ISMS Information A

Contributed to the IS
secur

UPDATE

Contents

Business Name(s):	
BISO:	
Date Completed:	

Issue	Date	Purpose	Author(s)
1.0	7/25/2008	Final	Stephen McColl
1.1	11/25/2009	Updated Classification Types	Stephen McColl
1.2	1/12/2010	Updated classification types, added integrity and availability types, included managemement summary section.	Stephen McColl
1.3	5/31/2012	Modified in preparation for 2012 updates.	Stephen McColl

Copyright

Asset Inventory Template

O27k Toolkit by Steve McColl
e-working.com

Dept. Name(s):	
BISO:	
Date Completed:	

Signed off by BISO and Business:	
Date Signed Off:	

The above sign off indicates that the BISO has authorized the contents of this document once complete together with the business entity (e.g. with the M.D. or head of department).

A record of this sign off will be available for auditing purposes.

Information Asset Inventory

	Organisation & relevant process			Information Asset Details												Current Level of Protection	
Nr	**Operating Unit / Function**	**Process name**	**Process owner**	**Name of Asset**	**Description of Asset**	**Type of Information Asset** [Hard copy, Electronic File (specify type), removable media/device (specify type)]	**Personal Data** (Y/N)	**Personal Sensitive Data** (Y/N)	**Sensitive Customer Data** (Y/N)	**Classification**	**Integrity**	**Availability**	**Asset Custodian** (if NOT Functional Owner)	**Data Retention Period**	**At Origin** (description)	**If Information is Moved** (description)
Example	UNIT A	New starter process	Some One	New starter form	Form used to initiate the new starter process and sent to UNIT B via email.	Electronic .xls template file	Y	Y	N	Confidential	Medium	Low	UNIT B	0.5 Years	On PC of line manager, stored on network. For some line managers, they store these files on their laptop. Unlikely to be password protected.	Form is emailed to UNIT B using internal email system. It is then held on System A and System B by UNIT B.
1																
2																
3																
4																
5																
6																
7																
8																
9																
10																
11																
12																
13																
14																
15																
16																
17																
18																
19																
20																
26																
28																
29																
30																
31																
32																
33																
34																
35																
36																
37																
38																
39																
40																
41																
42																
43																
44																
45																
46																
47																
48																
49																
50																
51																
52																
53																
54																
55																
56																
57																
58																
59																
60																
61																
62																
63																
64																
65																
66																
67																
68																
69																
70																
71																
72																
73																
74																
75																
76																
77																
78																
79																
80																
81																
82																
83																
84																
85																
86																
87																
88																
89																
90																
91																
92																
93																
94																
95																
96																
97																

98																
99																
100																
101																
102																
103																
104																
105																
106																
107																
108																
109																
110																
111																
112																
113																
114																
115																
116																
117																
118																
119																
120																
121																
122																
123																
124																
125																
126																
127																
128																
129																
130																
131																
132																
133																
134																
135																
136																
137																
138																
139																
140																
141																
142																
143																
144																
145																
146																
147																
148																
149																
150																
151																
152																
153																
154																
155																
156																
157																
158																
159																
160																
161																
162																
163																
164																
165																
166																
167																
168																
169																
170																
171																
172																
173																
174																
175																
176																
177																
178																
179																
180																
181																
182																
183																
184																
185																
186																
187																
188																
189																
190																
191																
192																
193																
194																
195																
196																
197																
198																
199																
200																
201																
202																
203																
204																
205																

206																
207																
208																
209																
210																
211																
212																
213																
214																
215																
216																
217																
218																
219																
220																
221																
222																
223																
224																
225																
226																
227																
228																
229																
230																
231																
232																
233																
234																
235																
236																
237																
238																
239																
240																
241																
242																
243																
244																

Once the Inventory is complete click the [Generate Gap Analysis] button below to highlight those information assets which require a risk assessment.
Your risk assessment needs to verify that the protection controls in place for the assets listed are adequate to the sensitivity of the data as guided by the *Information Handling Policy*.
Use <Columns S and T> to record necessary actions required of the process owner until complete.
[*DO NOT click GENERATE GAP ANALYSIS again unless you have created a copy of this document beforehand*]

	Organisation & relevant process			Information Asset Details										Current Level of Protection		BISO / TISO Assessment	BISO/Process Owner Action
No	**1. Operating Unit / Function**	**2. Process name**	**3. Process owner**	**4. Name of Asset**	**5. Description of Asset**	**7. Type of Information Asset** (Hard copy, Electronic File (specify type), removable media/device (specify type)]	**8. Personal Data** (Y/N)	**8.a Personal Sensitive Data** (Y/N)	**8. b Sensitive Customer Data** (Y/N)	**8. Classification**	**8.a Integrity**	**8.b Availability**	**9. Asset Custodian** (if NOT Functional Owner)	**10. Data Retention Period**	**10. At Origin** (description)	**11. If Information is Moved** (description)	**Security Conclusion**	**Process Owner Response and Date for Implementation** (Evidence is required ie. screenshots or similar where applicable to prove these controls are enforced)

Gap

Table 1- Process examples

Examples of processes and information assets	
Generic Processes	**Information Asset**
Core Business Processes	Production data
Budget Process	Budget Document, Invoices.
HR	CV, Salary letters, references, personal sensitive information, disciplinary information, pension information, starter mover joiner p
Resource Management	Skills matrix, appraisals, training details i.e. records.
Business Continuity	BCP & DR Plans, BIA.
Risk Management	Risk Registers, Risk & Issues Logs.
Audit	SAS70 reports, any internal or external audit reports.
Compliance	Incident reports, money laundering reports, data protection information, all policies.
Contracts	Service agreements, Service definitions, contracts, SCRs, NDAs.
Sales Collateral	Pricing information, RFIs, RFPs, presales leads (pipeline).
Reporting/Management Information/MIS	Quality, Production, Sales definitions.
Change management	All project or related documentation.
Project Management	Project status reporting, customer reporting, internal project documents/specs.

Table 2- Classification Types

Classification	**Protection requirements for information in printed format.**			
Usage	**Strictly Confidential**	**Confidential**	**Business use only**	**Public**
Labelling	Each page to be marked **STRICTLY CONFIDENTIAL**.	Each page to be marked **CONFIDENTIAL**.	Each page to be marked **Business use only**.	No security requirements.
Addressing	The storage medium must have two envelopes/layers of packaging. The outer envelope/layer must: -Show the recipients name and address. -Be marked **TO BE OPENED BY ADDRESSEE ONLY** -Show the name and phone number of the sender of the information. The inner envelope must be labelled **STRICTLY CONFIDENTIAL**.	The storage medium must have two envelopes/layers of packaging. The outer envelope/layer must: -Show the recipients name and address. -Be marked **TO BE OPENED BY ADDRESSEE ONLY** -Show the name and phone number of the sender of the information. The inner envelope must be labelled **CONFIDENTIAL**.	Show the recipients name and address on envelope.	Show the recipients name and address on envelope.
Mailing of Information	No classification marking on envelope; **STRICTLY CONFIDENTIAL** marking on cover sheet; confirmation of receipt at discretion of information owner.	No classification marking on envelope; **CONFIDENTIAL** marking on cover sheet; confirmation of receipt at discretion.	Mailing requirements determined by information owner.	No security requirements.
Storage	Must be stored within secure fire and water proof locked storage units within a locked office. This includes single instance documents where no electronic or paper copies exist.	Must be stored within locked storage units when not in the presence of the originator or recipient.	Secure office or other location. Room need not be locked if access to the building or floor is restricted to employees and authorised non-employees.	No security requirements.
Transportation	By hand or approved courier.	Registered mail.	Normal mail service.	Normal mail service.
Disposal	Information must be disposed of securely using cross-cut shredders or confidential waste bins which are certified for secure destruction. A record must be kept of how, when and by whom the information was destroyed (To provide an audit trail).	Information must be disposed of securely using strip-cut shredders or confidential waste bins which are certified for secure destruction.	Information must be disposed of securely using strip-cut shredders or confidential waste bins which are certified for secure destruction.	Information which is deemed appropriate for public disclosure can be disposed of using locally supplied waste paper facilities. If there is any doubt as to whether the information is commercially or personally sensitive, then use strip-cut shredders or confidential waste bins which are certified for secure destruction.
Classification	**Protection requirements for information in electronic format (computer data)**			
Usage	**Strictly Confidential**	**Confidential**	**Business use only**	**Public**
Electronic Labelling	The information medium must be marked **STRICTLY CONFIDENTIAL** on subject-line or header/footer.	Where information medium is not permanently held in locked storage or a secure environment, it must be labeled **CONFIDENTIAL** on subject-line or header/footer.	Must be marked **Business use only** on subject-line or header/footer.	No security requirements.
Transmission	Information must be transmitted in encrypted form (using a business-approved method). Transmission should have controlled access e.g. password protected account login.	Information must be transmitted in encrypted form (using a business-approved method). Transmissions should have controlled access e.g. password protected account login.	Information should be transmitted to a verified account (eMail address or login ID).	No security requirements.
Storage (e.g. digital file, eMail or web page)	Stored in a directory or folder with controlled access, e.g., password protection. Information must be stored encrypted using approved methods.	Stored in a directory or folder with controlled access, e.g., password protection. Information must be stored encrypted.	Stored in a directory or folder with restricted access, e.g., password protection.	No security requirements.
Removable media (e.g. USB stick, CD, laptop, Blackberry)	All removable media must have applied encryption including mobile devices e.g. Laptops, PDA's, iPhones, Blackberries, USB Sticks. Laptop hard disks are to be encrypted and the laptop is to be secure to desks using e.g. Kensington locks.	All removable media must have applied encryption including mobile devices e.g. Laptops, PDA's, iPhones, Blackberries, USB Sticks. Laptop hard disks are to be encrypted and the laptop is to be secure to desks using e.g. Kensington locks.	Secure office or other location. Room need not be locked if access to the floor is restricted to employees and authorised non-employees.	No security requirements.
Disposal of electronic information (digital file).	In addition to removing the directory entry for the file, the space used by the file must be over-written using state of the art approved solutions for the permanent removal of data.	In addition to removing the directory entry for the file, the space used by the file must be over-written using state of the art approved solutions for the permanent removal of data.	Removal of Directory entry for file.	Removal of Directory entry for file.
Disposal of physical medium (e.g. hard disks/drives).	Information must be disposed of securely using state of the art approved solutions for the permanent removal of data. A record must be kept of how, when and by whom the information was destroyed (to provide an audit trail).	Media must be disposed of securely using state of the art approved solutions for the permanent removal of data (e.g. shredding or physical destruction).	Media must be disposed of securely using state of the art approved solutions for the permanent removal of data (e.g. shredding or physical destruction).	Media must be disposed of securely using state of the art approved solutions for the permanent removal of data (e.g. shredding or physical destruction).

Table 3- Integrity Types

Integrity level	Definition	Examples/impact of unauthorised modification
High	100% error free.	Same as Confidentiality classification for Strictly Confidential information.
Medium	96-99% error free.	Same as Confidentiality classification for Confidential information.
Low	90-95% error free.	Same as Confidentiality classification for Business use only information.

Table 4- Availability Types

Availability level	Definition	Impact of unavailability
High	No interruption beyond 0.5 days.	Severe adverse impact.
Medium	No interruption of access beyond 1 day.	Significant adverse impact.
Low	No interruption of access beyond 7 days.	Limited adverse impact.

Table 5- Sensitive data examples

Personal, Sensitive Personal, and Sensitive Customer Data	
Information Asset Details	**Description**

Personal Data	An individual must be capable of being identified from that data or a number or sources of data - An example is a simple email address such as john.smith@company.com. We know that there is a company and that there is an individual called john smith who works for them so he can be identified from the email address, therefore the email address is enough to constitute personal information.
Sensitive Personal Data	Any data held either electronically or manually, which relates directly to a living individual and which covers specifically (including): racial or ethnic origin; political opinions; religious or other beliefs; Trade Union membership; health; sex life; criminal allegations, proceedings or convictions.
Sensitive Customer Data	Data which contains information specific to a customer including but not limited to bank account details, userids and passwords, list of employees.

Status Report

Classification Type Summary

Classification Type	Total
Strictly Confidential	#NAME?
Confidential	#NAME?
Business Use Only	#NAME?
Public	#NAME?

Management Summary

[Complete after review and distribute]