IT Security analysis on unit [redacted] [redacted]

Preparation

1 Review

Make the review using the questionnaire to identify threats.
Discuss impact and probability; fill in the chart below and the diagram under headline Risk evaluation.

No	Identified threat	Chapter	Impact	Proba-bility
1	Are you familiar with the Information Security policy?	[redacted]	[redacted]	[redacted]
2	Has the Information Security Policy been communicated to all co-workers			
3	Are you familiar with the six IT Security principles	[redacted]	[redacted]	[redacted]
4	Are you familiar with the four Basic rules			
5	Do the managers of the unit follow up the compliance of the Information Security policy, principles and rules			
6	Is an IT Security review carried out yearly	[redacted]	[redacted]	[redacted]
7	Is a definition of the IT Security responsibility included in the job description			
8	Do co-workers sign a secrecy agreement in connection with hiring	[redacted]	[redacted]	[redacted]
9	do the terms and conditions of employment specify the responsibility for IT Security	[redacted]	[redacted]	[redacted]
10	Rule 010101 – Information Security policy Rule 010102 – IT Security principles Rule 040206 – User training Rule 040311 – IT Security incident procedures	[redacted]	[redacted]	[redacted]
11	Are there documented instructions for the users of the respective systems?	[redacted]	[redacted]	[redacted]
12	Are all users aware that they are personally responsible for IT Security related to the information they receive or create?	[redacted]	[redacted]	[redacted]
13	Do co-workers know what consequences carelessness or offence against the IT Security regulations will have?	[redacted]	[redacted]	[redacted]
14	Are you familiar with the incident handling procedure?	[redacted]	[redacted]	[redacted]
15	Are there any routines for how to act if a co-worker violates the IT Security regulations?			
16	Are there any routines for how to act when a co-worker has been given notice?	[redacted]	[redacted]	[redacted]
17	Have actions been taken to reduce dependence on key persons?	[redacted]	[redacted]	[redacted]
18	Are all laptops equipped with encryption protection?			
19	Is information classified as confidential encrypted before e-mailed outside [redacted] network?			
20	If yes – Are there any routines for this?	[redacted]	[redacted]	[redacted]
21	Is there a clear desk recommendation?			
22	Do co-workers log off their computers when leaving their desk?			
23	Is there an alarm system?			
24	Is there a guard on duty 24 hours daily?			
25	Is there sufficient protection surrounding the server room e.g. TV surveillance?			

26	Does the server room have a computer floor with sufficient height? (45cm)	[redacted]	[redacted]	[redacted]
27	Is there a spare air conditioning system?	[redacted]	[redacted]	[redacted]
28	Is there a written document with instructions for how to act in the event of breakdown in the air conditioning system?	[redacted]	[redacted]	[redacted]
29	Is there a spare generator (diesel oil)?	[redacted]	[redacted]	[redacted]
30	Is there functioning emergency lighting in the room?	[redacted]	[redacted]	[redacted]
31	Does the equipment have permanent electrical connections?	[redacted]	[redacted]	[redacted]
32	If computer floor – Are all electrical and signal cables between the sub-floor and upper floor mounted on special spacer-plates?	[redacted]	[redacted]	[redacted]
33	Are there maintenance agreements?	[redacted]	[redacted]	[redacted]
34	Are the response times for service adequate according to the maintenance agreement?	[redacted]	[redacted]	[redacted]
35	Does the service agreement cover all critical components?	[redacted]	[redacted]	[redacted]
36	If yes – Do these routines ensure that confidential information is deleted from data media which are sent to external service provider?	[redacted]	[redacted]	[redacted]
37	Is flooding of the areas in the server room where computer equipment is placed, prevented?	[redacted]	[redacted]	[redacted]
38	Is the server room placed above ground level?	[redacted]	[redacted]	[redacted]
39	Are there moisture indicators in the server room that are connected to an alarm centre?	[redacted]	[redacted]	[redacted]
40	If computer floor – Are there moisture indicators under the computer floor?	[redacted]	[redacted]	[redacted]
41	Are there moisture indicators in the nearby area?	[redacted]	[redacted]	[redacted]
42	Are the cables/pipe ducts/lines that pass through firewalls sealed?	[redacted]	[redacted]	[redacted]
43	Is the fire door marked?	[redacted]	[redacted]	[redacted]
44	If computer floor – Is lifting equipment for computer floor easily accessible?	[redacted]	[redacted]	[redacted]
45	Do all emergency exits open outwards in the direction of evacuation?	[redacted]	[redacted]	[redacted]
46	Is the server room clear of papers?	[redacted]	[redacted]	[redacted]
47	Is there an emergency button for fire alarm in the server room that is connected to an alarm centre and/or fire department?	[redacted]	[redacted]	[redacted]
48	Is there a fire extinguishing system that is appropriately designed for the computer facility?	[redacted]	[redacted]	[redacted]
49	Is it possible to specify the duration of a user's access authorisation? Starting on – until.	[redacted]	[redacted]	[redacted]
50	Is a user ID automatically locked when a user's access authorisation is no longer valid?	[redacted]	[redacted]	[redacted]
51	Is there a routine for following up inactive user IDs?	[redacted]	[redacted]	[redacted]
52	Is there an action plan for measures to be taken in the event of a disruption?	[redacted]	[redacted]	[redacted]
53	Is the password changed every 90 days?	[redacted]	[redacted]	[redacted]
54	Is there equipment for recording incidents such as telephone threats?	[redacted]	[redacted]	[redacted]
55	Are the backups regularly checked to ensure that they can be used?	[redacted]	[redacted]	[redacted]
56	Is restart from backups tested regularly?	[redacted]	[redacted]	[redacted]
57	Are the backups stored in an approved safe for data media and in accordance with national and international standards?	[redacted]	[redacted]	[redacted]
58	Is the full backup stored in a separate building away from the area of operation?	[redacted]	[redacted]	[redacted]
59	If more than one generation of backup exist, is the latest generation stored in a building separate from the operation area?	[redacted]	[redacted]	[redacted]
60	Is the handling of removable data media, such as tapes, disks, cassettes and printed reports controlled?	[redacted]	[redacted]	[redacted]

61	Do the operational personnel take inventories of movable data media on a regular basis?	[redacted]	[redacted]	[redacted]
62	Are data media that are no longer required disposed of securely?	[redacted]	[redacted]	[redacted]
63	Are data media containing confidential information handled in accordance with the classification rule?	[redacted]	[redacted]	[redacted]
64	Are data media containing confidential information clearly marked with unique and irremovable numbers?	[redacted]	[redacted]	[redacted]
65	Is a yearly inventory made of data media that contain or have contained confidential information?	[redacted]	[redacted]	[redacted]
66	Are there documented instructions for how to destroy confidential data media?	[redacted]	[redacted]	[redacted]
67	Are there documented instructions for how to record the destruction of confidential data media?	[redacted]	[redacted]	[redacted]
68	Does the password require at least six characters and consist of not only letters?	[redacted]	[redacted]	[redacted]
69	Have you been educated in the system?	[redacted]	[redacted]	[redacted]
70	Do co-workers receive introductory training in the systems they will use?	[redacted]	[redacted]	[redacted]
71	Are new co-workers educated in the system?	[redacted]	[redacted]	[redacted]
72	Do all co-workers receive training in IT Security?	[redacted]	[redacted]	[redacted]
73	Are all users aware that they are personally responsible for IT Security related to the information they receive or create?	[redacted]	[redacted]	[redacted]
74	Are there documented instructions of the working method?	[redacted]	[redacted]	[redacted]
75	Do all users know what to do if an IT Security incident occurs?	[redacted]	[redacted]	[redacted]
76	Is there a routine for how to report IT Security incidents?	[redacted]	[redacted]	[redacted]
77	Are there controls in the access control system that prevent simple passwords?	[redacted]	[redacted]	[redacted]
78	Does the password in the access control system require at least six characters and consist of not only letters?	[redacted]	[redacted]	[redacted]
79	Business continuity plan	[redacted]	[redacted]	[redacted]
80	Testing business continuity plan	[redacted]	[redacted]	[redacted]
81	Updating business continuity plan	[redacted]	[redacted]	[redacted]
82	System and business continuity plan	[redacted]	[redacted]	[redacted]
83	If yes – Is there an appointed register administrator in accordance with the Data Protection Act?	[redacted]	[redacted]	[redacted]
84	Is there a routine for the administration of matters related to the Data Protection Act?	[redacted]	[redacted]	[redacted]

Chapter = Chapter in the questionnaire.

Impact If the event will occur.

1. Low Handled within the unit’s limit of the budget/resources.
2. Medium Creates difficulties, implies saving on other costs. It can affect the business but is manageable.
3. High Creates serious obstacle, can not be handled within the unit’s limit of the budget/resources.

Probability That the event will occur.

1. Low When co-workers assess that an undesired event can happen.
2. Medium When there is a clear tendency that an undesired event can happen.
3. High When an event actually has happened or when the probability for an event to happen is high.

1.1 Goodwill loss

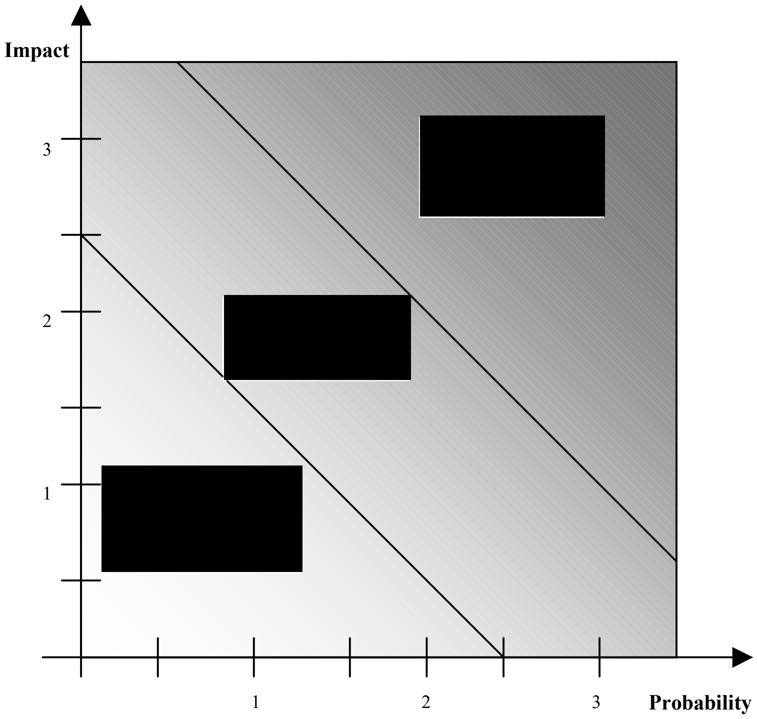
This is a description of threats and other considerable aspects that can create goodwill loss.

No	Goodwill loss	Impact	Proba-bility
G1	4.2.1.4 Are all users aware that they are personally responsible for IT Security related to the information they receive or create?	[redacted]	[redacted]
G2	10.1 Compliance with legal requirement	[redacted]	[redacted]

2 Risk evaluation

2.1 Mapping identified threats and goodwill loss

The diagram below shows how the identified threats are mapped depending on probability and impact.



The risks are classified in the following levels where risks are connected with to recommendations or demands:

Low risk	No action is necessary.	Recommendation
Medium risk	The risk has to be reduced.	Demand or recommendation
High risk	The risk has to be moved from this area.	Demand

2.2 Cost calculation

Collect information regarding costs per hour if the system is not working.
Costs could for example be when co-workers can not work.
Already filled in information shall not be changed.

A = Cost per hour
Fill in the cost from Background information, divided by working hours (8 hours/day), calculated in Euro. **Currency:**

B = Customer impact in %
Fill in the customer impact in % from Background information.

C = Gross margin profit loss per hour
Fill in the gross margin profit loss per hour. Check with your controller or economic department to get the correct percentage.

GPS/TOS

Time limits	A	B	C
1 day	[redacted]	0%	0
3 days	[redacted]	0%	0

ECIS

Time limits	A	B	C
1 day	[redacted]	0%	0
3 days	[redacted]	0%	0

Local system 1

Time limits	A	B	C
1 day	-	-	-
3 days	-	-	-

Local system 2

Time limits	A	B	C
1 day	-	-	-
3 days	-	-	-

2.3 Risk calculation

The consequence that is calculated refers to a total standstill of the system, and what this standstill costs. Use the information from prevous side (2.2 cost calculation).

A = Cost per hour

B = Customer impact in %

C = Gross margin profil loss per hour

GPS/TOS

Time limits	C*B+A =X, X = Total cost in Euro/hour
1 day	[redacted]
3 days	[redacted]

ECIS

Time limits	C*B+A =X, X = Total cost in Euro/hour
1 day	[redacted]
3 days	[redacted]

Local system 1

Time limits	C*B+A =X, X = Total cost in Euro/hour
1 day	-
3 days	-

Local system 2

Time limits	C*B+A =X, X = Total cost in Euro/hour
1 day	-
3 days	-

3 Business dependency evaluation

Discussions regarding the Background information documentation.
Fill in information for each system that are specified.

- Acceptable time of interruption, how long time an interruption can go on without impact on the business on the analysed unit?
- How long time after interruption the loss of information and system functionality will be critical on unit level.

	Acceptable interruption time	Critical interruption time
[redacted]	1 day	3 days
[redacted]	1 day	2 days
Local system 1	-	-
Local system 2	-	-
[redacted]	1 day	2 days [redacted]

4 Demand, recommendation

Fill in:

- Risks that are identified in chapter 2.1.
- Demands and/or recommendations, mark D for demand and R for recommendation.
- A risk factor, see below.
- Cost if the risk occur calculated in Euro. **Currency:**

No	Identified risk	Demand/recommendation	D/R	Risk factor	Cost
1	Are you familiar with the Information Security policy?	[redacted]	[redacted]	[redacted]	
2	Has the Information Security Policy been communicated to all co-workers	[redacted]	[redacted]	[redacted]	
3	Are you familiar with the six IT Security principles	[redacted]	[redacted]	[redacted]	
4	Are you familiar with the four Basic rules	[redacted]	[redacted]	[redacted]	
5	Do the managers of the unit follow up the compliance of the Information Security policy, principles and rules	[redacted]	[redacted]	[redacted]	
6	Is an IT Security review carried out yearly	[redacted]	[redacted]	[redacted]	
7	Is a definition of the IT Security responsibility included in the job description	[redacted]	[redacted]	[redacted]	
8	Do co-workers sign a secrecy agreement in connection with hiring	[redacted]	[redacted]	[redacted]	
9	Do the terms and conditions of employment specify the responsibility for IT Security	[redacted]	[redacted]	[redacted]	
10	Rule 010101 – Information Security policy Rule 010102 – IT Security principles Rule 040206 – User training Rule 040311 – IT Security incident procedures	[redacted]	[redacted]	[redacted]	
11	Are there documented instructions for the users of the respective systems?	[redacted]	[redacted]	[redacted]	
12	Are all users aware that they are personally responsible for IT Security related to the information they receive or create?	[redacted]	[redacted]	[redacted]	
13	Do co-workers know what consequences carelessness or offence against the IT Security regulations will have?	[redacted]	[redacted]	[redacted]	
14	Are you familiar with the incident handling procedure?	[redacted]	[redacted]	[redacted]	
15	Are there any routines for how to act if a co-worker violates the IT Security regulations?	[redacted]	[redacted]	[redacted]	

16	Are there any routines for how to act when a co-worker has been given notice?	[redacted]	[redacted]	[redacted]	
17	Have actions been taken to reduce dependence on key persons?	[redacted]	[redacted]	[redacted]	
18	Are all laptops equipped with encryption protection?	[redacted] .	[redacted]	[redacted]	
19	Is information classified as confidential encrypted before e-mailed outside [redacted] network?	[redacted]	[redacted]	[redacted]	
20	If yes – Are there any routines for this?	[redacted]	[redacted]	[redacted]	
21	Is there a clear desk recommendation?	[redacted]	[redacted]	[redacted]	
22	Do co-workers log off their computers when leaving their desk?	[redacted]	[redacted]	[redacted]	
23	Is there an alarm system?	[redacted]	[redacted]	[redacted]	
24	Is there a guard on duty 24 hours daily?	[redacted]	[redacted]	[redacted]	
25	Is there sufficient protection surrounding the server room e.g. TV surveillance?	[redacted]	[redacted]	[redacted]	
26	Does the server room have a computer floor with sufficient height? (45cm)	[redacted]	[redacted]	[redacted]	
27	Is there a spare air conditioning system?	[redacted]	[redacted]	[redacted]	
28	Is there a written document with instructions for how to act in the event of breakdown in the air conditioning system?	[redacted]	[redacted]	[redacted]	
29	Is there a spare generator (diesel oil)?	[redacted]	[redacted]	[redacted]	
30	Is there functioning emergency lighting in the room?	[redacted]	[redacted]	[redacted]	
31	Does the equipment have permanent electrical connections?	[redacted]	[redacted]	[redacted]	
32	If computer floor – Are all electrical and signal cables between the sub-floor and upper floor mounted on special spacer-plates?	[redacted]	[redacted]	[redacted]	
33	Are there maintenance agreements?	[redacted]	[redacted]	[redacted]	
34	Are the response times for service adequate according to the maintenance agreement?	[redacted]	[redacted]	[redacted]	
35	Does the service agreement cover all critical components?	[redacted]	[redacted]	[redacted]	
36	If yes – Do these routines ensure that confidential information is deleted from data media which are sent to external service provider?	[redacted]	[redacted]	[redacted]	
37	Is flooding of the areas in the server room where computer equipment is placed, prevented?	[redacted]	[redacted]	[redacted]	

38	Is the server room placed above ground level?	[redacted]	[redacted]	[redacted]	
39	Are there moisture indicators in the server room that are connected to an alarm centre?	[redacted]	[redacted]	[redacted]	
40	If computer floor – Are there moisture indicators under the computer floor?	[redacted]	[redacted]	[redacted]	
41	Are there moisture indicators in the nearby area?	[redacted]	[redacted]	[redacted]	
42	Are the cables/pipe ducts/lines that pass through firewalls sealed?	[redacted]	[redacted]	[redacted]	
43	Is the fire door marked?	[redacted]	[redacted]	[redacted]	
44	If computer floor – Is lifting equipment for computer floor easily accessible?	[redacted]	[redacted]	[redacted]	
45	Do all emergency exits open outwards in the direction of evacuation?	[redacted]	[redacted]	[redacted]	
46	Is the server room clear of papers?	[redacted]	[redacted]	[redacted]	
47	Is there an emergency button for fire alarm in the server room that is connected to an alarm centre and/or fire department?	[redacted]	[redacted]	[redacted]	
48	Is there a fire extinguishing system that is appropriately designed for the computer facility?	[redacted]	[redacted]	[redacted]	
49	Is it possible to specify the duration of a user’s access authorisation? Starting on – until.	[redacted]	[redacted]	[redacted]	
50	Is a user ID automatically locked when a user’s access authorisation is no longer valid?	[redacted]	[redacted]	[redacted]	
51	Is there a routine for following up inactive user IDs?	[redacted]	[redacted]	[redacted]	
52	Is there an action plan for measures to be taken in the event of a disruption?	[redacted]	[redacted]	[redacted]	
53	Is the password changed every 90 days?	[redacted]	[redacted]	[redacted]	
54	Is there equipment for recording incidents such as telephone threats?	[redacted]	[redacted]	[redacted]	
55	Are the backups regularly checked to ensure that they can be used?	[redacted]	[redacted]	[redacted]	
56	Is restart from backups tested regularly?	[redacted]	[redacted]	[redacted]	
57	Are the backups stored in an approved safe for data media and in accordance with national and international standards?	[redacted]	[redacted]	[redacted]	
58	Is the full backup stored in a separate building away from the area of operation?	[redacted]	[redacted]	[redacted]	
59	If more than one generation of backup exist, is the latest generation stored in a building separate from the operation area?	[redacted]	[redacted]	[redacted]	

60	Is the handling of removable data media, such as tapes, disks, cassettes and printed reports controlled?	[redacted]	[redacted]	[redacted]	
61	Do the operational personnel take inventories of movable data media on a regular basis?	[redacted]	[redacted]	[redacted]	
62	Are data media that are no longer required disposed of securely?	[redacted]	[redacted]	[redacted]	
63	Are data media containing confidential information handled in accordance with the classification rule?	[redacted]	[redacted]	[redacted]	
64	Are data media containing confidential information clearly marked with unique and irremovable numbers?	[redacted]	[redacted]	[redacted]	
65	Is a yearly inventory made of data media that contain or have contained confidential information?	[redacted]	[redacted]	[redacted]	
66	Are there documented instructions for how to destroy confidential data media?	[redacted]	[redacted]	[redacted]	
67	Are there documented instructions for how to record the destruction of confidential data media?	[redacted]	[redacted]	[redacted]	
68	Does the password require at least six characters and consist of not only letters?	[redacted].	[redacted]	[redacted]	
69	Have you been educated in the system?	[redacted]	[redacted]	[redacted]	
70	Do co-workers receive introductory training in the systems they will use?	[redacted]	[redacted]	[redacted]	
71	Are new co-workers educated in the system?	[redacted]	[redacted]	[redacted]	
72	Do all co-workers receive training in IT Security?	[redacted]	[redacted]	[redacted]	
73	Are all users aware that they are personally responsible for IT Security related to the information they receive or create?	[redacted]	[redacted]	[redacted]	
74	Are there documented instructions of the working method?	[redacted]	[redacted]	[redacted]	
75	Do all users know what to do if an IT Security incident occurs?	[redacted]	[redacted]	[redacted]	
76	Is there a routine for how to report IT Security incidents?	[redacted]	[redacted]	[redacted]	
77	Are there controls in the access control system that prevent simple passwords?	[redacted]	[redacted]	[redacted]	
78	Does the password in the access control system require at least six characters and consist of not only letters?	[redacted]	[redacted]	[redacted]	
79	Business continuity plan	[redacted]	[redacted]	[redacted]	

80	Testing business continuity plan	[redacted]	[redacted]	[redacted]	
81	Updating business continuity plan	[redacted]	[redacted]	[redacted]	
82	System and business continuity plan	[redacted]	[redacted]	[redacted]	
83	If yes – Is there an appointed register administrator in accordance with the Data Protection Act?	[redacted]	[redacted]	[redacted]	
84	Is there a routine for the administration of matters related to the Data Protection Act?	[redacted]	[redacted]	[redacted]	

Risk factors:

L	=	Low risk	Recommendation
M	=	Medium risk	Demand or recommendation
H	=	High risk	Demand

COST: it is impossible to estimate cost for all the risks as it is unclear which cost source we should take.