IT Security analysis report

[redacted]

[redacted]

[redacted]
Choroba Uschi, [redacted]

Distribution list:
[redacted]

1 SUMMARY 3

1.1 INVESTIGATED UNIT AND COUNTRY 3
1.2 GOODWILL LOSS 3
1.3 RISK CALCULATION 3
1.4 BUSINESS DEPENDENCY EVALUATION 3
1.5 IDENTIFIED HIGH RISKS 3

2 BACKGROUND 4

2.1 IT SECURITY GOAL 4
2.2 SHORT DESCRIPTION OF THE UNIT 4
2.3 METHOD 4

3 IT SECURITY REVIEW 5

3.1 IDENTIFIED THREATS 5
3.2 GOODWILL LOSS 7

4 RISK EVALUATION 8

4.1 MAPPING IDENTIFIED THREATS AND GOODWILL LOSS 8
4.2 RISK CALCULATION 8

5 BUSINESS DEPENDENCY EVALUATION 9

6 DEMAND, RECOMMENDATION 10

6.1 IDENTIFIED MEDIUM AND HIGH RISKS 10
6.2 OBSERVATION OF RISKS 13
6.3 OBSERVATION OF GOODWILL LOSS 19

1 Summary

1.1 Investigated unit and country

Interviewed persons:

[redacted]

1.2 Goodwill loss

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

1.3 Risk calculation

The table contains costs at a total standstill of specified systems.

Time limits	[redacted]	[redacted]	Local system 1	Local system 2
1 day	[redacted]	[redacted]	-	-
3 days	[redacted]	[redacted]	-	-

The impact is calculated with the formula **C*B+A=X**.

X = Impact in Euro/hour
A = Cost
B = Customer impact
C = Gross margin profit loss

1.4 Business dependency evaluation

The table contains critical systems, acceptable interruption time and critical interruption time.

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

1.5 Identified high risk

The table contains identified and evaluated high risks from chapter 3.1 and 3.2. Demands are presented. Further down in the report the findings are presented in more detail under each chapter within the IKEA questionnaire.

No	Identified high risk	Demand
1	[redacted]	[redacted]
2	[redacted]	[redacted]
3	[redacted]	[redacted]