ISO27001 Management Review

<Company> - <Date Completed>

Contents

[2 Usage guide – Manual 3](#_Toc167462132)

[2.1 Point of attention/Topic 3](#_Toc167462133)

[2.2 Document parameters 3](#_Toc167462134)

[3 Agenda 4](#_Toc167462135)

[4 (Optional) overview agenda - Important events 4](#_Toc167462136)

[5 Status of actions from previous reviews 5](#_Toc167462137)

[6 Changes in external and internal issues (relevant to ISMS 5](#_Toc167462138)

[6.1 External (Part 1/2) 5](#_Toc167462139)

[6.2 Internal (Part 2/2) 5](#_Toc167462140)

[7 Changes in needs from interested parties 5](#_Toc167462141)

[8 Feedback on security performance 6](#_Toc167462142)

[8.1 NCs and corrective actions 6](#_Toc167462143)

[8.1.1 List NCs 6](#_Toc167462144)

[8.1.2 Corrective actions 6](#_Toc167462145)

[8.2 Monitoring/Measurement results 6](#_Toc167462146)

[8.3 External/Internal Audit Results 6](#_Toc167462147)

[8.3.1 Legend 6](#_Toc167462148)

[8.3.2 External Audit 6](#_Toc167462149)

[8.3.3 Internal Audit 7](#_Toc167462150)

[8.4 Fullfilment of ISMS objectives 8](#_Toc167462151)

[9 Feedback from interested parties 8](#_Toc167462152)

[9.1 Management 9](#_Toc167462153)

[9.2 Employees 9](#_Toc167462154)

[9.3 Customers 9](#_Toc167462155)

[9.4 Suppliers 9](#_Toc167462156)

[9.5 <other> 9](#_Toc167462157)

[10 Results of risk management and status of treatment plan 9](#_Toc167462158)

[11 Business - Opportunities for improvement (management) 9](#_Toc167462159)

[11.1 Improvement opportunities for company (mgmt level) 9](#_Toc167462160)

[12 Management decisions 9](#_Toc167462161)

[13 Planning next management review ISO27001 9](#_Toc167462162)

[14 Annexes 10](#_Toc167462163)

[14.1 (ISMS) Reference documentation 10](#_Toc167462164)

[14.2 (Link to) External Audit reports ISO27001 10](#_Toc167462165)

[14.3 (Link to) Internal audit report ISO27001 10](#_Toc167462166)

[14.4 (Link to) Other audit reports (pentest, SOC, ...) 10](#_Toc167462167)

[14.5 Customer Surveys 10](#_Toc167462168)

[14.6 Tickets 10](#_Toc167462169)

[14.7 Risk management plan 10](#_Toc167462170)

[14.8 … 10](#_Toc167462171)

# Usage guide – Manual

## Point of attention/Topic

* Fields marked in light blue should be filled with content
* Make sure to add ISMS document classification (footer of slide)
* Hide/remove first slide
* Reuse previous meeting presentation to build next meeting presentation

## Document parameters

You can easily change some basic document parameters like

* Company name
* Date completed
* Classification code (header left field)
* Classification explanation (header right field)

Via the document properties.

* Word > Menu File
* Menu Info > Properties (right hand side of screen)

Update the attributes as needed. (update the fields in Word with the F9 button)

A screenshot of a computer

Description automatically generated

# Agenda

* Status of actions from previous reviews
* Changes in external and internal issues (relevant to ISMS)
* Feedback on security performance including trends
  + NCs and corrective actions
  + Monitoring and measuring results
  + Audit results
  + Fullfilment of objectives
* Feedback from interested parties
* Results of risk management and status of risk treatment plant
* Opportunity for improvement
* Management decisions
* Neds for changes to the ISMS
* Documentation as evidence of results of ISMS

# (Optional) overview agenda - Important events

* Previous Management Review = <add date>
* Previous external audit ISO27001 = <add date>
* Previous internal audit ISO27001 = <add date>
* Previous other relevant audits = <add date>
* Previous company meetings / quarterly meetings = <add date>
* Other events (BCM test, …) = <add date>

# Status of actions from previous reviews

**[Reference: ISO27001 Clause 9.3.2 a)]**

Previous Management Review = <add date>

Status of actions

* Action definition & reference from previous meeting
* include status, like
  + Closed
  + open/ongoing
  + halted, …

# Changes in external and internal issues (relevant to ISMS

**[Reference: ISO27001 Clause 9.3.2 b)]**

## External (Part 1/2)

* Prospects
* Customers
* Legal
* Government
* Competition
* Market
* Politics

## Internal (Part 2/2)

* HR
* Legal
* Business
* Sales
* Marketing
* IT
* Security
* ISMS
* …

# Changes in needs from interested parties

**[Reference: ISO27001 Clause 9.3.2 c)]**

Document changes in needs and expectations of interested parties

Feedback from internal & external interested parties

* Customers
* Partners
* Visitors
* Management
* Employees
* Staff
* Contractors
* Suppliers
* …

# Feedback on security performance

**[Reference: ISO27001 Clause 9.3.2 d)]**

Feedback on security performance includes

* NCs and corrective actions
* Monitoring and measuring results
* Audit results
* Fullfilment of objectives

## NCs and corrective actions

**[Reference: ISO27001 Clause 9.3.2 b) 1)]**

### List NCs

* #Major NC
* #Minor NC
* OFI
* But also …Incidents

### Corrective actions

* …

## Monitoring/Measurement results

**[Reference: ISO27001 Clause 9.3.2 b) 2)]**

* Metric 1
* Metric 2

## External/Internal Audit Results

**[Reference: ISO27001 Clause 9.3.2 b) 3)]**

### Legend

* STR = strength
* OFI = opportunity for improvement
  + Risk to nc
  + Evaluation by company for action, or not
* -nc = minor nonconformity
  + Action plan required
* +NC = major nonconformity
  + Immediate Action (plan) required

### External Audit

#### Results overview

* # STR (strength)
* # OFI (opportunity for improvement)
* # -nc = minor conformity
* # +NC = major nonconformity

#### Audit results (short description)

(<date previous audit>)

##### STR

* STR1= <explication>
* STR2= <explication>
* …

##### NC+

* NC1 = <explanation>
* NC2 = <explanation>
* NC3 = <explanation>

##### Nc-

* -nc1 = <explanation>
* -nc2 = <explanation>
* -nc3 = <explanation>

##### OFI

* OFI1= <explication>
* OFI2= <explication>
* …

### Internal Audit

#### Results overview

* # STR (strength)
* # OFI (opportunity for improvement)
* # -nc = minor conformity
* # +NC = major nonconformity

#### Audit results (short description)

(<date previous audit>)

##### STR

* STR1= <explication>
* STR2= <explication>
* …

##### NC+

* NC1 = <explanation>
* NC2 = <explanation>
* NC3 = <explanation>

##### Nc-

* -nc1 = <explanation>
* -nc2 = <explanation>
* -nc3 = <explanation>

##### OFI

* OFI1= <explication>
* OFI2= <explication>
* …

## Fullfilment of ISMS objectives

**[Reference: ISO27001 Clause 9.3.2 b) 4)]**

Objectives (as defined in ISMS)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Objective name | Metric | Target Value | Achieved or not | Trend |
|  |  |  |  |  |
|  |  |  |  |  |

**Trend Legend**

* ⬆️ ++
* ↗️+
* ➡️=
* ↘️ -
* ⬇️ --

# Feedback from interested parties

**[Reference: ISO27001 Clause 9.3.2 e)]**

Document changes in needs and expectations of interested parties

Feedback from internal & external interested parties

* Customers
* Partners
* Visitors
* Management
* Employees
* Staff
* Contractors
* Suppliers
* …

Feedback can be

* Direct from surveys, interactions, questionaires
* Indirect from continued sales, new orders, social media feedback, …

## Management

## Employees

## Customers

## Suppliers

## <other>

# Results of risk management and status of treatment plan

**[Reference: ISO27001 Clause 9.3.2 f)]**

* Sources
  + Tickets
  + Incidents
  + Changes
  + …
* Risk Assessment result
* New / changed / mitigated risks
* Action plans
* Other
* …

# Business - Opportunities for improvement (management)

**[Reference: ISO27001 Clause 9.3.2 g) 1)]**

## Improvement opportunities for company (mgmt level)

* OFI 1
* …

# Management decisions

**[Reference: ISO27001 Clause 9.3.3 ]**

* + Decision 1
  + Decision 2
  + …

# Planning next management review ISO27001

Set date for next management review meeting

# Annexes

## (ISMS) Reference documentation

## (Link to) External Audit reports ISO27001

## (Link to) Internal audit report ISO27001

## (Link to) Other audit reports (pentest, SOC, ...)

## Customer Surveys

## Tickets

## Risk management plan

## …