WELCOME

# Success stories for Small & Medium Enterprises (SME) risk management and ISMS implementation

10 February 2021

# Some Housekeeping before we start

- Make sure you appear on MS Teams with the same
  First Name, Last Name used for registration to acquire CPEs.
- Presentation might be recorded,
  along with the slides it might be released by mail after the session
- Please mute your microphone and stop sharing your video camera
  as soon as you enter the session
- If you have any questions, please use the raise hand feature
  or type it in the chat box

# Thanks for attending ISACA Square Tables

Next Square Table Webinar: February 17, 2021

Different Time: 18:00 – 19:00h

Oh! My supplier did not deliver…
How to build resiliency in supply chain
Speaker: Sunil Bakshi

# Agenda

- About the speakers
- SME in the Netherlands
- ISMS example 1 (Atlassian)
- ISMS example 2 (Office 365)

# Gilbert van Zeijl

- Certified Security and Privacy Officer
- > 25 years IT experience
- > 20 years Health care experience
- Information quality and security
- Privacy
- IT Risk management
- IT auditor

- Software & SAAS companies
- Health Care & Cure
- Small Medium Enterprises

✉ G.vanzeijl@zorgzuid.nl

in Gilbert Van Zeijl (CISA, CISM, CIPP-E, CIPM) | LinkedIn

# Nico van Rooyen

- Certified Information Security Manager
- Certified Information Systems Auditor
- Certified Ethical Hacker
- > 8 years Privacy and security experience
- Regulation Compliance
- IT auditor
- ISO 27001

- Online gambling
- E-Commerce
- Small Medium Enterprises

✉ onvanrooyen@gmail.com

in Nico van Rooyen | LinkedIn

# Small Medium Enterprises in the Netherlands

70% werkzame personen
marktsector in MKB
2018

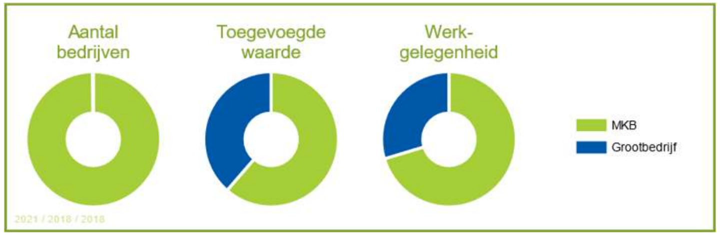
70% Dutch employed persons

€1 027 miljard
omzet door MKB
€
2018

€1027 Bilion yearly revenue

1,92 miljoen
bedrijven in het MKB
2021

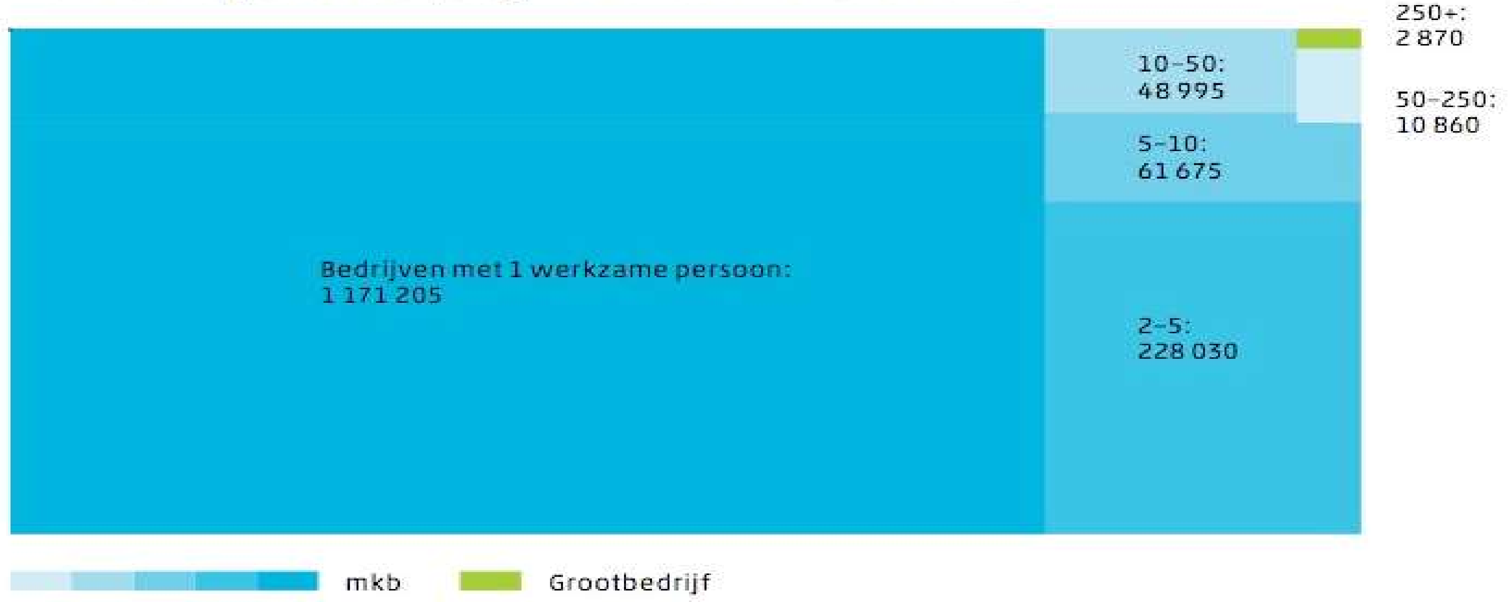
1.92 Milion SME companies



60% added value

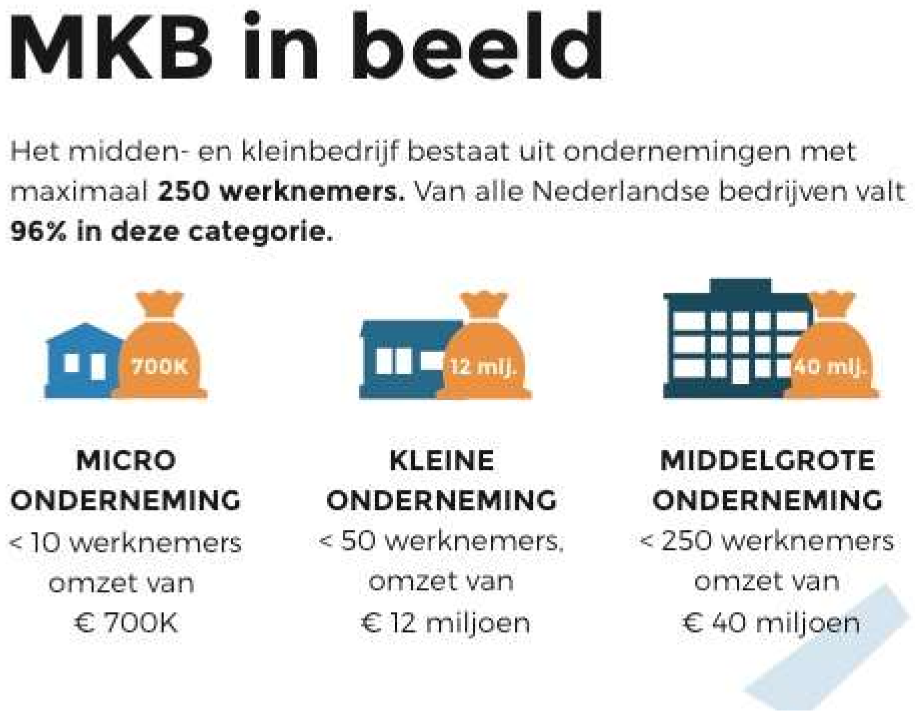
# Company size, The Netherlands

werkzame personen, begin vierde kwartaal 2015



Source: De Staat van het MKB 2015; CBS

# SME definition



## MKB in beeld

Het midden- en kleinbedrijf bestaat uit ondernemingen met maximaal **250 werknemers.** Van alle Nederlandse bedrijven valt **96% in deze categorie.**

700K
12 mlj.
40 mlj.

**MICRO ONDERNEMING**
< 10 werknemers
omzet van
€ 700K

**KLEINE ONDERNEMING**
< 50 werknemers,
omzet van
€ 12 miljoen

**MIDDELGROTE ONDERNEMING**
< 250 werknemers
omzet van
€ 40 miljoen

Micro: < 10 employees
< €700 k

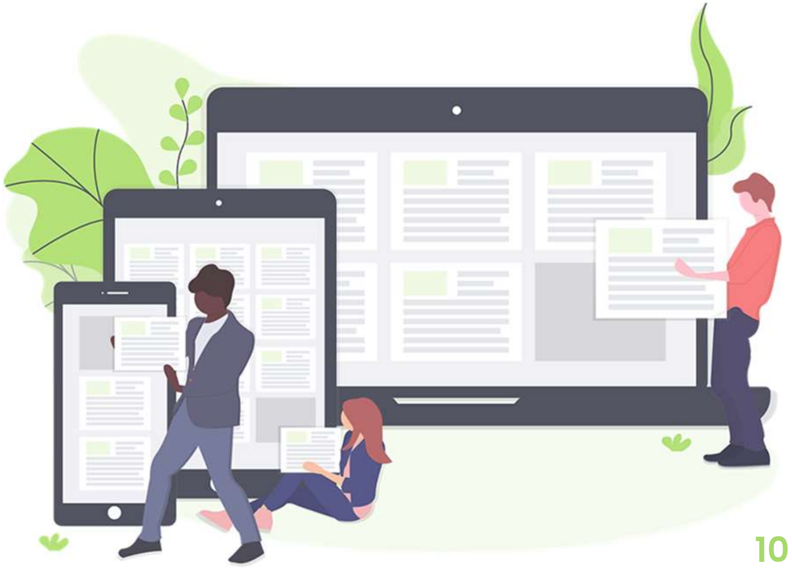
Small: < 50 employees
< €12 M

Medium: < 250 employees
<€40 M

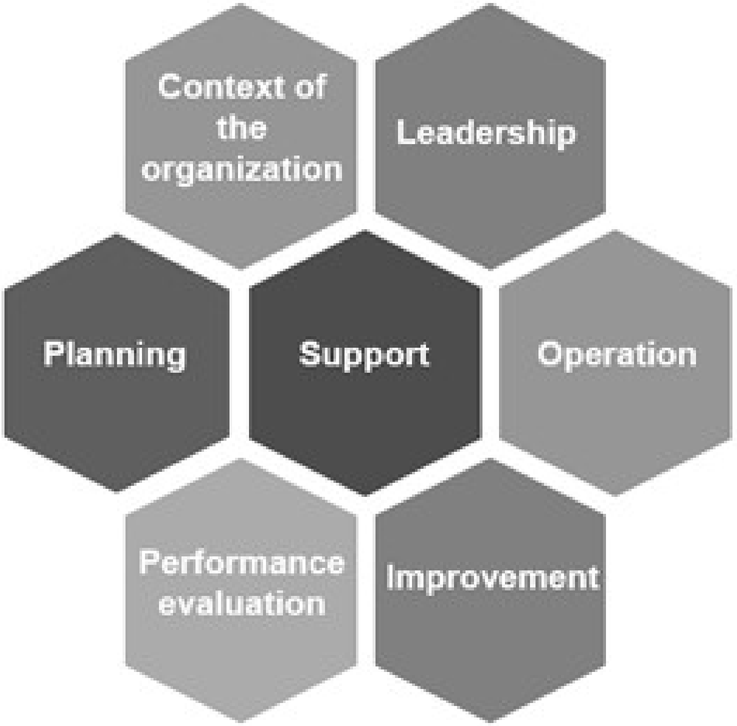
Source: MKB in beeld (MKB servicedesk.nl)

# ISMS example 1

- Using Atlassian



# ISO High Level Structure



# Example of a Software company

Context of the organisation using Business Canvas

Key Partners

IT hosting partner
IT housing partner

Marketing partner
Knowledge partner

External developers
External testers

Finance & administration

Key Activities

**Product Development**

**Product delivery**

**Customer Support**

**Sales & Marketing**

Key resources

IP / knowledge
Employees
Director/owner

Primary Information system

Customer data

Value Proposition

SAAS dienst, App of Web.

Software

Consultancy

Customer relationships

Channels

Webpage
Digital newsletter

Direct marketing

Customer Segments

Cost Structures

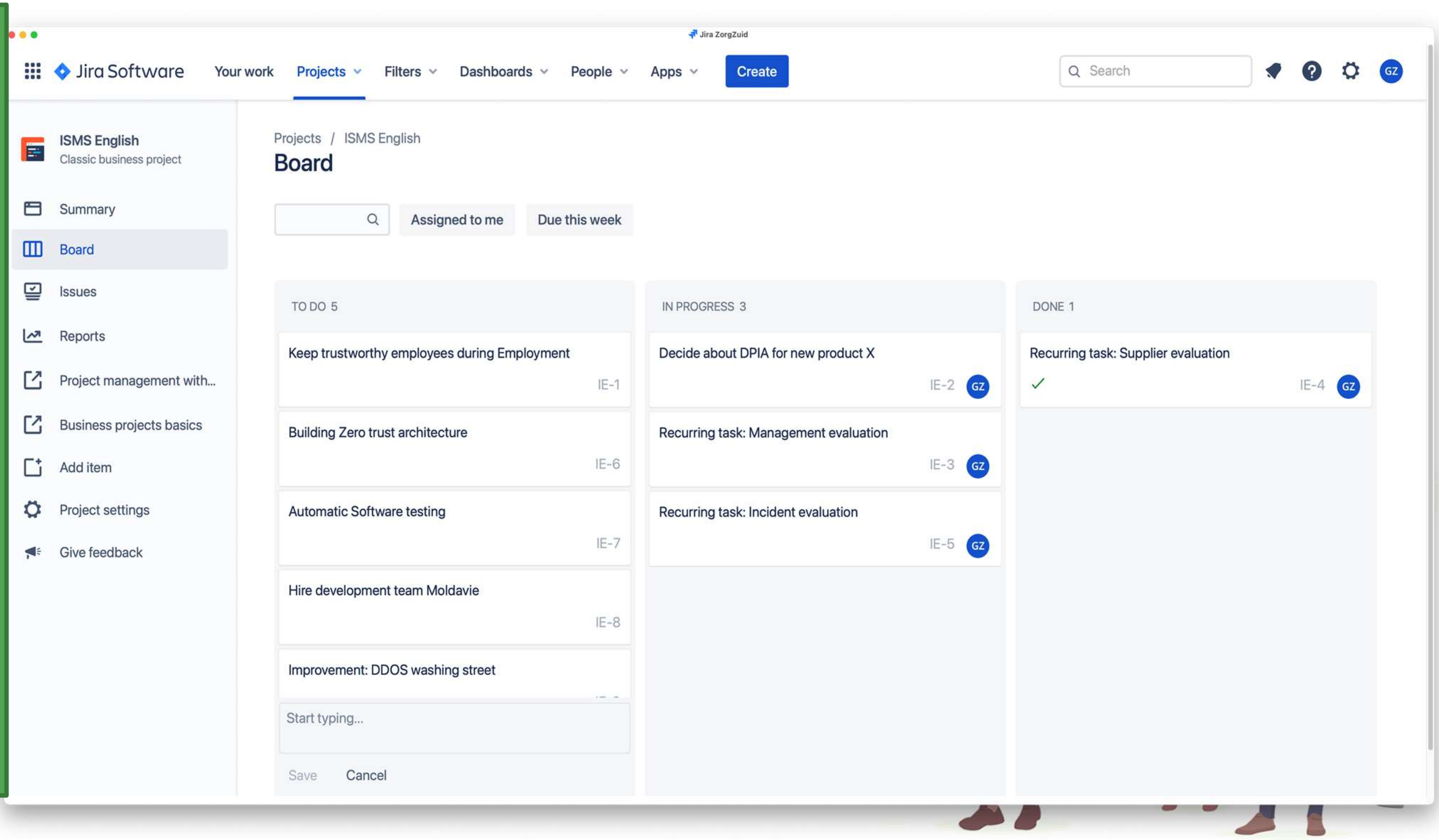
Labour / personell (In- External) 80%
Hosting / housing IT
Rest: marketing, administration, advisors, suppliers

Revenu Streams

Recurring revenu.

One-time / project revenue

Planning, support, operation



## Board

TO DO 5

- Keep trustworthy employees during Employment IE-1
- Building Zero trust architecture IE-6
- Automatic Software testing IE-7
- Hire development team Moldavie IE-8
- Improvement: DDOS washing street

Start typing...

Save Cancel

IN PROGRESS 3

- Decide about DPIA for new product X IE-2 GZ
- Recurring task: Management evaluation IE-3 GZ
- Recurring task: Incident evaluation IE-5 GZ

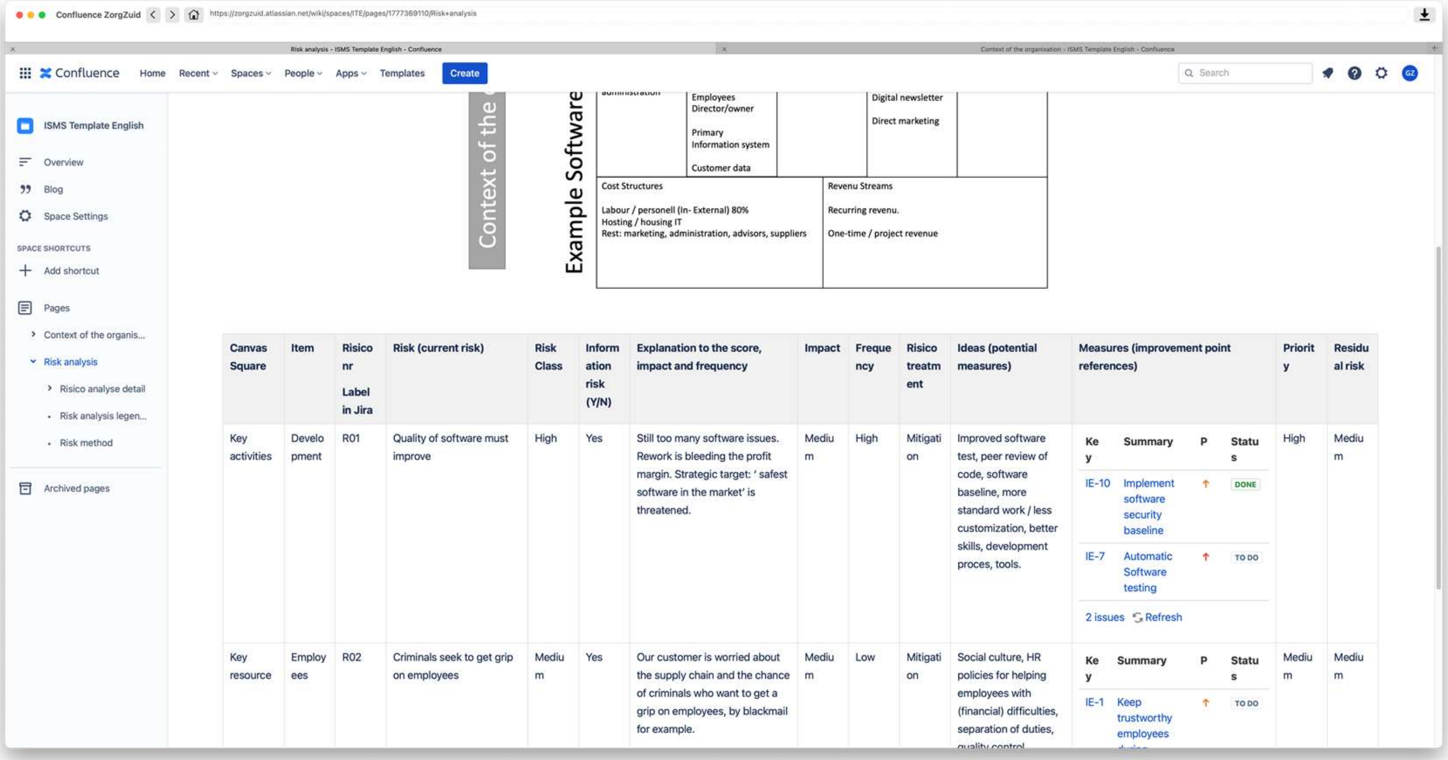
DONE 1

- Recurring task: Supplier evaluation ✓ IE-4 GZ

# Risk management

- Management involvement
- Based on business canvas as risk framework
- Percieved risk is thus business risk
- Mitigating measures defined on improvement board (Jira)
- Simple feedback on status in risk matrix (Jira Query)
- Examples in Jira / Confluence

# Risk management Example



Employees
Director/owner

Primary
Information system

Customer data

Digital newsletter

Direct marketing

Cost Structures

Labour / personell (In- External) 80%
Hosting / housing IT
Rest: marketing, administration, advisors, suppliers

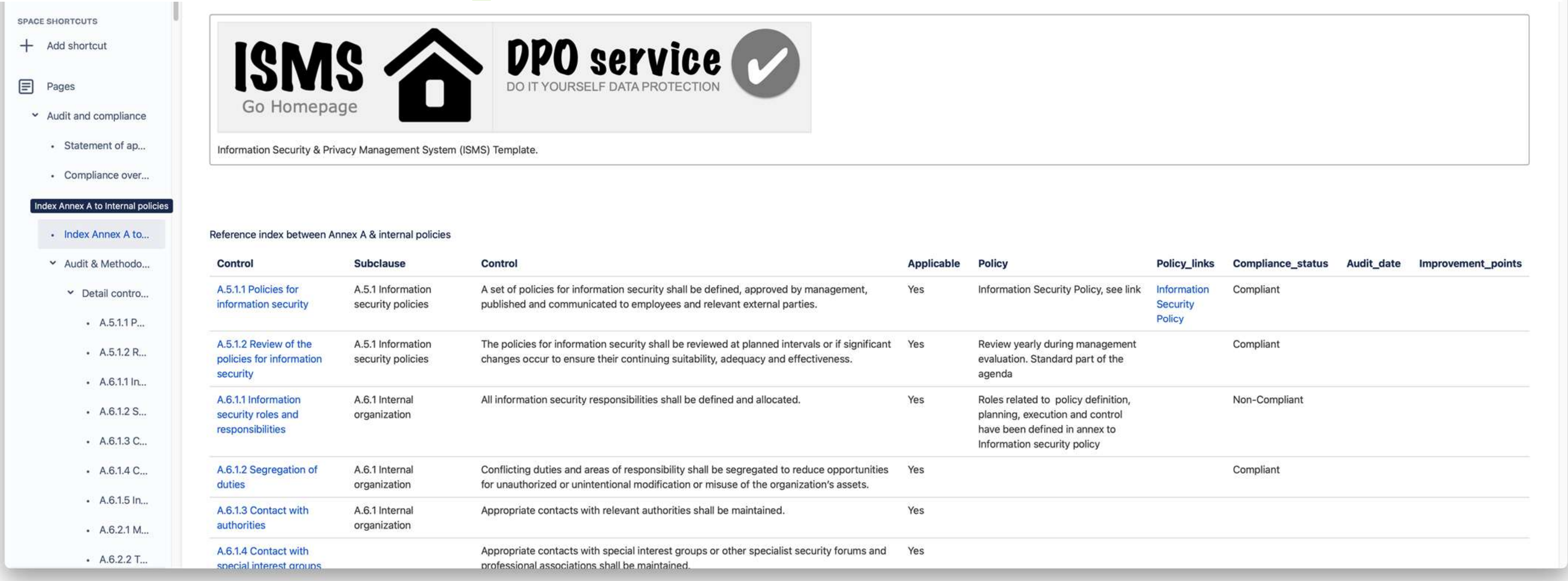
Revenu Streams

Recurring revenu.

One-time / project revenue

| Canvas Square | Item | Risico nr<br>Label in Jira | Risk (current risk) | Risk Class | Information risk (Y/N) | Explanation to the score, impact and frequency | Impact | Frequency | Risico treatment | Ideas (potential measures) | Measures (improvement point references) | Priority | Residual risk |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Key activities | Development | R01 | Quality of software must improve | High | Yes | Still too many software issues. Rework is bleeding the profit margin. Strategic target: ' safest software in the market' is threatened. | Medium | High | Mitigation | Improved software test, peer review of code, software baseline, more standard work / less customization, better skills, development proces, tools. | Key · Summary · P · Status<br>IE-10 · Implement software security baseline · ↑ · DONE<br>IE-7 · Automatic Software testing · ↑ · TO DO<br>2 issues Refresh | High | Medium |
| Key resource | Employees | R02 | Criminals seek to get grip on employees | Medium | Yes | Our customer is worried about the supply chain and the chance of criminals who want to get a grip on employees, by blackmail for example. | Medium | Low | Mitigation | Social culture, HR policies for helping employees with (financial) difficulties, separation of duties, quality control | Key · Summary · P · Status<br>IE-1 · Keep trustworthy employees during · ↑ · TO DO | Medium | Medium |

# Link ISO standard with internal policies



Information Security & Privacy Management System (ISMS) Template.

Reference index between Annex A & internal policies

| Control | Subclause | Control | Applicable | Policy | Policy_links | Compliance_status | Audit_date | Improvement_points |
|---|---|---|---|---|---|---|---|---|
| A.5.1.1 Policies for information security | A.5.1 Information security policies | A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties. | Yes | Information Security Policy, see link | Information Security Policy | Compliant | | |
| A.5.1.2 Review of the policies for information security | A.5.1 Information security policies | The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | Yes | Review yearly during management evaluation. Standard part of the agenda | | Compliant | | |
| A.6.1.1 Information security roles and responsibilities | A.6.1 Internal organization | All information security responsibilities shall be defined and allocated. | Yes | Roles related to policy definition, planning, execution and control have been defined in annex to Information security policy | | Non-Compliant | | |
| A.6.1.2 Segregation of duties | A.6.1 Internal organization | Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. | Yes | | | Compliant | | |
| A.6.1.3 Contact with authorities | A.6.1 Internal organization | Appropriate contacts with relevant authorities shall be maintained. | Yes | | | | | |
| A.6.1.4 Contact with special interest groups | | Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained. | Yes | | | | | |

# ISMS example 2

- Using Office 365

# Working with SMEs

### The Good

- Limited bureaucracy
- Few decision makers
- Fast adapting and ever changing organisation culture
- Major contributions by few people

### The Bad

- Limited resources (man power and funds)
- Dependency on key recourses
- Projects loose momentum
- Expect more pay less attitude
- Limited accountability

### The Ugly truth

- More systems than employees
- Outsourcing is often cost effective
- Limited skill inhouse

# Before you start your ISMS

**What do you need to know?**

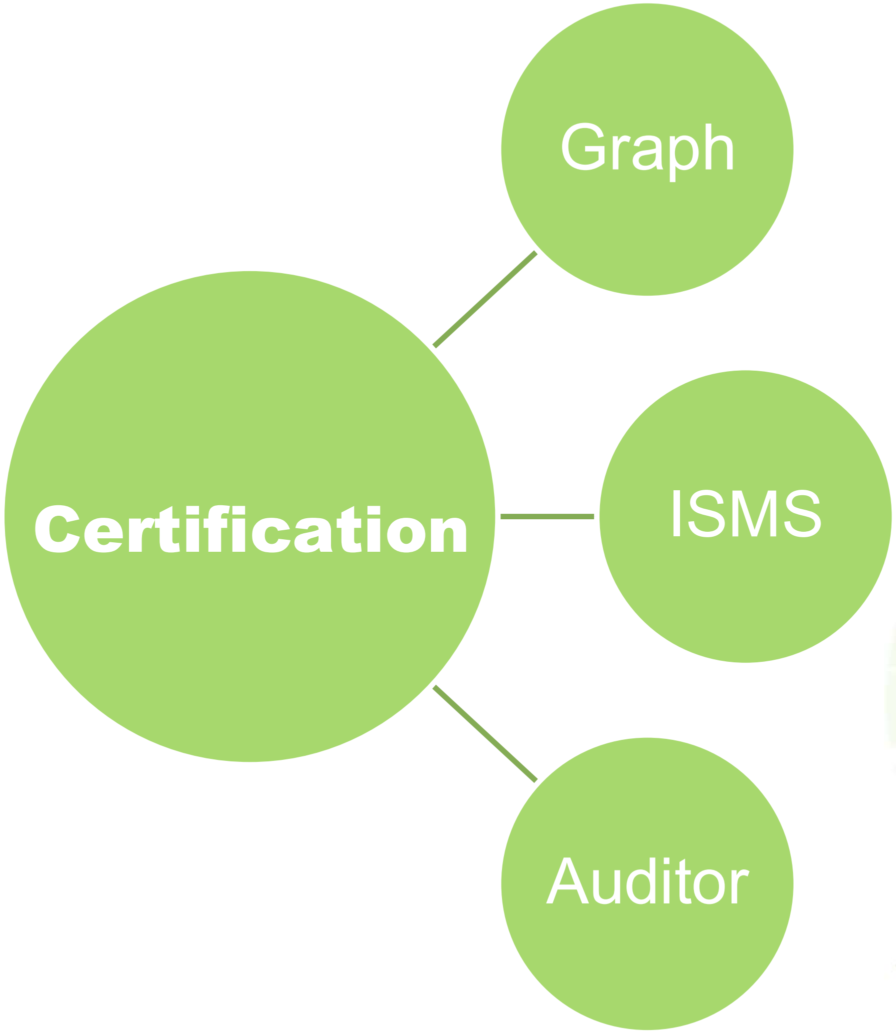
- Your organisational strategy
- Your cost per control
- The impact of the ISMS on the way of working
- Tools and skills at your disposal

**What do you need to do?/ Where do you start?**

- First, Integrate effective controls
- Integrate low hanging fruit
- Integrate full or limited audit scope
- Lastly, integrate failed controls by designing them as effective controls

**Automation is key!** Comply with more controls using fewer people and less resources.

“Auditors
think in lists.  Auditees think in graphs.
As long as this is true,-
auditees  win.”
John Lambert



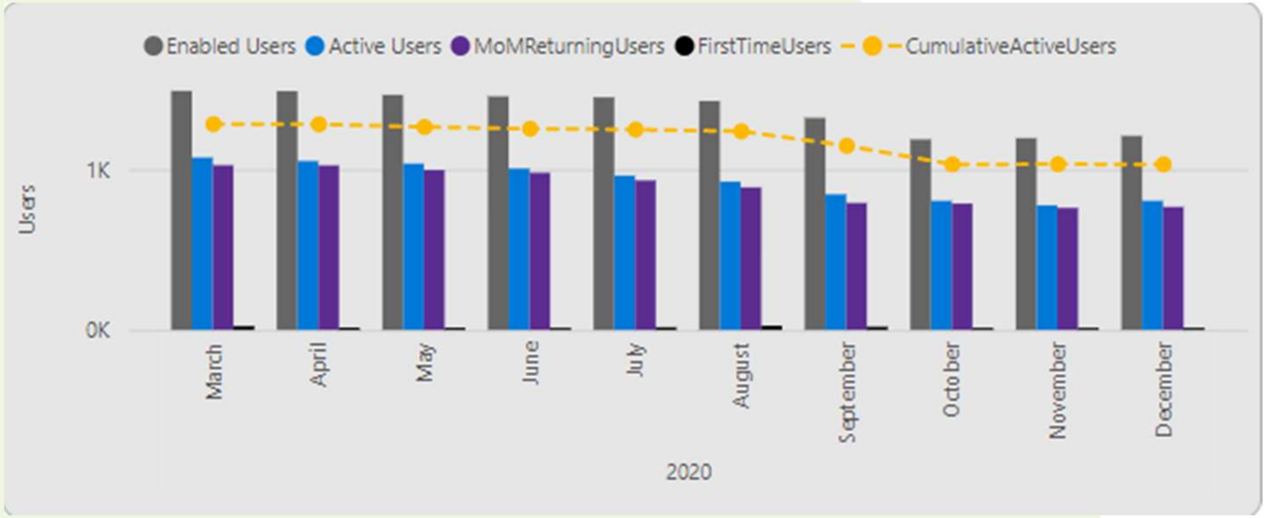
**Certification**

Graph

ISMS

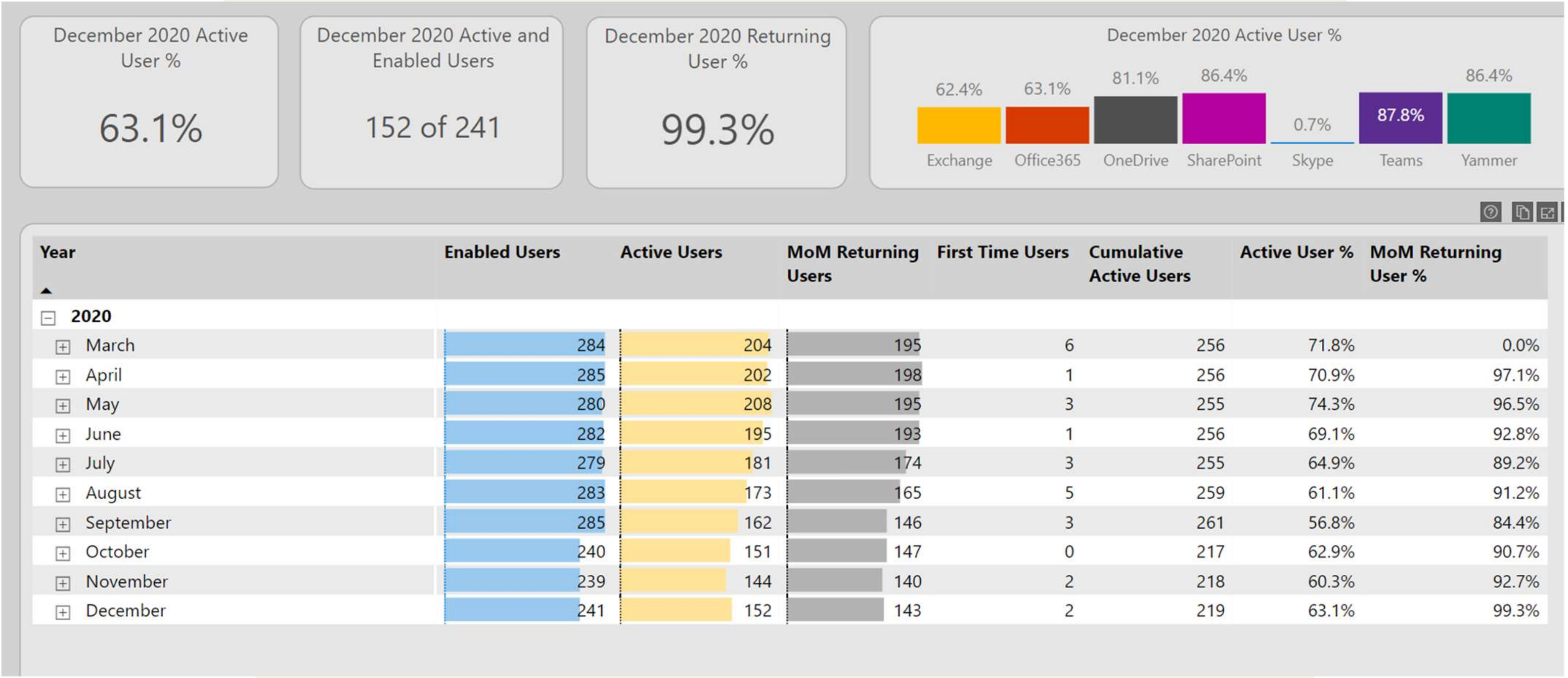
Auditor

# Graph



- Enabled users = number of licences allocated / available
- Active users = users active in the month
- MoM returning users = users active in the month that were also active in the preceding month
- First time users = New users / employees

# Drill down view



December 2020 Active User %

63.1%

December 2020 Active and Enabled Users

152 of 241

December 2020 Returning User %

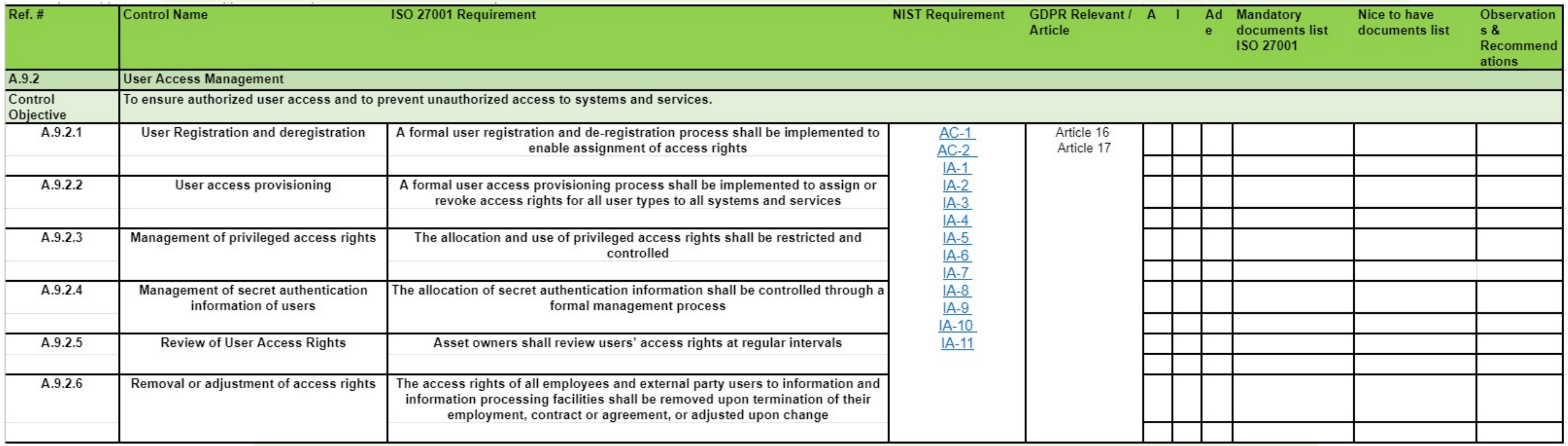
99.3%

December 2020 Active User %

| Exchange | Office365 | OneDrive | SharePoint | Skype | Teams | Yammer |
|---|---|---|---|---|---|---|
| 62.4% | 63.1% | 81.1% | 86.4% | 0.7% | 87.8% | 86.4% |

| Year | Enabled Users | Active Users | MoM Returning Users | First Time Users | Cumulative Active Users | Active User % | MoM Returning User % |
|---|---|---|---|---|---|---|---|
| ⊟ 2020 | | | | | | | |
| ⊞ March | 284 | 204 | 195 | 6 | 256 | 71.8% | 0.0% |
| ⊞ April | 285 | 202 | 198 | 1 | 256 | 70.9% | 97.1% |
| ⊞ May | 280 | 208 | 195 | 3 | 255 | 74.3% | 96.5% |
| ⊞ June | 282 | 195 | 193 | 1 | 256 | 69.1% | 92.8% |
| ⊞ July | 279 | 181 | 174 | 3 | 255 | 64.9% | 89.2% |
| ⊞ August | 283 | 173 | 165 | 5 | 259 | 61.1% | 91.2% |
| ⊞ September | 285 | 162 | 146 | 3 | 261 | 56.8% | 84.4% |
| ⊞ October | 240 | 151 | 147 | 0 | 217 | 62.9% | 90.7% |
| ⊞ November | 239 | 144 | 140 | 2 | 218 | 60.3% | 92.7% |
| ⊞ December | 241 | 152 | 143 | 2 | 219 | 63.1% | 99.3% |

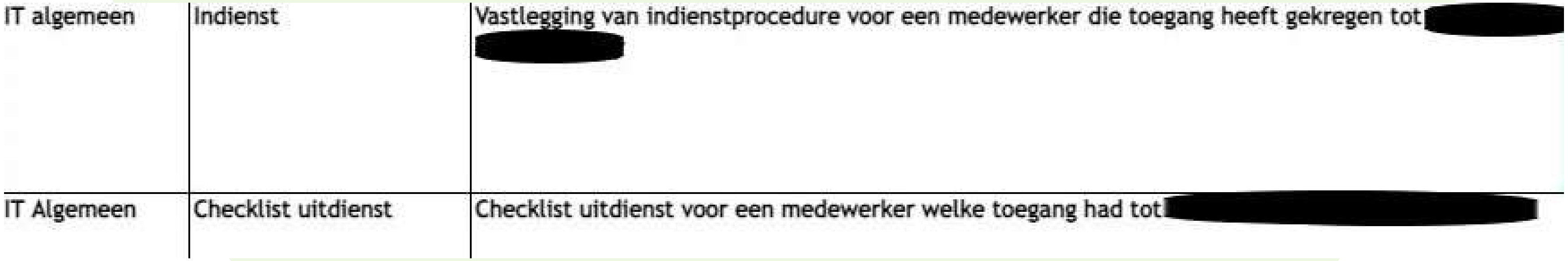
# ISMS



| Ref. # | Control Name | ISO 27001 Requirement | NIST Requirement | GDPR Relevant / Article | A | I | Ade | Mandatory documents list ISO 27001 | Nice to have documents list | Observations & Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|
| A.9.2 | User Access Management | | | | | | | | | |
| Control Objective | To ensure authorized user access and to prevent unauthorized access to systems and services. | | | | | | | | | |
| A.9.2.1 | User Registration and deregistration | A formal user registration and de-registration process shall be implemented to enable assignment of access rights | AC-1<br>AC-2<br>IA-1<br>IA-2<br>IA-3<br>IA-4<br>IA-5<br>IA-6<br>IA-7<br>IA-8<br>IA-9<br>IA-10<br>IA-11 | Article 16<br>Article 17 | | | | | | |
| A.9.2.2 | User access provisioning | A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services | | | | | | | | |
| A.9.2.3 | Management of privileged access rights | The allocation and use of privileged access rights shall be restricted and controlled | | | | | | | | |
| A.9.2.4 | Management of secret authentication information of users | The allocation of secret authentication information shall be controlled through a formal management process | | | | | | | | |
| A.9.2.5 | Review of User Access Rights | Asset owners shall review users' access rights at regular intervals | | | | | | | | |
| A.9.2.6 | Removal or adjustment of access rights | The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change | | | | | | | | |

Auditor

# Audit PBC list



| | | |
|---|---|---|
| IT algemeen | Indienst | Vastlegging van indienstprocedure voor een medewerker die toegang heeft gekregen tot [redacted] |
| IT Algemeen | Checklist uitdienst | Checklist uitdienst voor een medewerker welke toegang had tot [redacted] |

# The end