ISO27001 Management Review

<Company> - <Date Completed>

Contents

[2 Usage guide – Manual 3](#_Toc167460320)

[2.1 Point of attention/Topic 3](#_Toc167460321)

[2.2 Document parameters 3](#_Toc167460322)

[3 Agenda 4](#_Toc167460323)

[4 (Optional) overview agenda - Important events 4](#_Toc167460324)

[5 Status of actions from previous reviews 5](#_Toc167460325)

[6 Changes in external and internal issues (relevant to ISMS) 5](#_Toc167460326)

[6.1 External (Part 1/2) 5](#_Toc167460327)

[6.2 Internal (Part 2/2) 5](#_Toc167460328)

[7 Feedback on security performance 5](#_Toc167460329)

[7.1 NCs and corrective actions 5](#_Toc167460330)

[7.1.1 List NCs and corrective actions 5](#_Toc167460331)

[7.1.2 Corrective actions 6](#_Toc167460332)

[7.2 Monitoring/Measurement results 6](#_Toc167460333)

[8 External/Internal Audit Results 6](#_Toc167460334)

[8.1 legend 6](#_Toc167460335)

[8.2 External Audit 6](#_Toc167460336)

[8.2.1 Results overview 6](#_Toc167460337)

[8.2.2 Audit results (short description) 6](#_Toc167460338)

[8.3 Internal Audit: 7](#_Toc167460339)

[8.3.1 Results overview 7](#_Toc167460340)

[8.3.2 Audit results (short description) 7](#_Toc167460341)

[9 Feedback on security performance 7](#_Toc167460342)

[9.1 Fullfilment of ISMS objectives 7](#_Toc167460343)

[10 Feedback from interested parties 7](#_Toc167460344)

[10.1 Management 8](#_Toc167460345)

[10.2 Employees 8](#_Toc167460346)

[10.3 Customers 8](#_Toc167460347)

[10.4 Suppliers 8](#_Toc167460348)

[10.5 <other> 8](#_Toc167460349)

[11 Results of risk management and status of treatment plan 8](#_Toc167460350)

[12 Business - Opportunities for improvement (management) 8](#_Toc167460351)

[12.1 Improvement opportunities for company (mgmt level) 8](#_Toc167460352)

[13 Management decisions 8](#_Toc167460353)

[14 Planning next management review ISO27001 9](#_Toc167460354)

[15 Annexes 9](#_Toc167460355)

[15.1 (ISMS) Reference documentation 9](#_Toc167460356)

[15.2 (Link to) External Audit reports ISO27001 9](#_Toc167460357)

[15.3 (Link to) Internal audit report ISO27001 9](#_Toc167460358)

[15.4 (Link to) Other audit reports (pentest, SOC, ...) 9](#_Toc167460359)

[15.5 Customer Surveys 9](#_Toc167460360)

[15.6 Tickets 9](#_Toc167460361)

[15.7 Risk management plan 9](#_Toc167460362)

[15.8 … 9](#_Toc167460363)

# 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

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)

## External (Part 1/2)

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

## Internal (Part 2/2)

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

# Feedback on security performance

Feedback on security performance includes

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

## NCs and corrective actions

### List NCs and corrective actions

* #Major NC
* #Minor NC
* OFI
* Incidents

### Corrective actions

* …

## Monitoring/Measurement results

* Metric 1
* Metric 2

# External/Internal Audit Results

## 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>
* …

# Feedback on security performance

## Fullfilment of ISMS objectives

Objectives (as defined in ISMS)

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

**Trend Legend**

* ⬆️ ++
* ↗️+
* ➡️=
* ↘️ -
* ⬇️ --

# Feedback from 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

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

# Business - Opportunities for improvement (management)

## Improvement opportunities for company (mgmt level)

* OFI 1
* …

# Management decisions

* + 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

## …