13. INFORMATION SECURITY INCIDENT MANAGEMENT			RESPONSES			ASSIGNED TO	START	FINISH
13.1 REPORT INFORMATION SECURITY EVENTS AND WEAKNESSES								
1	**GOAL**	Make sure that information system security incidents are promptly reported.	TODO	DONE	NA			
2	**GOAL**	Make sure that information system security events and weaknesses are promptly communicated.	TODO	DONE	NA			
3	**GOAL**	Make sure that information security incident reports and communications allow timely corrective actions to be taken.	TODO	DONE	NA			
4	**GOAL**	Establish formal security event reporting procedures.	TODO	DONE	NA			
5	**GOAL**	Establish formal security escalation procedures.	TODO	DONE	NA			
6	**GOAL**	Make sure that all employees know how to report information security events and weaknesses.	TODO	DONE	NA			
7	**GOAL**	Make sure that all contractors know how to report information security events and weaknesses.	TODO	DONE	NA			
8	**GOAL**	Make sure that all third party users know how to report information security events and weaknesses.	TODO	DONE	NA			
9	**GOAL**	Make sure that employees are officially required to report information security events and weaknesses to a designated point of contact.	TODO	DONE	NA			
10	**GOAL**	Make sure that contractors are officially required to report information security events and weaknesses to a designated point of contact.	TODO	DONE	NA			
11	**GOAL**	Make sure that third party users are officially required to report information security events and weaknesses to a designated point of contact.	TODO	DONE	NA			
13.1.1 REPORT INFORMATION SECURITY EVENTS AS QUICKLY AS POSSIBLE								
12	**CTRL**	Report information security events using the appropriate management reporting channels.	TODO	DONE	NA			
13	**CTRL**	Make sure that security events are reported promptly.	TODO	DONE	NA			
14	GUIDE	Establish a formal information security event reporting procedure.	TODO	DONE	NA			

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

13. INFORMATION SECURITY INCIDENT MANAGEMENT			RESPONSES			ASSIGNED TO	START	FINISH
15	GUIDE	Make sure that your information security event reporting procedure establishes a point of contact.	TODO	DONE	N/A			
16	GUIDE	Make sure that your point of contact is known throughout your organization.	TODO	DONE	N/A			
17	GUIDE	Make sure that your organization's point of contact is always available.	TODO	DONE	N/A			
18	GUIDE	Make sure that your point of contact is able to respond adequately.	TODO	DONE	N/A			
19	GUIDE	Make sure that your point of contact can respond in a timely manner.	TODO	DONE	N/A			
20	GUIDE	Establish a formal incident response and escalation procedure.	TODO	DONE	N/A			
21	GUIDE	Make sure that your incident response and escalation procedure identifies the actions that must be taken when an information security report is received.	TODO	DONE	N/A			
22	GUIDE	Make sure that all employees are aware of their responsibility to promptly report all information security events.	TODO	DONE	N/A			
23	GUIDE	Make sure that all contractors are aware of their responsibility to promptly report all information security events.	TODO	DONE	N/A			
24	GUIDE	Make sure that all third party users are aware of their responsibility to promptly report all information security events.	TODO	DONE	N/A			
25	GUIDE	Make sure that all employees know how to use your information security event reporting procedure to report to the point of contact.	TODO	DONE	N/A			
26	GUIDE	Make sure that all contractors know how to use your information security event reporting procedure to report to the point of contact.	TODO	DONE	N/A			
27	GUIDE	Make sure that all third party users know how to use your information security event reporting procedure to report to the point of contact.	TODO	DONE	N/A			

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

13. INFORMATION SECURITY INCIDENT MANAGEMENT			RESPONSES			ASSIGNED TO	START	FINISH
28	GUIDE	Make sure that your information security event reporting procedure includes a suitable feedback process to ensure that people are informed about the results that were achieved.	TODO	DONE	N/A			
29	GUIDE	Make sure that your information security event reporting procedure includes a form that people can use to report and record security events.	TODO	DONE	N/A			
30	GUIDE	Make sure that your information security event reporting procedure makes it clear that all important event details must be recorded immediately.	TODO	DONE	N/A			
31	GUIDE	Make sure that your information security event reporting procedure makes it clear that people should record the type of breach or malfunction, the message on the screen, in addition to any other strange or unusual aspects.	TODO	DONE	N/A			
32	GUIDE	Make sure that your information security event reporting procedure makes it clear that people should avoid taking any remedial actions, and should, instead, immediately report the event to the point of contact.	TODO	DONE	N/A			
33	GUIDE	Make sure that your information security event reporting procedure makes it clear that a formal disciplinary process will be followed when someone commits a security breach.	TODO	DONE	N/A			
34	GUIDE	Establish duress alarms that people working in high-risk environments can secretly use to indicate that a serious security event is occurring.	TODO	DONE	N/A			
35	GUIDE	Establish duress alarm response procedures to ensure that every duress alarm is handled properly and without delay.	TODO	DONE	N/A			
36	NOTE	Make sure that your security incident reporting and response procedures handle loss of service incidents.	TODO	DONE	N/A			
37	NOTE	Make sure that your security incident reporting and response procedures handle loss of equipment incidents.	TODO	DONE	N/A			
38	NOTE	Make sure that your security incident reporting and response procedures handle loss of facilities incidents.	TODO	DONE	N/A			
39	NOTE	Make sure that your security incident reporting and response procedures handle system malfunctions.	TODO	DONE	N/A			
40	NOTE	Make sure that your security incident reporting and response procedures handle system overloads.	TODO	DONE	N/A			

13. INFORMATION SECURITY INCIDENT MANAGEMENT			RESPONSES			ASSIGNED TO	START	FINISH
41	NOTE	Make sure that your security incident reporting and response procedures handle human errors.	TODO	DONE	N/A			
42	NOTE	Make sure that your security incident reporting and response procedures handle policy noncompliances.	TODO	DONE	N/A			
43	NOTE	Make sure that your security incident reporting and response procedures handle guideline violations.	TODO	DONE	N/A			
44	NOTE	Make sure that your security incident reporting and response procedures handle access violations.	TODO	DONE	N/A			
45	NOTE	Make sure that your security incident reporting and response procedures handle software malfunctions.	TODO	DONE	N/A			
46	NOTE	Make sure that your security incident reporting and response procedures handle hardware malfunctions.	TODO	DONE	N/A			
47	NOTE	Make sure that your security incident reporting and response procedures handle physical security breaches.	TODO	DONE	N/A			
48	NOTE	Make sure that your security incident reporting and response procedures handle uncontrolled system changes.	TODO	DONE	N/A			
49	NOTE	Use anonymous information security incidents to make users aware of security issues and what they can do to avoid and respond to similar incidents (also see 8.2.2).	TODO	DONE	N/A			
50	NOTE	Collect evidence as soon as possible after the occurrence of an information security incident or event (see 13.2.3).	TODO	DONE	N/A			
51	NOTE	See ISO/IEC TR 18044 for more information about reporting and managing information security incidents.	TODO	DONE	N/A			
13.1.2 REPORT SECURITY WEAKNESSES IN SYSTEMS AND SERVICES								
52	**CTRL**	Make sure that all employees are officially required to record and report all observed or suspected security weaknesses in information systems and services.	TODO	DONE	N/A			
53	**CTRL**	Make sure that all contractors are officially required to record and report all observed or suspected security weaknesses in information systems and services.	TODO	DONE	N/A			
54	**CTRL**	Make sure that all third party users are officially required to record and report all observed or suspected security weaknesses in information systems and services.	TODO	DONE	N/A			

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

13. INFORMATION SECURITY INCIDENT MANAGEMENT			RESPONSES			ASSIGNED TO	START	FINISH
55	GUIDE	Prevent information security incidents by making sure that all employees promptly report observed or suspected security weaknesses to their manager or service provider.	TODO	DONE	N/A			
56	GUIDE	Prevent information security incidents by making sure that all contractors promptly report observed or suspected security weaknesses to their manager or service provider.	TODO	DONE	N/A			
57	GUIDE	Prevent information security incidents by making sure that all third party users promptly report observed or suspected security weaknesses to their manager or service provider.	TODO	DONE	N/A			
58	GUIDE	Make sure that your security weakness reporting mechanism is easy to use and always available.	TODO	DONE	N/A			
59	NOTE	Make sure that all employees understand that they should not try to test a suspected weakness or prove that it is real.	TODO	DONE	N/A			
60	NOTE	Make sure that all contractors understand that they should not try to test a suspected weakness or prove that it is real.	TODO	DONE	N/A			
61	NOTE	Make sure that third party users understand that they should not try to test a suspected weakness or prove that it is real.	TODO	DONE	N/A			
13.2 MANAGE INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS								
62	**GOAL**	Make sure that your information security incident management approach is both effective and consistently applied.	TODO	DONE	N/A			
63	**GOAL**	Make people responsible for handling information security events and weaknesses once they have been reported.	TODO	DONE	N/A			
64	**GOAL**	Establish procedures for handling information security events and weaknesses once they have been reported.	TODO	DONE	N/A			
65	**GOAL**	Continually improve how you manage your organization's information security incidents.	TODO	DONE	N/A			
66	**GOAL**	Continually improve how you respond to your organization's information security incidents.	TODO	DONE	N/A			
67	**GOAL**	Continually improve how you monitor your organization's information security incidents.	TODO	DONE	N/A			
68	**GOAL**	Continually improve how you evaluate your organization's information security incidents.	TODO	DONE	N/A			
69	**GOAL**	Collect evidence about information security incidents whenever it is required in order to support legal action.	TODO	DONE	N/A			

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

13. INFORMATION SECURITY INCIDENT MANAGEMENT			RESPONSES			ASSIGNED TO	START	FINISH
13.2.1 ESTABLISH INCIDENT RESPONSE RESPONSIBILITIES AND PROCEDURES								
70	**CTRL**	Assign information security incident response responsibilities.	TODO	DONE	N/A			
71	**CTRL**	Establish information security incident response procedures.	TODO	DONE	N/A			
72	**CTRL**	Make sure that your response to information security incidents is quick, effective, and orderly.	TODO	DONE	N/A			
73	GUIDE	Make sure that your incident response procedures can handle a wide variety of information security incidents.	TODO	DONE	N/A			
74	GUIDE	Develop procedures to handle information system failures.	TODO	DONE	N/A			
75	GUIDE	Develop procedures to handle the misuse of systems.	TODO	DONE	N/A			
76	GUIDE	Develop procedures to handle the loss of service.	TODO	DONE	N/A			
77	GUIDE	Develop procedures to handle malicious code incidents.	TODO	DONE	N/A			
78	GUIDE	Develop procedures to handle denial of service attacks.	TODO	DONE	N/A			
79	GUIDE	Develop procedures to handle incomplete business data.	TODO	DONE	N/A			
80	GUIDE	Develop procedures to handle inaccurate business data.	TODO	DONE	N/A			
81	GUIDE	Develop procedures to handle confidentiality breaches.	TODO	DONE	N/A			
82	GUIDE	Develop procedures to handle integrity breaches.	TODO	DONE	N/A			
83	GUIDE	Make sure that your security incident response procedures expect people to identify and analyze the causes of your information security incidents.	TODO	DONE	N/A			
84	GUIDE	Make sure that your security incident response procedures expect people to figure out how to contain the damage.	TODO	DONE	N/A			
85	GUIDE	Make sure that your security incident response procedures expect people to plan how to implement corrective actions.	TODO	DONE	N/A			
86	GUIDE	Make sure that your security incident response procedures expect people to plan how to implement preventive actions.	TODO	DONE	N/A			
87	GUIDE	Make sure that your security incident response procedures expect people to take corrective and preventive actions.	TODO	DONE	N/A			

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

13. INFORMATION SECURITY INCIDENT MANAGEMENT			RESPONSES			ASSIGNED TO	START	FINISH
88	GUIDE	Make sure that your security incident response procedures expect people to communicate with those who are affected by information security incidents.	TODO	DONE	N/A			
89	GUIDE	Make sure that your security incident response procedures expect people to communicate with those who are trying to recover from information security incidents.	TODO	DONE	N/A			
90	GUIDE	Make sure that your security incident response procedures expect people to report corrective and preventive actions to the appropriate authorities.	TODO	DONE	N/A			
91	GUIDE	Make sure that your security incident response procedures expect people to study audit trails and collect evidence about your information security incidents (see 13.2.3).	TODO	DONE	N/A			
92	GUIDE	Use evidence to analyze your security incidents.	TODO	DONE	N/A			
93	GUIDE	Collect forensic evidence for breach of contract purposes.	TODO	DONE	N/A			
94	GUIDE	Collect forensic evidence to address regulatory violations.	TODO	DONE	N/A			
95	GUIDE	Collect forensic evidence to support legal proceedings.	TODO	DONE	N/A			
96	GUIDE	Collect evidence in compliance with computer misuse or data protection legislation.	TODO	DONE	N/A			
97	GUIDE	Collect evidence to support your compensation negotiations with software and service suppliers.	TODO	DONE	N/A			
98	GUIDE	Control actions taken to recover from security breaches.	TODO	DONE	N/A			
99	GUIDE	Control actions taken to correct information system failures.	TODO	DONE	N/A			
100	GUIDE	Establish procedures to control how people correct and recover from information security failures.	TODO	DONE	N/A			
101	GUIDE	Make sure that your recovery procedures allow only authorized personnel to access live systems and data (see section 6.2 on controlling external party access).	TODO	DONE	N/A			
102	GUIDE	Make sure that your recovery procedures expect people to document all emergency responses in great detail.	TODO	DONE	N/A			
103	GUIDE	Make sure that your recovery procedures expect people to report emergency responses to management.	TODO	DONE	N/A			

13. INFORMATION SECURITY INCIDENT MANAGEMENT			RESPONSES			ASSIGNED TO	START	FINISH
104	GUIDE	Make sure that recovery procedures expect management to carry out an orderly review of emergency responses.	TODO	DONE	N/A			
105	GUIDE	Make sure that your recovery procedures expect people to promptly verify the integrity of vulnerable business systems.	TODO	DONE	N/A			
106	GUIDE	Make sure that your recovery procedures expect people to promptly verify that all relevant controls are still effective.	TODO	DONE	N/A			
107	GUIDE	Establish your organization's information security incident management objectives and priorities.	TODO	DONE	N/A			
108	GUIDE	Make sure that those responsible for handling security incidents understand your organization's information security incident management objectives and priorities.	TODO	DONE	N/A			
109	NOTE	Coordinate your response to information security incidents with external organizations whenever security incidents transcend organizational boundaries.	TODO	DONE	N/A			
110	NOTE	Coordinate your response to information security incidents with external organizations whenever security incidents transcend national boundaries.	TODO	DONE	N/A			
13.2.2 LEARN FROM YOUR INFORMATION SECURITY INCIDENTS								
111	**CTRL**	Develop mechanisms that you can use to learn about your organization's information security incidents.	TODO	DONE	N/A			
112	**CTRL**	Monitor and quantify the types of security incidents.	TODO	DONE	N/A			
113	**CTRL**	Monitor and quantify the volume of security incidents.	TODO	DONE	N/A			
114	**CTRL**	Monitor and quantify the costs of security incidents.	TODO	DONE	N/A			
115	**CTRL**	Evaluate your organization's information security incidents.	TODO	DONE	N/A			
116	GUIDE	Use your organization's security incident evaluations to identify recurring information security incidents.	TODO	DONE	N/A			
117	GUIDE	Use your organization's security incident evaluations to identify high impact information security incidents.	TODO	DONE	N/A			
118	NOTE	Use what you learn about security incidents to improve your organization's information security program.	TODO	DONE	N/A			

13. INFORMATION SECURITY INCIDENT MANAGEMENT			RESPONSES			ASSIGNED TO	START	FINISH
119	NOTE	Use what you learn about security incidents to decide whether or not you need to enhance your information security controls or to add new ones.	TODO	DONE	N/A			
120	NOTE	Use what you learn about security incidents to reduce the frequency of future information security incidents.	TODO	DONE	N/A			
121	NOTE	Use what you learn about security incidents to reduce the damage caused by future information security incidents.	TODO	DONE	N/A			
122	NOTE	Use what you learn about security incidents to reduce the cost of future information security incidents.	TODO	DONE	N/A			
123	NOTE	Use what you learn about security incidents to improve your organization's information security policy (see 5.1.2).	TODO	DONE	N/A			
13.2.3 COLLECT EVIDENCE TO SUPPORT YOUR ACTIONS								
124	**CTRL**	Collect evidence after an information security incident whenever a civil or criminal action against a person or organization may be necessary.	TODO	DONE	N/A			
125	**CTRL**	Retain evidence related to information security incidents whenever civil or criminal action may be necessary.	TODO	DONE	N/A			
126	**CTRL**	Make sure that your evidence complies with the rules of evidence established by the jurisdictions that govern your organization.	TODO	DONE	N/A			
127	GUIDE	Establish procedures to control how evidence to support internal disciplinary actions is collected and presented.	TODO	DONE	N/A			
128	GUIDE	Follow the procedures you have developed to collect and present evidence in support of internal disciplinary actions.	TODO	DONE	N/A			
129	GUIDE	Make sure that your evidence will be admissible and can be formally used in a court of law.	TODO	DONE	N/A			
130	GUIDE	Safeguard the quality and completeness of your evidence to ensure that your evidence supports your legal position.	TODO	DONE	N/A			
131	GUIDE	Identify a published standard or code of practice that you can use to help prove that your information systems are able to produce evidence that is admissible in a court of law.	TODO	DONE	N/A			
132	GUIDE	Make sure that your information systems comply with a published evidentiary standard or code of practice.	TODO	DONE	N/A			

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

13. INFORMATION SECURITY INCIDENT MANAGEMENT			RESPONSES			ASSIGNED TO	START	FINISH
133	GUIDE	Make sure that you can prove that your process controls are working correctly and consistently and are therefore able to protect the quality of the evidence that is being processed and stored in your information systems.	TODO	DONE	N/A			
134	GUIDE	Make sure that the weight of your evidence can support any legal actions that may need to be taken.	TODO	DONE	N/A			
135	GUIDE	Increase the weight of your evidence by establishing a strong trail of evidence.	TODO	DONE	N/A			
136	GUIDE	Establish a strong evidence trail by safeguarding all related original paper records and documents.	TODO	DONE	N/A			
137	GUIDE	Establish a strong evidence trail by recording who found related paper documents including when and where they were found.	TODO	DONE	N/A			
138	GUIDE	Establish a strong evidence trail by recording who witnessed the discovery of related paper documents.	TODO	DONE	N/A			
139	GUIDE	Establish a strong evidence trail by ensuring that original paper documents are not tampered with during an investigation.	TODO	DONE	N/A			
140	GUIDE	Establish a strong evidence trail by safeguarding related information on all computer media.	TODO	DONE	N/A			
141	GUIDE	Establish a strong evidence trail by taking copies of related removable media in order to ensure that your evidence is available when you need it.	TODO	DONE	N/A			
142	GUIDE	Establish a strong evidence trail by taking copies of related information on hard disks or memory in order to ensure that your evidence is available when you need it.	TODO	DONE	N/A			
143	GUIDE	Establish a strong evidence trail by making sure that your copying processes are witnessed by trustworthy personnel.	TODO	DONE	N/A			
144	GUIDE	Establish a strong evidence trail by ensuring that the original media is untouched and securely stored.	TODO	DONE	N/A			
145	GUIDE	Establish a strong evidence trail by keeping a log of all steps taken during the copying process.	TODO	DONE	N/A			
146	GUIDE	Establish a strong evidence trail by ensuring that a log of all copying activities is untouched and securely stored.	TODO	DONE	N/A			

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

13. INFORMATION SECURITY INCIDENT MANAGEMENT			RESPONSES			ASSIGNED TO	START	FINISH
147	GUIDE	Protect the integrity of all evidential material.	TODO	DONE	N/A			
148	GUIDE	Perform forensic work on copies (not originals) of evidential material.	TODO	DONE	N/A			
149	GUIDE	Make sure that the copying of forensic materials is observed and supervised by trustworthy personnel.	TODO	DONE	N/A			
150	GUIDE	Maintain a log of all steps taken to copy forensic materials.	TODO	DONE	N/A			
151	GUIDE	Record who copied your forensic materials, what tools and programs were used, and when and where this was done.	TODO	DONE	N/A			
152	NOTE	Make sure that evidence related to information security incidents is not accidentally or intentionally destroyed before you grasp the seriousness of the incident.	TODO	DONE	N/A			
153	NOTE	Involve a lawyer or the police as early as possible whenever you believe that a serious security incident has occurred that could result in legal action.	TODO	DONE	N/A			
154	NOTE	Make sure that your organization is entitled to collect evidence even though the evidence transcends organizational boundaries.	TODO	DONE	N/A			
155	NOTE	Make sure that your organization is entitled to collect evidence even though the evidence transcends jurisdictional boundaries.	TODO	DONE	N/A			
156	NOTE	Make sure that your evidence will be admissible in all relevant jurisdictions.	TODO	DONE	N/A			

Consider each task on the left and select a response. If you haven't done it and you feel it needs to be done, select *TODO*. Select *TODO* if the task addresses one of your information security risks or needs. If you've already done the task, select *DONE*. If the task is not applicable in your situation or it does not address your security risks and needs, then answer N/A (not applicable). Also, please use the three columns on the right to assign tasks to people and to record the date the task was started and the date it was finished.

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: