y	N	X	
7.1.2 USE CONTRACTS TO PROTECT YOUR INFORMATION						
40	**CTRL**	Do you use contractual terms and conditions to specify your *organization's* information security responsibilities?	Y	N	X	
41	**CTRL**	Do you use contractual terms and conditions to specify your *employees'* information security responsibilities?	Y	N	X	
42	**CTRL**	Do you use contractual terms and conditions to specify your *contractors'* information security responsibilities?	Y	N	X	

ISO IEC 27002 2013 INFORMATION SECURITY AUDIT TOOL

7. PERSONNEL SECURITY MANAGEMENT AUDIT

43	GUIDE	Do you draft confidentiality and nondisclosure agreements (see 13.2.4)?	Y	N	X	
44	GUIDE	Do you ensure that agreements comply with your security policies?	Y	N	X	
45	GUIDE	Do you prepare suitable confidentiality and nondisclosure agreements?	Y	N	X	
46	GUIDE	Do you clarify information security obligations and responsibilities?	Y	N	X	
47	GUIDE	Do you clarify all relevant legal obligations and responsibilities?	Y	N	X	
48	GUIDE	Do you clarify copyright and data protection laws (18.1.2, 18.1.4)?	Y	N	X	
49	GUIDE	Do you clarify how other people's information must be handled?	Y	N	X	
50	GUIDE	Do you safeguard information received from external parties?	Y	N	X	
51	GUIDE	Do you safeguard information received from other companies?	Y	N	X	
52	GUIDE	Do you clarify asset protection obligations and responsibilities (8)?	Y	N	X	
53	GUIDE	Do you ensure that information is appropriately classified?	Y	N	X	
54	GUIDE	Do you ensure that information services are properly protected?	Y	N	X	
55	GUIDE	Do you ensure that information processing facilities are safeguarded?	Y	N	X	
56	GUIDE	Do you clarify what happens if security requirements are disregarded?	Y	N	X	
57	GUIDE	Do you clarify the actions and legal steps that will be taken (7.2.3)?	Y	N	X	
58	GUIDE	Do you tell job candidates that they will be expected to sign agreements?	Y	N	X	
59	GUIDE	Do you clarify their specific duties during the pre-employment process?	Y	N	X	
60	GUIDE	Do you clarify their information security roles and responsibilities?	Y	N	X	
61	GUIDE	Do you explain that obligations may continue after job ends (see 7.3)?	Y	N	X	
62	GUIDE	Do you ensure that agreements are signed before access is allowed?	Y	N	X	
63	GUIDE	Do you ask both employees and contractors to sign agreements?	Y	N	X	
64	GUIDE	Do you ensure that terms and conditions are appropriate to the job?	Y	N	X	
65	GUIDE	Do you ensure that they agree with your terms and conditions?	Y	N	X	
66	GUIDE	Do you use contractual agreements to protect confidential information?	Y	N	X	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

7. PERSONNEL SECURITY MANAGEMENT AUDIT

7.2 EMPHASIZE SECURITY DURING EMPLOYMENT

7.2.1 EXPECT YOUR MANAGERS TO EMPHASIZE SECURITY

67	CTRL	Do you make sure that your managers require all *employees* to apply your organization’s information security policies and procedures?	Y	N	X	
68	CTRL	Do you make sure that your managers require all *contractors* to apply your organization’s information security policies and procedures?	Y	N	X	
69	GUIDE	Do you expect managers to act as information security role models?	Y	N	X	
70	GUIDE	Do you expect managers to support policies, procedures, and controls?	Y	N	X	
71	GUIDE	Do you expect managers to enforce security policies and procedures?	Y	N	X	
72	GUIDE	Do you expect managers to motivate employees and contractors?	Y	N	X	
73	GUIDE	Do you expect managers to control access to information and systems?	Y	N	X	
74	GUIDE	Do you clarify security roles and responsibilities before allowing access?	Y	N	X	
75	GUIDE	Do you provide information security briefings before granting access?	Y	N	X	
76	GUIDE	Do you provide information security guidelines before granting access?	Y	N	X	
77	GUIDE	Do you expect managers to make people aware of their responsibilities?	Y	N	X	
78	GUIDE	Do you clarify information security responsibilities specific to each job?	Y	N	X	
79	GUIDE	Do you expect people to achieve a suitable level of security awareness?	Y	N	X	
80	GUIDE	Do you expect managers to enforce terms and conditions of employment?	Y	N	X	
81	GUIDE	Do you expect all personnel to use the appropriate work methods?	Y	N	X	
82	GUIDE	Do you expect managers to ensure that all personnel are competent?	Y	N	X	
83	GUIDE	Do they ensure that people have the right skills and qualifications?	Y	N	X	
84	GUIDE	Do they ensure that people continue to have the right knowledge?	Y	N	X	
85	GUIDE	Do you expect managers to provide an anonymous reporting channel?	Y	N	X	
86	GUIDE	Do you expect people to report security policy and procedure violations?	Y	N	X	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

7.2.2 DELIVER INFORMATION SECURITY AWARENESS PROGRAMS

87	CTRL	Do you make sure that your organization’s employees receive regular information security briefings and updates?	Y	N	X	
88	CTRL	Do you make sure that employees are aware of your security policies and procedures and are kept up-to-date with the latest changes?	Y	N	X	
89	CTRL	Do you make sure that employees receive the information security training and education they need to properly carry out their jobs?	Y	N	X	
90	CTRL	Do you make sure that your organization’s contractors receive regular information security briefings and updates?	Y	N	X	
91	CTRL	Do you make sure that contractors are aware of your security policies and procedures and are kept up-to-date with the latest changes?	Y	N	X	
92	CTRL	Do you make sure that your organization’s contractors receive the information security training and education they need to do their jobs?	Y	N	X	
93	GUIDE	Have you established an information security awareness program?	Y	N	X	
94	GUIDE	Did you ensure that the program complies with your security policies?	Y	N	X	
95	GUIDE	Did you ensure that the program complies with your security procedures?	Y	N	X	
96	GUIDE	Did you design and plan an information security awareness program?	Y	N	X	
97	GUIDE	Did you think about the jobs people do and what you expect from them?	Y	N	X	
98	GUIDE	Did you think about what employees should know about security?	Y	N	X	
99	GUIDE	Did you think about what contractors should know about security?	Y	N	X	
100	GUIDE	Did you think about what your awareness program should discuss?	Y	N	X	
101	GUIDE	Did you think about your organization’s specific security obligations?	Y	N	X	
102	GUIDE	Did you think about what kinds of information should be protected?	Y	N	X	
103	GUIDE	Did you think about your organization’s information security controls?	Y	N	X	
104	GUIDE	Did you think about your current information security controls?	Y	N	X	
105	GUIDE	Did you think about newly adopted information security controls?	Y	N	X	
106	GUIDE	Did you think about how your awareness program should be delivered?	Y	N	X	

107	GUIDE	Did you consider using booklets and newsletters to raise awareness?	Y	N	X	
108	GUIDE	Did you consider using campaigns to raise security awareness?	Y	N	X	
109	GUIDE	Did you consider using classroom-based teaching methods?	Y	N	X	
110	GUIDE	Did you consider using web-based learning methods?	Y	N	X	
111	GUIDE	Did you consider using self-paced learning methods?	Y	N	X	
112	GUIDE	Did you consider using distance learning methods?	Y	N	X	
113	GUIDE	Did you think about how awareness activities should be scheduled?	Y	N	X	
114	GUIDE	Did you consider scheduling regular security awareness activities?	Y	N	X	
115	GUIDE	Do you schedule activities for new employees and contractors?	Y	N	X	
116	GUIDE	Do you schedule activities for current employees and contractors?	Y	N	X	
117	GUIDE	Do you schedule activities for people with new roles or positions?	Y	N	X	
118	GUIDE	Do you provide training before people start their new jobs?	Y	N	X	
119	GUIDE	Did you consider scheduling periodic security awareness sessions?	Y	N	X	
120	GUIDE	Do you use your awareness program to talk about information security?	Y	N	X	
121	GUIDE	Do you talk about your organization's approach to information security?	Y	N	X	
122	GUIDE	Do you discuss management's commitment to information security?	Y	N	X	
123	GUIDE	Do you explain whose information must be protected and why?	Y	N	X	
124	GUIDE	Do you discuss the need to be accountable for actions and inactions?	Y	N	X	
125	GUIDE	Do you explain why personal accountability is so important?	Y	N	X	
126	GUIDE	Do you talk about relevant information security rules and regulations?	Y	N	X	
127	GUIDE	Do you explain why they must be familiar with rules and regulations?	Y	N	X	
128	GUIDE	Do you explain why they must comply with rules and regulations?	Y	N	X	
129	GUIDE	Do you explain why they must comply with security policies?	Y	N	X	
130	GUIDE	Do you explain why they must comply with security legislation?	Y	N	X	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

ISO IEC 27002 2013 INFORMATION SECURITY AUDIT TOOL

7. PERSONNEL SECURITY MANAGEMENT AUDIT

131	GUIDE	Do you explain why they must comply with security regulations?	Y	N	X	
132	GUIDE	Do you explain why they must comply with security agreements?	Y	N	X	
133	GUIDE	Do you explain why they must comply with security standards?	Y	N	X	
134	GUIDE	Do you explain why they must comply with security contracts?	Y	N	X	
135	GUIDE	Do you talk about your organization’s information security expectations?	Y	N	X	
136	GUIDE	Do you teach people about their information security responsibilities?	Y	N	X	
137	GUIDE	Do you make employees aware of their security responsibilities?	Y	N	X	
138	GUIDE	Do you explain how employees can meet their responsibilities?	Y	N	X	
139	GUIDE	Do you make contractors aware of their security responsibilities?	Y	N	X	
140	GUIDE	Do you explain how contractors can meet their responsibilities?	Y	N	X	
141	GUIDE	Do you teach people about the information that must be protected?	Y	N	X	
142	GUIDE	Do you teach people about your information security procedures?	Y	N	X	
143	GUIDE	Do you teach people about your incident reporting procedures?	Y	N	X	
144	GUIDE	Do you teach people about your information security controls?	Y	N	X	
145	GUIDE	Do you teach people about your password security measures?	Y	N	X	
146	GUIDE	Do you teach people about your malware control mechanisms?	Y	N	X	
147	GUIDE	Do you teach people about your clear desk and screen policy?	Y	N	X	
148	GUIDE	Do you teach people about how they can learn more about security?	Y	N	X	
149	GUIDE	Do you explain who they can contact to get more information?	Y	N	X	
150	GUIDE	Do you explain how they can access more security resources?	Y	N	X	
151	GUIDE	Do you explain where they can get more training materials?	Y	N	X	
152	GUIDE	Do you evaluate your information security awareness program?	Y	N	X	
153	GUIDE	Do you see if it still complies with security policies and procedures?	Y	N	X	
154	GUIDE	Do you update your information security awareness program?	Y	N	X	
155	GUIDE	Do you base updates on lessons learned from security incidents?	Y	N	X	

ORGANIZATION: YOUR LOCATION:

COMPLETED BY: DATE COMPLETED:

REVIEWED BY: DATE REVIEWED:

7.2.3 SET UP A DISCIPLINARY PROCESS FOR SECURITY BREACHES

156	CTRL	Have you established a formal disciplinary process to handle employees who have committed a security breach?	Y	N	X	
157	CTRL	Do you communicate your disciplinary process and make sure that all employees are aware of what happens when security is breached?	Y	N	X	
158	GUIDE	Did you design a formal disciplinary process to handle security breaches?	Y	N	X	
159	GUIDE	Did you design a process that treats offenders fairly and correctly?	Y	N	X	
160	GUIDE	Did you design a graduated process that requires a measured response?	Y	N	X	
161	GUIDE	Do you consider the nature and the gravity of security breaches?	Y	N	X	
162	GUIDE	Do you consider the impact security breaches have on business?	Y	N	X	
163	GUIDE	Do you consider legal obligations and contractual requirements?	Y	N	X	
164	GUIDE	Do you consider how much security training the offender has?	Y	N	X	
165	GUIDE	Do you consider whether or not it is a first or repeat offence?	Y	N	X	
166	GUIDE	Do you consider whether or not it is a deliberate breach?	Y	N	X	
167	GUIDE	Do you apply your disciplinary process whenever a breach occurs?	Y	N	X	
168	GUIDE	Do you collect evidence before you initiate a disciplinary process?	Y	N	X	
169	GUIDE	Do you make sure that a breach has occurred before you take action?	Y	N	X	
170	GUIDE	Do you use your disciplinary process to deter future security breaches?	Y	N	X	
171	GUIDE	Do you make it clear that security violations will not be tolerated?	Y	N	X	

7.3 EMPHASIZE SECURITY AT TERMINATION OF EMPLOYMENT

7.3.1 EMPHASIZE POST-EMPLOYMENT SECURITY REQUIREMENTS

172	CTRL	Have you defined information security responsibilities and duties that remain valid after personnel are terminated or responsibilities change?	Y	N	X	
173	CTRL	Do you communicate your post-employment information security requirements to both employees and contractors?	Y	N	X	

7. PERSONNEL SECURITY MANAGEMENT AUDIT

174	CTRL	Do you ensure that both employees and contractors clearly understand what their information security responsibilities and duties will continue to be even after they have been terminated or their responsibilities have changed?	Y	N	X	
175	CTRL	Do you enforce your organization's post-employment information security expectations and requirements?	Y	N	X	
176	GUIDE	Do you identify responsibilities still valid after termination of employment?	Y	N	X	
177	GUIDE	Do you clarify which legal responsibilities remain valid after termination?	Y	N	X	
178	GUIDE	Do you clarify which information security responsibilities remain valid?	Y	N	X	
179	GUIDE	Do you clarify nondisclosure requirements that remain valid?	Y	N	X	
180	GUIDE	Do you clarify confidentiality requirements that remain valid (13.2.4)?	Y	N	X	
181	GUIDE	Do you clarify employment contract requirements that remain valid?	Y	N	X	
182	GUIDE	Do you clarify how long security requirements are valid (7.1.2)?	Y	N	X	
183	GUIDE	Do you clarify information security responsibilities when job duties change?	Y	N	X	
184	GUIDE	Do you identify old responsibilities still valid after job duties change?	Y	N	X	
185	GUIDE	Do you identify newly acquired information security responsibilities?	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:	