Appendix.1 Risk Check Instruction

Risk Check Book Instruction	
Risk Check Book is used in a plan phase of ISMS. Follow the instruction below step by step.	
Step 1	Identify assets.
Step 1.1	Walkthrough the assets listed at column C in Risk Check sheet. It defines six types of asset; Information, People, Facility, Paper, Client hardware and software, and Network and server.
Step 1.2	Divide assets according to the organization structure.
	Information and People assets are supposed to be defined at ministry level in accordance with the usual governance .
	Facility, Paper, Client hardware and software, Network and server assets are supposed to be defined by department for each to check by itself.
Step 1.3	Edit column C & D according to the division you made at Step 1.2.
	You can copy & paste an asset by row in order to check by department. However, an asset has multiple check items to identify risks. Be careful to copy a group of rows to include all items.
Step 2	Evaluate assets.
Step 2.1	Evaluate confidentiality, integrity and availability to apply the criteria described in Evaluation Table sheet.
	You can select one from a pull down menu in each field at column G, H and I.
	Use a default value if you feel difficult to evaluate.
Step 2.2	Risk Check sheet automatically display the total evaluation of an asset at column J.
	Review the result and check with the criteria listed in Evaluation Table sheet. Revise confidentiality, integrity and availability evaluation if you feel a total asset value is different from actual.
Step 3	Check assets.
Step 3.1	Read column L and M, and choose just yes or no at column N.
Step 4	Evaluate risks.
Step 4.1	Evaluate threat and vulnerability to apply the criteria described in Evaluation Table sheet.
	You can select one from a pull down menu in each field at column P and R.
	Read the description of each threat at column Q for assistance to decide threat evaluation.
	Use a default value if you feel difficult to evaluate.
Step 4.2	Risk Check sheet automatically display the total evaluation of a risk at column T.
	Review the result and check with the criteria listed in Evaluation Table sheet. Revise threat and vulnerability evaluation if you feel a total risk value is different from actual.
	Go to Step 5 if the total risk is High. Consider the consistency of ISMS if the total risk is Low and make an arrangement if any (e.g. update the existing rulebook or update the control reference at column V.)
Step 5	Decide controls.
Step 5.1	Read the description of default control contents at column U.
Step 5.2	Read the description of sample information security rulebook referred at column V.
Step 5.3	Decide the applicability of implementing the rule and procedures in the sample information security rulebook. Decide the alternatives if not applicable.
Step 5.4	Update the control contents at column U, reference at column V, and the rule and procedures which is applicable and can be implemented to the organization.
Step 6	Evaluate risks after control.
Step 6.1	Evaluate threat and vulnerability to apply the criteria described in Evaluation Table sheet.
	You can select one from a pull down menu in each field at column W and Y.
	Use a default value if you do not change the controls and the rule and procedures in the sample IS handbook.
Step 6.2	Risk Check sheet automatically display the total evaluation of a risk at column AA.
	Review the result and check with the criteria listed in Evaluation Table sheet. Revise threat and vulnerability valuation if you feel a total risk value is different from actual.
Step 6.3	Make sure it is preferable to get each total risk classified as Low. Decide take additional actions to lessen risks, or describe a residual risk statement to accept.

SECTION 4
Government Information Security Management System Risk Check

- Drafted by Yusuke Tanaka, JICA Expert
- Edited by ICT Security Management Technical Team (iSMTT).

Risk Check

#	Assets L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Asset Evaluation Confidential	Integrity	Availability	Total	Check item Check Type	Check item	Check results	Comments on Check Results
1	Basic Check List								Basic			
2	NIDA_CISO											
3		Information										
4			Classification		5: Confident	5: High	5: High	3: High				
5									Classification	Define the security classification of information.	1: No	
6									Control	Define information control according to the classification.	1: No	
7									Protection	Define how to save and protect information against unauthorized access.	1: No	
8									Record	Define how to keep a record. (a media and a keeping period)	1: No	
9			Privacy information		5: Confident	5: High	5: High	3: High				
10									Classification	Classify privacy information always as confidential.	1: No	
11		People										
12			Information security organization		5: Confident	5: High	5: High	3: High				
13									Organization	Define and name information security manager (IS manager).	1: No	
14			Government officials						-to be defined and implemented in the future.			
15									Hiring	Evaluate information security factors when selecting candidates.	0: Yes / NA	
16									Orientation	Get trained information security and state the nondisclosure obligation.	0: Yes / NA	
17									Termination	Check ...	0: Yes / NA	
18			External parties						-to be defined and implemented in the future.			
19									Accessible area	Define an accessible area for each external party.	0: Yes / NA	
20			Purchasing equipments						-to be defined and implemented in the future.			
21			Outsourcing						-to be defined and implemented in the future.			
22									Contractor selection	Evaluate information security factors when selecting contractors.	0: Yes / NA	
23									Contract	Define the nondisclosure obligation clearly in a contract.	0: Yes / NA	
24			Software development						-to be defined and implemented in the future.			
25		Facility										
26			Office building		2: Internal	5: High	5: High	2: Middle				
27									User definition	Define those who can enter the facility/room.	1: No	
28									Key system	Implement an appropriate key system for an entrance of the facility/room.	1: No	
29									Zoning	Separate an office space and the other accessible common space.	1: No	
30									Outsiders	Get outsiders with an insider attendant.	1: No	
31									Entry /exit record	Record an entry and exit.	1: No	
32									Goods shipping record	Keep records of courier service.	1: No	
33			Cabinet		2: Internal	5: High	5: High	2: Middle				
34									Cabinet lock-up	Store information assets with confidential information and lock up cabinets.	1: No	
35			Fax machines and printers		2: Internal	5: High	5: High	2: Middle				
36									Disposal	Dispose printed materials/faxed materials with care.	1: No	
37									Faxing record	Keep record of faxing (sending/receiving).	1: No	
38			Desk		2: Internal	5: High	5: High	2: Middle				
39									Desk lock-up	Lock up desk drawers when leaving.	1: No	
40									Desktop clean-up	Leave nothing on a desktop, especially confidential information.	1: No	
41		Physical information										
42			Paper		2: Internal	5: High	5: High	2: Middle				
43									Classification	Identify confidential information within each paper/document.	1: No	
44									Protection	Save confidential paper/documents in safe against unauthorized access.	1: No	
45									Disposal	Use a paper shredder when disposing confidentials, Or burn it by official.	1: No	
46			Digital Archives (DVDs/CDs/FDs/Tapes)		2: Internal	3: Middle	1: Low	1: Low				
47									Classification	Identify confidential information within each archive.	1: No	
48									Protection	Save confidential archives in safe against unauthorized access.	1: No	
49									Disposal	Scrap a media (Tape/FD/CD/DVD) physically.	1: No	

	Assets				Asset Evaluation				Check item			
#	L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Confidential	Integrity	Availability	Total	Check Type	Check item	Check results	Comments on Check Results
50				Client PC (hardware and software)								
51				Desktop PC	2: Internal	3: Middle	1: Low	1: Low				
52									Assignment	Assign one main user at minimum to all PCs.	1: No	
53									User ID and password	Use a robust password and change one periodically.	1: No	
54									User ID sharing	Prohibit share user ID and password with several people.	1: No	
55									Cleared screen	Clear a display screen by setting screen saver function with password.	1: No	
56									Anti-virus protection	Scan a local storage with anti-virus software periodically.	1: No	
57									Anti-virus protection	Use an automatic virus detection function usually.	1: No	
58									Anti-virus protection	Update a virus definition file periodically.	1: No	
59									Anti-virus protection	Keep records of scanning and updating virus definitions.	1: No	
60									UPS	Connect UPS for all desktop PCs.	1: No	
61									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
62				Laptop /mobile PC (All desktop PC check items must be applied.)	2: Internal	3: Middle	1: Low	1: Low				
63									Security wire	Wire all laptop /mobile PCs physically to desks or store at a locked facility.	1: No	
64				Storage devices (Portable HDDs /Memory sticks /Memory cards)	2: Internal	3: Middle	1: Low	1: Low				
65									Anti-virus protection	Scan storage devices with anti-virus software periodically.	1: No	
66									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
67				Personal asset (Personally owned PC, storage devices and digital archi	2: Internal	3: Middle	1: Low	1: Low				
68									Permission	Get a permission from IS manager to take in/out a personal asset to/from an office.	1: No	
69				Software	2: Internal	3: Middle	1: Low	1: Low				
70									Installation	Install software explicitly allowed by IS manager.	1: No	
71									Software configuration	Configure software according to IS managers' instruction.	1: No	
72									Patch application	Apply patches according to IS managers' request.	1: No	
73									Mail encryption	Encrypt to send an e-mail.	1: No	
74									Miss-addressing mails	Report and take appropriate actions when miss-addressing mails.	1: No	
75									Integrity consideration	Consider the integrity of a document and deliver one in PDF format when copying.	1: No	
76									Web downloading	Download a web browser executable only which has an electronic signature.	1: No	

#	Assets L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Asset Evaluation Confidential	Integrity	Availability	Total	Check item Check Type	Check item	Check results	Comments on Check Results
77	NiDA: CamCERT											
78		Facility										
79			Office building		2: Internal	5: High	5: High	2: Middle				
80									User definition	Define those who can enter the facility/room.	1: No	
81									Key system	Implement an appropriate key system for an entrance of the facility/room.	1: No	
82									Zoning	Separate an office space and the other accessible common space.	1: No	
83									Outsiders	Get outsiders with an insider attendant.	1: No	
84									Entry /exit record	Record an entry and exit.	1: No	
85									Goods shipping record	Keep records of courier service.	1: No	
86			Cabinet		2: Internal	5: High	5: High	2: Middle				
87									Cabinet lock-up	Store information assets with confidential information and lock up cabinets.	1: No	
88			Fax machines and printers		2: Internal	5: High	5: High	2: Middle				
89									Disposal	Dispose printed materials/faxed materials with care.	1: No	
90									Faxing record	Keep record of faxing (sending/receiving).	1: No	
91			Desk		2: Internal	5: High	5: High	2: Middle				
92									Desk lock-up	Lock up desk drawers when leaving.	1: No	
93									Desktop clean-up	Leave nothing on a desktop, especially confidential information.	1: No	
94		Physical information										
95			Paper		2: Internal	5: High	5: High	2: Middle				
96									Classification	Identify confidential information within each paper/document.	0: Yes / NA	
97									Protection	Save confidential paper/documents in safe against unauthorized access.	1: No	
98									Disposal	Use a paper shredder when disposing confidentials. Or burn it by official.	1: No	
99			Digital Archives (DVDs/CDs/FDs/Tapes)		2: Internal	3: Middle	1: Low	1: Low				
100									Classification	Identify confidential information within each archive.	1: No	
101									Protection	Save confidential archives in safe against unauthorized access.	1: No	
102									Disposal	Scrap a media (Tape/FD/CD/DVD) physically.	1: No	
103		Client PC (hardware and software)										
104			Desktop PC		2: Internal	3: Middle	1: Low	1: Low				
105									Assignment	Assign one main user at minimum to all PCs.	1: No	
106									User ID and password	Use a robust password and change one periodically.	1: No	
107									User ID sharing	Prohibit share user ID and password with several people.	1: No	
108									Cleared screen	Clear a display screen by setting screen saver function with password.	1: No	
109									Anti-virus protection	Scan a local storage with anti-virus software periodically.	1: No	
110									Anti-virus protection	Use an automatic virus detection function usually.	1: No	
111									Anti-virus protection	Update a virus definition file periodically.	1: No	
112									Anti-virus protection	Keep records of scanning and updating virus definitions.	1: No	
113									UPS	Connect UPS for all desktop PCs.	1: No	
114									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
115			Laptop /mobile PC (All desktop PC check items must be applied.)		2: Internal	3: Middle	1: Low	1: Low				
116									Security wire	Wire all laptop /mobile PCs physically to desks or store at a locked facility.	1: No	
117			Storage devices (Portable HDDs /Memory sticks /Memory cards)		2: Internal	3: Middle	1: Low	1: Low				
118									Anti-virus protection	Scan storage devices with anti-virus software periodically.	1: No	
119									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
120			Personal asset (Personally owned PC, storage devices and digital archi		2: Internal	3: Middle	1: Low	1: Low				
121									Permission	Get a permission from IS manager to take in/out a personal asset to/from an office.	1: No	
122			Software		2: Internal	3: Middle	1: Low	1: Low				
123									Installation	Install software explicitly allowed by IS manager.	1: No	
124									Software configuration	Configure software according to IS managers' instruction.	1: No	
125									Patch application	Apply patches according to IS managers' request.	1: No	
126									Mail encryption	Encrypt to send an e-mail.	1: No	
127									Miss-addressing mails	Report and take appropriate actions when miss-addressing mails.	1: No	
128									Integrity consideration	Consider the integrity of a document and deliver one in PDF format when copying.	1: No	
129									Web downloading	Download a web browser executable only which has an electronic signature.	1: No	

	Assets			Asset Evaluation				Check item			
#	L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Confidential	Integrity	Availability	Total	Check Type	Check item	Check results	Comments on Check Results
130				Network and server								
131				LAN and Internet	2: Internal	3: Middle	1: Low	1: Low				
132									Firewall	Disconnect an internal network from an external network.	1: No	
133									Record	Record a network access.	1: No	
134									Audit and action	Audit records, detect unauthorized access and take actions promptly.	1: No	
135									UPS	Connect UPS for all network devices.	1: No	
136				Server common	2: Internal	3: Middle	1: Low	1: Low				
137									Zoning control	Segregate a server room and lock up the room usually.	1: No	
138									Physical installation	Install servers physically in safe from destruction.	1: No	
139									Physical protection	Lock up a server rack from unauthorized access.	1: No	
140									User definition	Define those who can enter the server room.	1: No	
141									User ID and password	Use a robust password and change one periodically.	1: No	
142									User ID sharing	Prohibit share user ID and password with several people.	1: No	
143									Operation manual	Document an operation manual and lessen human errors.	1: No	
144									Data access control	Control data access appropriately with the access control functions of file/data systems.	1: No	
145									Data protection	Encrypt data appropriately in case of a forced attack.	1: No	
146									Data back-up	Back up data periodically.	1: No	
147									Archive protection	Save confidential archives in safe against unauthorized access.	1: No	
148									Data recovery	Have a capacity to recover data defined in a service level agreement.	1: No	
149									Record	Record a data access and keep it for the defined period of time.	1: No	
150									Anti-virus protection	Scan a local storage with anti-virus software periodically.	1: No	
151									Anti-virus protection	Use an automatic virus detection function usually.	1: No	
152									Anti-virus protection	Update a virus definition file peripdically.	1: No	
153									Anti-virus protection	Keep records of scanning and updating virus definitions.	1: No	
154									Audit and action	Audit records, detect unauthorized access /execution and take actions promptly.	1: No	
155									Information gathering	Gather external security information to take actions proactively.	1: No	
156									Patch application	Apply patches depending on its emergency and stability.	1: No	
157									UPS	Connect UPS for all servers.	1: No	

	Assets				Asset Evaluation				Check item			
#	L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Confidential	Integrity	Availability	Total	Check Type	Check item	Check results	Comments on Check Results
158	GAIS											
159		Network and server			2: Internal	3: Middle	3: Middle	2: Middle				
160									Firewall	Disconnect an internal network from an external network.	1: No	Suspended until PAIS integrating GAIS
161									Record	Record a network access.	1: No	
162									Audit and action	Audit records, detect unauthorized access and take actions promptly.	1: No	
163									UPS	Connect UPS for all network devices.	1: No	
164			Server common		2: Internal	3: Middle	3: Middle	2: Middle				
165									Zoning control	Segregate a server room and lock up the room usually.	1: No	
166									Physical installation	Install servers physically in safe from destruction.	1: No	
167									Physical protection	Lock up a server rack from unauthorized access.	1: No	
168									User definition	Define those who can enter the server room.	1: No	
169									User ID and password	Use a robust password and change one periodically.	1: No	
170									User ID sharing	Prohibit share user ID and password with several people.	1: No	
171									Operation manual	Document an operation manual and lessen human errors.	1: No	
172									Data access control	Control data access appropriately with the access control functions of file/data systems.	1: No	
173									Data protection	Encrypt data appropriately in case of a forced attack.	1: No	
174									Data back-up	Back up data periodically.	1: No	
175									Archive protection	Save confidential archives in safe against unauthorized access.	1: No	
176									Data recovery	Have a capacity to recover data defined in a service level agreement.	1: No	
177									Record	Record a data access and keep it for the defined period of time.	1: No	
178									Anti-virus protection	Scan a local storage with anti-virus software periodically.	1: No	
179									Anti-virus protection	Use an automatic virus detection function usually.	1: No	
180									Anti-virus protection	Update a virus definition file periodically.	1: No	
181									Anti-virus protection	Keep records of scanning and updating virus definitions.	1: No	
182									Audit and action	Audit records, detect unauthorized access /execution and take actions promptly.	1: No	
183									Information gathering	Gather external security information to take actions proactively.	1: No	
184									Patch application	Apply patches depending on its emergency and stability.	1: No	
185									UPS	Connect UPS for all servers.	1: No	

#	Assets L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Asset Evaluation Confidential	Integrity	Availability	Total	Check item Check Type	Check item	Check results	Comments on Check Results
186	Secretary General Office											
187		Facility										
188			Office building		2: Internal	5: High	5: High	2: Middle				
189									User definition	Define those who can enter the facility/room.	0: Yes / NA	
190									Key system	Implement an appropriate key system for an entrance of the facility/room.	0: Yes / NA	
191									Zoning	Separate an office space and the other accessible common space.	0: Yes / NA	
192									Outsiders	Get outsiders with an insider attendant.	0: Yes / NA	
193									Entry /exit record	Record an entry and exit.	1: No	
194									Goods shipping record	Keep records of courier service.	1: No	
195			Cabinet		5: Confident	5: High	5: High	3: High				
196									Cabinet lock-up	Store information assets with confidential information and lock up cabinets.	1: No	
197			Fax machines and printers		2: Internal	5: High	5: High	2: Middle				
198									Disposal	Dispose printed materials/faxed materials with care.	0: Yes / NA	
199									Faxing record	Keep record of faxing (sending/receiving).	1: No	
200			Desk		5: Confident	5: High	5: High	3: High				
201									Desk lock-up	Lock up desk drawers when leaving	0: Yes / NA	
202									Desktop clean-up	Leave nothing on a desktop, especially confidential information.	0: Yes / NA	
203		Physical information										
204			Paper		5: Confident	5: High	5: High	3: High				
205									Classification	Identify confidential information within each paper/document.	0: Yes / NA	
206									Protection	Save confidential paper/documents in safe against unauthorized access.	0: Yes / NA	
207									Disposal	Use a paper shredder when disposing confidentials. Or burn it by official.	0: Yes / NA	
208			Digital Archives (DVDs/CDs/FDs/Tapes)		2: Internal	3: Middle	1: Low	1: Low				
209									Classification	Identify confidential information within each archive.	1: No	
210									Protection	Save confidential archives in safe against unauthorized access.	1: No	
211									Disposal	Scrap a media (Tape/FD/CD/DVD) physically.	1: No	
212		Client PC (hardware and software)										
213			Desktop PC		5: Confident	3: Middle	3: Middle	2: Middle				
214									Assignment	Assign one main user at minimum to all PCs.	0: Yes / NA	
215									User ID and password	Use a robust password and change one periodically.	1: No	
216									User ID sharing	Prohibit share user ID and password with several people.	1: No	
217									Cleared screen	Clear a display screen by setting screen saver function with password.	1: No	
218									Anti-virus protection	Scan a local storage with anti-virus software periodically.	1: No	
219									Anti-virus protection	Use an automatic virus detection function usually.	0: Yes / NA	
220									Anti-virus protection	Update a virus definition file periodically.	0: Yes / NA	
221									Anti-virus protection	Keep records of scanning and updating virus definitions.	1: No	
222									UPS	Connect UPS for all desktop PCs.	1: No	
223									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
224			Laptop /mobile PC (All desktop PC check items must be applied.)		2: Internal	3: Middle	1: Low	1: Low				
225									Security wire	Wire all laptop /mobile PCs physically to desks or store at a locked facility.	1: No	
226			Storage devices (Portable HDDs /Memory sticks /Memory cards)		2: Internal	3: Middle	1: Low	1: Low				
227									Anti-virus protection	Scan storage devices with anti-virus software periodically.	1: No	
228									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
229			Personal asset (Personally owned PC, storage devices and digital archi		2: Internal	3: Middle	1: Low	1: Low				
230									Permission	Get a permission from IS manager to take in/out a personal asset to/from an office.	1: No	
231			Software		2: Internal	3: Middle	1: Low	1: Low				
232									Installation	Install software explicitly allowed by IS manager.	1: No	
233									Software configuration	Configure software according to IS managers' instruction.	1: No	
234									Patch application	Apply patches according to IS managers' request.	1: No	
235									Mail encryption	Encrypt to send an e-mail.	1: No	
236									Miss-addressing mails	Report and take appropriate actions when miss-addressing mails.	1: No	
237									Integrity consideration	Consider the integrity of a document and deliver one in PDF format when copying.	1: No	
238									Web downloading	Download a web browser executable only which has an electronic signature.	1: No	
239												
240												

Risk Check

	Assets				Asset Evaluation				Check item			
#	L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Confidential	Integrity	Availability	Total	Check Type	Check item	Check results	Comments on Check Results
241	Extended								Extended			
242				Network and Server								
243				LAN and Internet					-to be defined and implemented in the future.			
244										Protection of network	0: Yes / NA	
245										Security measure of network equipment	0: Yes / NA	
246									Remote access	Limit an access capacity from external networks considering its risks.	0: Yes / NA	
247									Wireless LAN	Consider its risks to...	0: Yes / NA	
248				Server common					-to be defined and implemented in the future.			
249									Security holes treatment		0: Yes / NA	
250									Malware treatment		0: Yes / NA	
251									DOS treatment		0: Yes / NA	
252									Stepping stone treatment		0: Yes / NA	
253									Domain name		0: Yes / NA	
254				Server application common					-to be defined and implemented in the future.			
255									Authentication		0: Yes / NA	
256									Access control		0: Yes / NA	
257									Administration		0: Yes / NA	
258									Audit trail		0: Yes / NA	
259									Assurance		0: Yes / NA	
260									Encryption		0: Yes / NA	
261												

	Assets			Asset Evaluation				Check item			
#	1.1	1.2	1.3	Description (Attributes, Location, Manager in charge, # of Assets)	Confidential	Integrity	Availability	Total	Check Type	Check item	Check results	Comments on Check Results
262	Network											
263		Facility										
264				Office building	2: Internal	5: High	5: High	2: Middle				
265									User definition	Define those who can enter the facility/room.	0: Yes / NA	
266									Key system	Implement an appropriate key system for an entrance of the facility/room.	1: No	
267									Zoning	Separate an office space and the other accessible common space.	0: Yes / NA	
268									Outsiders	Get outsiders with an insider attendant.	1: No	
269									Entry /exit record	Record an entry and exit.	1: No	
270									Goods shipping record	Keep records of courier service.	1: No	
271				Cabinet	2: Internal	5: High	5: High	2: Middle				
272									Cabinet lock-up	Store information assets with confidential information and lock up cabinets.	1: No	
273				Fax machines and printers	2: Internal	5: High	5: High	2: Middle				
274									Disposal	Dispose printed materials/faxed materials with care.	1: No	
275									Faxing record	Keep record of faxing (sending/receiving)	1: No	
276				Desk	2: Internal	5: High	5: High	2: Middle				
277									Desk lock-up	Lock up desk drawers when leaving	1: No	
278									Desktop clean-up	Leave nothing on a desktop, especially confidential information.	1: No	
279		Physical information										
280				Paper	2: Internal	5: High	5: High	2: Middle				
281									Classification	Identify confidential information within each paper/document.	1: No	
282									Protection	Save confidential paper/documents in safe against unauthorized access.	1: No	
283									Disposal	Use a paper shredder when disposing confidentials. Or burn it by official.	1: No	
284				Digital Archives (DVDs/CDs/FDs/Tapes)	2: Internal	5: High	5: High	2: Middle				
285									Classification	Identify confidential information within each archive.	1: No	
286									Protection	Save confidential archives in safe against unauthorized access.	1: No	
287									Disposal	Scrap a media (Tape/FD/CD/DVD) physically.	1: No	
288				Client PC (hardware and software)								
289				Desktop PC	2: Internal	5: High	5: High	2: Middle				
290									Assignment	Assign one main user at minimum to all PCs.	1: No	
291									User ID and password	Use a robust password and change one periodically.	1: No	
292									User ID sharing	Prohibit share user ID and password with several people.	0: Yes / NA	
293									Cleared screen	Clear a display screen by setting screen saver function with password.	0: Yes / NA	
294									Anti-virus protection	Scan a local storage with anti-virus software periodically.	1: No	
295									Anti-virus protection	Use an automatic virus detection function usually.	0: Yes / NA	
296									Anti-virus protection	Update a virus definition file periodically.	0: Yes / NA	
297									Anti-virus protection	Keep records of scanning and updating virus definitions.	1: No	
298									UPS	Connect UPS for all desktop PCs.	1: No	
299									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
300				Laptop /mobile PC (All desktop PC check items must be applied.)	2: Internal	5: High	5: High	2: Middle				
301									Security wire	Wire all laptop /mobile PCs physically to desks or store at a locked facility.	1: No	
302				Storage devices (Portable HDDs /Memory sticks /Memory cards)	2: Internal	5: High	5: High	2: Middle				
303									Anti-virus protection	Scan storage devices with anti-virus software periodically.	1: No	
304									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
305				Personal asset (Personally owned PC, storage devices and digital archi	2: Internal	5: High	5: High	2: Middle				
306									Permission	Get a permission from IS manager to take in/out a personal asset to/from an office.	1: No	
307				Software	2: Internal	5: High	5: High	2: Middle				
308									Installation	Install software explicitly allowed by IS manager.	1: No	
309									Software configuration	Configure software according to IS managers' instruction.	1: No	
310									Patch application	Apply patches according to IS managers' request.	1: No	
311									Mail encryption	Encrypt to send an e-mail.	1: No	
312									Miss-addressing mails	Report and take appropriate actions when miss-addressing mails.	1: No	
313									Integrity consideration	Consider the integrity of a document and deliver one in PDF format when copying.	1: No	
314									Web downloading	Download a web browser executable only which has an electronic signature.	1: No	

#	Assets L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Asset Evaluation Confidential	Integrity	Availability	Total	Check item Check Type	Check item	Check results	Comments on Check Results
315	Enterprise											
316		Facility										
317			Office building		2: Internal	5: High	5: High	2: Middle				
318									User definition	Define those who can enter the facility/room.	0: Yes / NA	
319									Key system	Implement an appropriate key system for an entrance of the facility/room.	1: No	
320									Zoning	Separate an office space and the other accessible common space.	0: Yes / NA	
321									Outsiders	Get outsiders with an insider attendant.	0: Yes / NA	
322									Entry /exit record	Record an entry and exit.	1: No	
323									Goods shipping record	Keep records of courier service.	1: No	
324			Cabinet		2: Internal	5: High	5: High	2: Middle				
325									Cabinet lock-up	Store information assets with confidential information and lock up cabinets.	1: No	
326			Fax machines and printers		2: Internal	5: High	5: High	2: Middle				
327									Disposal	Dispose printed materials/faxed materials with care.	1: No	
328									Faxing record	Keep record of faxing (sending/receiving)	1: No	
329			Desk		2: Internal	5: High	5: High	2: Middle				
330									Desk lock-up	Lock up desk drawers when leaving	1: No	
331									Desktop clean-up	Leave nothing on a desktop, especially confidential information.	0: Yes / NA	
332		Physical information										
333			Paper		2: Internal	5: High	5: High	2: Middle				
334									Classification	Identify confidential information within each paper/document.	0: Yes / NA	
335									Protection	Save confidential paper/documents in safe against unauthorized access.	1: No	
336									Disposal	Use a paper shredder when disposing confidentials. Or burn it by offcial.	1: No	
337			Digital Archives (DVDs/CDs/FDs/Tapes)		2: Internal	5: High	5: High	2: Middle				
338									Classification	Identify confidential information within each archive.	1: No	
339									Protection	Save confidential archives in safe against unauthorized access.	1: No	
340									Disposal	Scrap a media (Tape/FD/CD/DVD) physically.	1: No	
341		Client PC (hardware and software)										
342			Desktop PC		2: Internal	5: High	5: High	2: Middle				
343									Assignment	Assign one main user at minimum to all PCs.	1: No	
344									User ID and password	Use a robust password and change one periodically.	1: No	
345									User ID sharing	Prohibit share user ID and password with several people.	1: No	
346									Cleared screen	Clear a display screen by setting screen saver function with password.	1: No	
347									Anti-virus protection	Scan a local storage with anti-virus software periodically.	1: No	
348									Anti-virus protection	Use an automatic virus detection function usually.	0: Yes / NA	
349									Anti-virus protection	Update a virus definition file periodically.	0: Yes / NA	
350									Anti-virus protection	Keep records of scanning and updating virus definitions.	1: No	
351									UPS	Connect UPS for all desktop PCs.	1: No	
352									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
353			Laptop /mobile PC (All desktop PC check items must be applied)		2: Internal	5: High	5: High	2: Middle				
354									Security wire	Wire all laptop /mobile PCs physically to desks or store at a locked facility.	1: No	
355			Storage devices (Portable HDDs /Memory sticks /Memory cards)		2: Internal	5: High	5: High	2: Middle				
356									Anti-virus protection	Scan storage devices with anti-virus software periodically.	1: No	
357									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
358			Personal asset (Personally owned PC, storage devices and digital arch		2: Internal	5: High	5: High	2: Middle				
359									Permission	Get a permission from IS manager to take in/out a personal asset to/from an office.	1: No	
360			Software		2: Internal	5: High	5: High	2: Middle				
361									Installation	Install software explicitly allowed by IS manager.	0: Yes / NA	
362									Software configuration	Configure software according to IS managers' instruction.	0: Yes / NA	
363									Patch application	Apply patches according to IS managers' request.	1: No	
364									Mail encryption	Encrypt to send an e-mail.	1: No	
365									Miss-addressing mails	Report and take appropriate actions when miss-addressing mails.	1: No	
366									Integrity consideration	Consider the integrity of a document and deliver one in PDF format when copying.	1: No	
367									Web downloading	Download a web browser executable only which has an electronic signature.	1: No	

#	Assets L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Asset Evaluation Confidential	Integrity	Availability	Total	Check item Check Type	Check item	Check results	Comments on Check Results
368	Content & Applications											
369		Facility										
370			Office building		2: Internal	5: High	5: High	2: Middle				
371									User definition	Define those who can enter the facility/room.	0: Yes / NA	
372									Key system	Implement an appropriate key system for an entrance of the facility/room.	0: Yes / NA	
373									Zoning	Separate an office space and the other accessible common space.	0: Yes / NA	
374									Outsiders	Get outsiders with an insider attendant.	0: Yes / NA	
375									Entry /exit record	Record an antry and exit.	1: No	
376									Goods shipping record	Keep records of courier service.	1: No	
377			Cabinet		2: Internal	5: High	5: High	2: Middle				
378									Cabinet lock-up	Store information assets with confidential information and lock up cabinets.	1: No	
379			Fax machines and printers		2: Internal	5: High	5: High	2: Middle				
380									Disposal	Dispose printed materials/faxed materials with care.	1: No	
381									Faxing record	Keep record of faxing (sending/receiving).	1: No	
382			Desk		5: Confident	5: High	5: High	3: High				
383									Desk lock-up	Lock up desk drawers when leaving.	0: Yes / NA	
384									Desktop clean-up	Leave nothing on a desktop, especially confidential information.	0: Yes / NA	
385		Physical information										
386			Paper		2: Internal	5: High	5: High	2: Middle				
387									Classification	Identify confidential information within each paper/document.	1: No	
388									Protection	Save confidential paper/documents in safe against unauthorized access.	0: Yes / NA	
389									Disposal	Use a paper shredder when disposing confidentials. Or burn it by offcial.	1: No	
390			Digital Archives (DVDs/CDs/FDs/Tapes)		5: Confident	5: High	5: High	3: High				
391									Classification	Identify confidential information within each archive.	0: Yes / NA	
392									Protection	Save confidential archives in safe against unauthorized access.	0: Yes / NA	
393									Disposal	Scrap a media (Tape/FD/CD/DVD) physically.	1: No	
394		Client PC (hardware and software)										
395			Desktop PC		5: Confident	5: High	5: High	3: High				
396									Assignment	Assign one main user at minimum to all PCs.	0: Yes / NA	
397									User ID and password	Use a robust password and change one periodically.	0: Yes / NA	
398									User ID sharing	Prohibit share user ID and password with several people.	0: Yes / NA	
399									Cleared screen	Clear a display screen by setting screen savar function with password.	0: Yes / NA	
400									Anti-virus protection	Scan a local storage with anti-virus software periodically.	0: Yes / NA	
401									Anti-virus protection	Use an automatic virus detection function usually.	0: Yes / NA	
402									Anti-virus protection	Update a virus definition file periodically.	0: Yes / NA	
403									Anti-virus protection	Keep records of scanning and updating virus definitions.	1: No	
404									UPS	Connect UPS for all desktop PCs.	1: No	
405									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
406			Laptop /mobile PC (All desktop PC check items must be applied.)		2: Internal	5: High	5: High	2: Middle				
407									Security wire	Wire all laptop /mobile PCs physically to desks or store at a locked facility.	1: No	
408			Storage devices (Portable HDDs /Memory sticks /Memory cards)		2: Internal	5: High	5: High	2: Middle				
409									Anti-virus protection	Scan storage devices with anti-virus software periodically.	0: Yes / NA	
410									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
411			Personal asset (Personally owned PC, storage devices and digital arch		2: Internal	5: High	5: High	2: Middle				
412									Permission	Get a permission from IS manager to take in/out a personal asset to/from an office.	1: No	
413			Software		2: Internal	5: High	5: High	2: Middle				
414									Installation	Install software explicitly allowed by IS manager.	1: No	
415									Software configuration	Configure software according to IS managers' instruction.	1: No	
416									Patch application	Apply patches according to IS managers' request.	1: No	
417									Mail encryption	Encrypt to send an e-mail.	1: No	
418									Miss-addressing mails	Report and take appropriate actions when miss-addressing mails.	1: No	
419									Integrity consideration	Consider the integrity of a document and deliver one in PDF format when copying.	0: Yes / NA	
420									Web downloading	Download a web browser executable only which has an electronic signature.	1: No	

#	Assets L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Asset Evaluation Confidential	Integrity	Availability	Total	Check item Check Type	Check item	Check results	Comments on Check Results
512	HRD & FOSS (only the training team room was assessed.)											
513		Facility										
514			Office building		2: Internal	5: High	5: High	2: Middle				
515									User definition	Define those who can enter the facility/room.	0: Yes / NA	
516									Key system	Implement an appropriate key system for an entrance of the facility/room.	1: No	
517									Zoning	Separate an office space and the other accessible common space.	0: Yes / NA	
518									Outsiders	Get outsiders with an insider attendant.	0: Yes / NA	
519									Entry /exit record	Record an entry and exit.	1: No	
520									Goods shipping record	Keep records of courier service.	1: No	
521			Cabinet		2: Internal	5: High	5: High	2: Middle				
522									Cabinet lock-up	Store information assets with confidential information and lock up cabinets.	1: No	
523			Fax machines and printers		2: Internal	5: High	5: High	2: Middle				
524									Disposal	Dispose printed materials/faxed materials with care.	1: No	
525									Faxing record	Keep record of faxing (sending/receiving).	1: No	
526			Desk		2: Internal	5: High	5: High	2: Middle				
527									Desk lock-up	Lock up desk drawers when leaving.	1: No	
528									Desktop clean-up	Leave nothing on a desktop, especially confidential information.	0: Yes / NA	
529		Physical information										
530			Paper		2: Internal	5: High	5: High	2: Middle				
531									Classification	Identify confidential information within each paper/document.	1: No	
532									Protection	Save confidential paper/documents in safe against unauthorized access.	1: No	
533									Disposal	Use a paper shredder when disposing confidentials. Or burn it by official.	1: No	
534			Digital Archives (DVDs/CDs/FDs/Tapes)		2: Internal	5: High	5: High	2: Middle				
535									Classification	Identify confidential information within each archive.	0: Yes / NA	
536									Protection	Save confidential archives in safe against unauthorized access.	0: Yes / NA	
537									Disposal	Scrap a media (Tape/FD/CD/DVD) physically.	1: No	
538		Client PC (hardware and software)										
539			Desktop PC		2: Internal	5: High	5: High	2: Middle				
540									Assignment	Assign one main user at minimum to all PCs.	1: No	
541									User ID and password	Use a robust password and change one periodically.	1: No	
542									User ID sharing	Prohibit share user ID and password with several people.	1: No	
543									Cleared screen	Clear a display screen by setting screen saver function with password.	1: No	
544									Anti-virus protection	Scan a local storage with anti-virus software periodically.	1: No	
545									Anti-virus protection	Use an automatic virus detection function usually.	0: Yes / NA	
546									Anti-virus protection	Update a virus definition file periodically.	0: Yes / NA	
547									Anti-virus protection	Keep records of scanning and updating virus definitions.	1: No	
548									UPS	Connect UPS for all desktop PCs.	1: No	
549									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
550			Laptop /mobile PC (All desktop PC check items must be applied)		2: Internal	5: High	5: High	2: Middle				
551									Security wire	Wire all laptop /mobile PCs physically to desks or store at a locked facility.	1: No	
552			Storage devices (Portable HDDs /Memory sticks /Memory cards)		2: Internal	5: High	5: High	2: Middle				
553									Anti-virus protection	Scan storage devices with anti-virus software periodically.	1: No	
554									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
555			Personal asset (Personally owned PC, storage devices and digital archi		2: Internal	5: High	5: High	2: Middle				
556									Permission	Get a permission from IS manager to take in/out a personal asset to/from an office.	1: No	
557			Software		2: Internal	5: High	5: High	2: Middle				
558									Installation	Install software explicitly allowed by IS manager.	1: No	
559									Software configuration	Configure software according to IS managers' instruction.	1: No	
560									Patch application	Apply patches according to IS managers' request.	1: No	
561									Mail encryption	Encrypt to send an e-mail.	1: No	
562									Miss-addressing mails	Report and take appropriate actions when miss-addressing mails.	1: No	
563									Integrity consideration	Consider the integrity of a document and deliver one in PDF format when copying.	1: No	
564									Web downloading	Download a web browser executable only which has an electronic signature.	1: No	

Risk Check

	Risk Evaluation					Control		Risk Evaluation after Control		
#	Threat	Comments on Threat	Vulnarability	Comments on Vulnarability	Total Risk	Control Contents	References	Threat	Vulnarability	Total Risk
1							Rule book or Residual Risk List			
2										
3										
4										
5	2: Middle	Overall	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
6	2: Middle	Overall	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
7	2: Middle	Overall	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
8	2: Middle	Overall	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
9										
10	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
11										
12										
13	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
14										
15										
16										
17										
18										
19										
20										
21										
22										
23										
24										
25										
26										
27	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
28	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
29	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
30	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
31	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
32	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
33										
34	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
35										
36	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
37	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
38										
39	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
40	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
41										
42										
43	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
44	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
45	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
46										
47	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
48	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
49	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)

#	Risk Evaluation					Control		Risk Evaluation after Control		
	Threat	Comments on Threat	Vulnarability	Comments on Vulnarability	Total Risk	Control Contents	References	Threat	Vulnarability	Total Risk
50										
51										
52	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
53	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
54	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
55	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
56	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
57	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
58	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
59	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
60	2: Middle	Circuit breaker down	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
61	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
62										
63	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
64										
65	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
66	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
67										
68	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
69										
70	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
71	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
72	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
73	2: Middle	Unauthorized access, falsification	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
74	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
75	2: Middle	falsification	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
76	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)

	Risk Evaluation					Control		Risk Evaluation after Control		
#	Threat	Comments on Threat	Vulnarability	Comments on Vulnarability	Total Risk	Control Contents	References	Threat	Vulnarability	Total Risk
77										
78										
79										
80	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
81	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
82	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
83	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
84	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
85	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
86										
87	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
88										
89	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
90	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
91										
92	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
93	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
94										
95										
96	2: Middle	Staff errors to treat confidential information	3: Middle		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
97	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
98	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
99										
100	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
101	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
102	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
103										
104										
105	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
106	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
107	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
108	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
109	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
110	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
111	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
112	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
113	2: Middle	Circuit breaker down	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
114	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
115										
116	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
117										
118	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
119	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
120										
121	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
122										
123	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
124	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
125	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
126	2: Middle	Unauthorized access, falsification	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
127	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
128	2: Middle	falsification	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
129	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)

	Risk Evaluation					Control		Risk Evaluation after Control		
#	Threat	Comments on Threat	Vulnarability	Comments on Vulnarability	Total Risk	Control Contents	References	Threat	Vulnarability	Total Risk
130										
131										
132	2: Middle	Entry for external hackers	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
133	2: Middle	Continuous unauthorized access	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
134	2: Middle	Continuous unauthorized access	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
135	2: Middle	Circuit breaker down	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
136										
137	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
138	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
139	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
140	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
141	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
142	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
143	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
144	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
145	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
146	2: Middle	Data damage by software flaw and malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
147	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
148	2: Middle	Service unavailable for a long time	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
149	2: Middle	Continuous unauthorized access	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
150	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
151	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
152	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
153	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
154	2: Middle	Continuous unauthorized access	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
155	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
156	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
157	2: Middle	Circuit breaker down	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)

	Risk Evaluation					Control		Risk Evaluation after Control		
#	Threat	Comments on Threat	Vulnarability	Comments on Vulnarability	Total Risk	Control Contents	References	Threat	Vulnarability	Total Risk
158										
159										
160	2: Middle	Entry for external hackers	3: Middle		2: High (12pt)	Suspended until PAIS integrating GAIS		2: Middle	3: Middle	2: High (12pt)
161	2: Middle	Continuous unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
162	2: Middle	Continuous unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
163	2: Middle	Circuit breaker down	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
164										
165	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
166	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
167	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
168	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
169	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
170	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
171	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
172	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
173	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
174	2: Middle	Data damage by software flaw and malfunction	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
175	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
176	2: Middle	Service unavailable for a long time	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
177	2: Middle	Continuous unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
178	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
179	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
180	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
181	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
182	2: Middle	Continuous unauthorized access	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
183	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
184	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)
185	2: Middle	Circuit breaker down	3: Middle		2: High (12pt)			2: Middle	3: Middle	2: High (12pt)

	Risk Evaluation					Control		Risk Evaluation after Control		
#	Threat	Comments on Threat	Vulnarability	Comments on Vulnarability	Total Risk	Control Contents	References	Threat	Vulnarability	Total Risk
186										
187										
188										
189	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
190	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
191	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
192	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
193	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
194	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
195										
196	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
197										
198	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
199	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
200										
201	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
202	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
203										
204										
205	2: Middle	Staff errors to treat confidential information	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
206	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
207	2: Middle	Information leak	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
208										
209	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
210	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
211	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
212										
213										
214	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
215	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
216	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
217	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
218	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
219	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
220	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
221	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
222	2: Middle	Circuit breaker down	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
223	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
224										
225	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
226										
227	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
228	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
229										
230	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
231										
232	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
233	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
234	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
235	2: Middle	Unauthorized access, falsification	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
236	2: Middle	Information leak	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
237	2: Middle	falsification	3: Middle		2: High (9pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
238	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (9pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
239										
240										

	Risk Evaluation					Control		Risk Evaluation after Control		
#	Threat	Comments on Threat	Vulnarability	Comments on Vulnarability	Total Risk	Control Contents	References	Threat	Vulnarability	Total Risk
241							Rule book or Risk assessment plan			
242										
243										
244										
245										
246										
247										
248										
249										
250										
251										
252										
253										
254										
255										
256										
257										
258										
259										
260										
261										

	Risk Evaluation					Control		Risk Evaluation after Control		
#	Threat	Comments on Threat	Vulnarability	Comments on Vulnarability	Total Risk	Control Contents	References	Threat	Vulnarability	Total Risk
262										
263										
264										
265	1: Low	Forced entry, unauthorized access	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
266	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
267	2: Middle	Forced entry, unauthorized access	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
268	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
269	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
270	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
271										
272	3: High	Forced entry, unauthorized access	4: High		2: High (20pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
273										
274	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
275	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
276										
277	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
278	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
279										
280										
281	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
282	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
283	2: Middle	Information leak	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
284										
285	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
286	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
287	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
288										
289										
290	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
291	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
292	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
293	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
294	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
295	1: Low	Unauthorized access, falsification, malfunction	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
296	1: Low	Unauthorized access, falsification, malfunction	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
297	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
298	2: Middle	Circuit breaker down	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
299	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
300										
301	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
302										
303	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
304	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
305										
306	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
307										
308	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
309	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
310	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
311	3: High	Unauthorized access, falsification	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
312	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
313	2: Middle	falsification	4: High		2: High (16pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
314	3: High	Software flaw, malfunction, malware	4: High		2: High (20pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)

	Risk Evaluation					Control		Risk Evaluation after Control		
#	Threat	Comments on Threat	Vulnarability	Comments on Vulnarability	Total Risk	Control Contents	References	Threat	Vulnarability	Total Risk
315										
316										
317										
318	2: Middle	Forced entry, unauthorized access	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
319	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
320	2: Middle	Forced entry, unauthorized access	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
321	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
322	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
323	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
324										
325	3: High	Forced entry, unauthorized access	4: High		2: High (20pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
326										
327	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
328	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
329										
330	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
331	2: Middle	Forced entry, unauthorized access	2: Fair		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
332										
333										
334	3: High	Staff errors to treat confidential information	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
335	3: High	Forced entry, unauthorized access	4: High		2: High (20pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
336	3: High	Information leak	4: High		2: High (20pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
337										
338	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
339	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
340	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
341										
342										
343	2: Middle	Unauthorized access, falsification, malfunction	2: Fair		2: High (8pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
344	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
345	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
346	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
347	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
348	1: Low	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
349	1: Low	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
350	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
351	2: Middle	Circuit breaker down	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
352	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
353										
354	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
355										
356	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
357	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
358										
359	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
360										
361	1: Low	Software flaw, malfunction, malware	2: Fair		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
362	1: Low	Software flaw, malfunction, malware	2: Fair		1: Low (0pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
363	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
364	3: High	Unauthorized access, falsification	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
365	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
366	2: Middle	falsification	4: High		2: High (16pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
367	3: High	Software flaw, malfunction, malware	4: High		2: High (20pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)

	Risk Evaluation					Control		Risk Evaluation after Control		
#	Threat	Comments on Threat	Vulnarability	Comments on Vulnarability	Total Risk	Control Contents	References	Threat	Vulnarability	Total Risk
368										
369										
370										
371	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
372	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
373	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
374	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
375	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
376	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
377										
378	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
379										
380	3: High	Forced entry, unauthorized access	3: Middle		2: High (15pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
381	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
382										
383	1: Low	Forced entry, unauthorized access	2: Fair		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
384	1: Low	Forced entry, unauthorized access	2: Fair		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
385										
386										
387	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
388	1: Low	Forced entry, unauthorized access	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
389	2: Middle	Information leak	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
390										
391	1: Low	Staff errors to treat confidential information	2: Fair		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
392	1: Low	Forced entry, unauthorized access	1: Low		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
393	2: Middle	Information leak	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
394										
395										
396	1: Low	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
397	1: Low	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
398	1: Low	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
399	1: Low	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
400	1: Low	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
401	1: Low	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
402	1: Low	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
403	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (15pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
404	2: Middle	Circuit breaker down	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
405	2: Middle	Information leak	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (5pt)
406										
407	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
408										
409	2: Middle	Unauthorized access, falsification, malfunction	2: Fair		1: Low (0pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
410	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
411										
412	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
413										
414	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
415	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
416	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
417	3: High	Unauthorized access, falsification	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
418	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
419	1: Low	falsification	1: Low		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
420	2: Middle	Software flaw, malfunction, malware	4: High		2: High (16pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)

	Risk Evaluation					Control		Risk Evaluation after Control		
#	Threat	Comments on Threat	Vulnarability	Comments on Vulnarability	Total Risk	Control Contents	References	Threat	Vulnarability	Total Risk
512										
513										
514										
515	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
516	3: High	Forced entry, unauthorized access	3: Middle		2: High (15pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
517	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
518	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
519	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
520	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
521										
522	3: High	Forced entry, unauthorized access	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
523										
524	3: High	Forced entry, unauthorized access	3: Middle		2: High (15pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
525	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
526										
527	2: Middle	Forced entry, unauthorized access	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
528	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
529										
530										
531	3: High	Staff errors to treat confidential information	3: Middle		2: High (15pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
532	3: High	Forced entry, unauthorized access	3: Middle		2: High (15pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
533	3: High	Information leak	3: Middle		2: High (15pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
534										
535	2: Middle	Staff errors to treat confidential information	3: Middle		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
536	2: Middle	Forced entry, unauthorized access	3: Middle		1: Low (0pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
537	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
538										
539										
540	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
541	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
542	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
543	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
544	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
545	1: Low	Unauthorized access, falsification, malfunction	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
546	1: Low	Unauthorized access, falsification, malfunction	3: Middle		1: Low (0pt)	Define Rules as Implemented.	GIS Rule Book	2: Middle	1: Low	1: Low (0pt)
547	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
548	2: Middle	Circuit breaker down	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
549	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
550										
551	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
552										
553	2: Middle	Unauthorized access, falsification, malfunction	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
554	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
555										
556	2: Middle	Staff errors to treat confidential information	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
557										
558	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
559	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
560	2: Middle	Software flaw, malfunction, malware	3: Middle		2: High (12pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
561	3: High	Unauthorized access, falsification	3: Middle		2: High (15pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
562	2: Middle	Information leak	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
563	2: Middle	falsification	3: Middle		2: High (12pt)	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)
564	2: Middle	Software flaw, malfunction, malware	4: High		2: High (16pt)	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (4pt)