SURF

# Enhancing member satisfaction about security of your NREN

With certified security & suitability classification

Helma de Boer
Information Security Officer at SURF NL

Géant Security Days – Prague, 9-11 April 2024

# About SURF

**Around:**

- 500 staff
- 60 IT services
- 100+ members/institutes

**100+ Members:**

- Vocational and adult education
- Higher education
- Universities/scientific education
- University medical centres
- Research institutes

SURF Amsterdam
SURF Utrecht

# ISO 27001 certification Suitability classification

# Security Framework

## Global ISO 27001/27002 standard for infosec

January 2024:

- 24 SURF services under the ISO 27001 certification

Scope: “*computing, data storage and analysis, visualisation, authentication, authorisation and cloud and grid services*”

An external audit takes place annually in which compliance with this standard is tested.

NIS2

surge in cyber attacks

nationwide programme cyber resilience
educational sector

# Why??

Ministry of Education, Culture, Science

digital defence

the stakes are high

cyber attack 2019
Universiteit Maastricht

We are SURF!

# Compliance is not security

**This is true. Of course. Yes.**

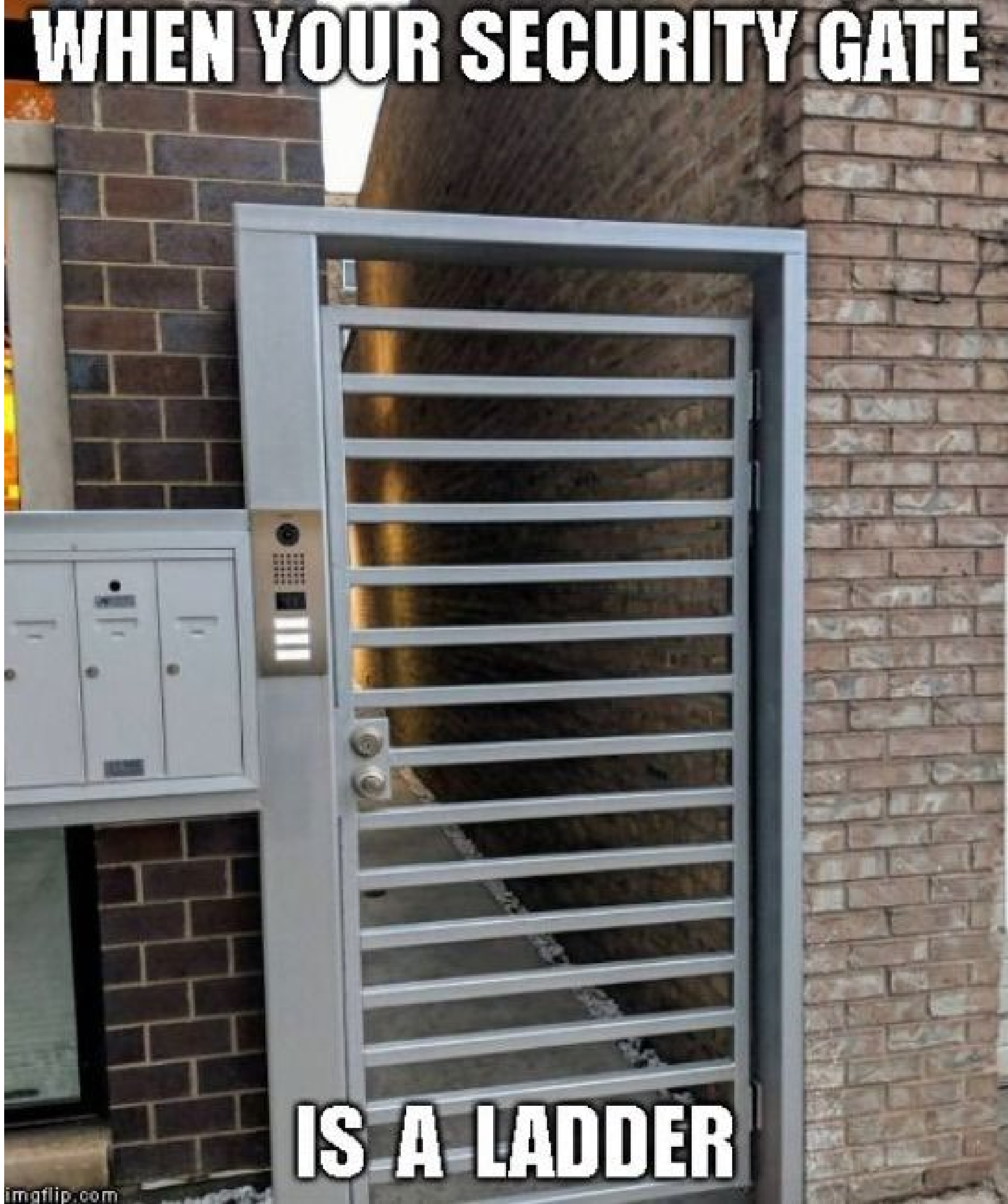
Framework says:

*<<some number – physical measures>>*
"A security gate is required to secure the premises and entrance of a building with your server room."

Implementation for compliance:

A security gate is installed

Actual "compliant" situation:



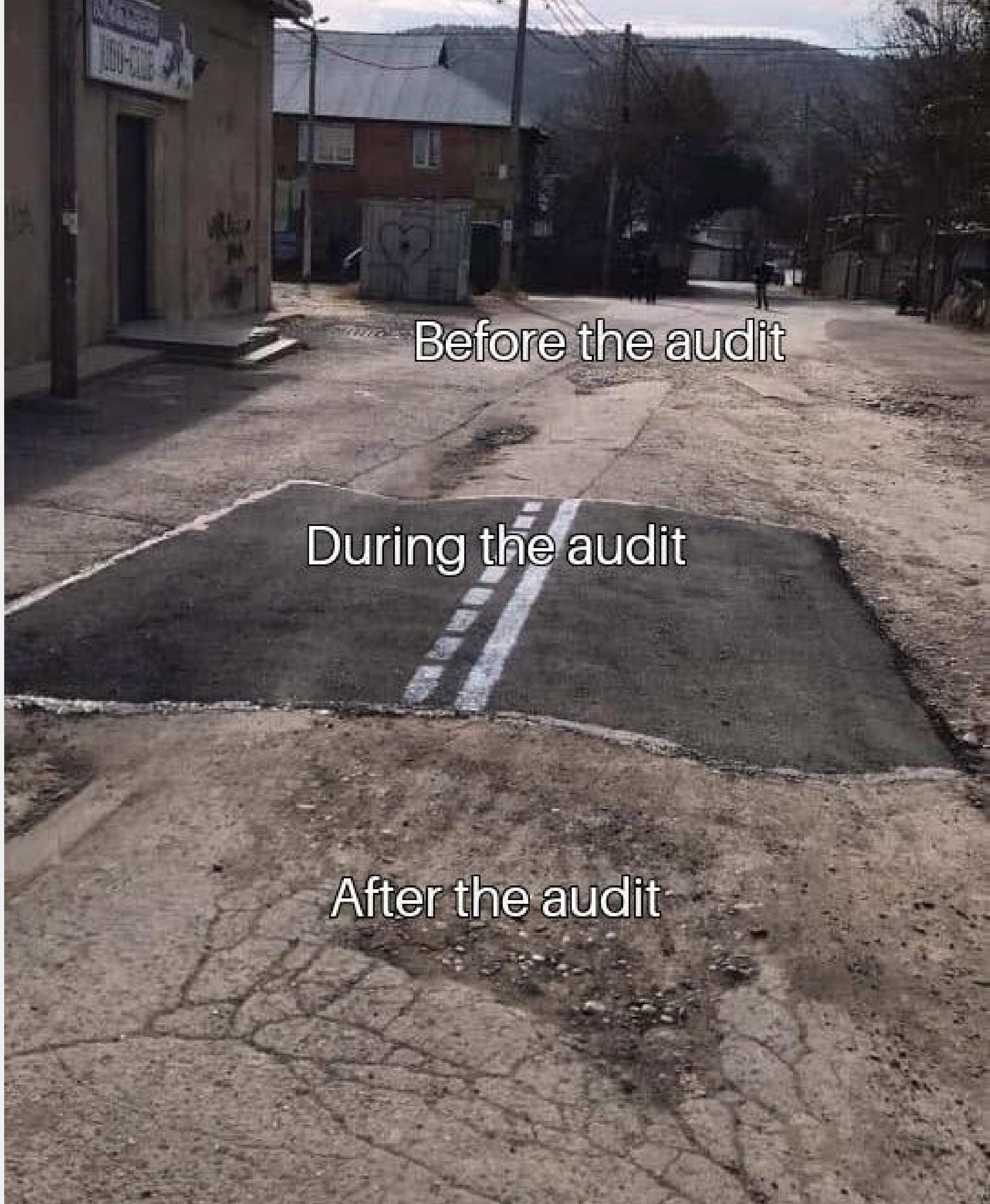
# It is not about nonconformities

# It is about effectiveness

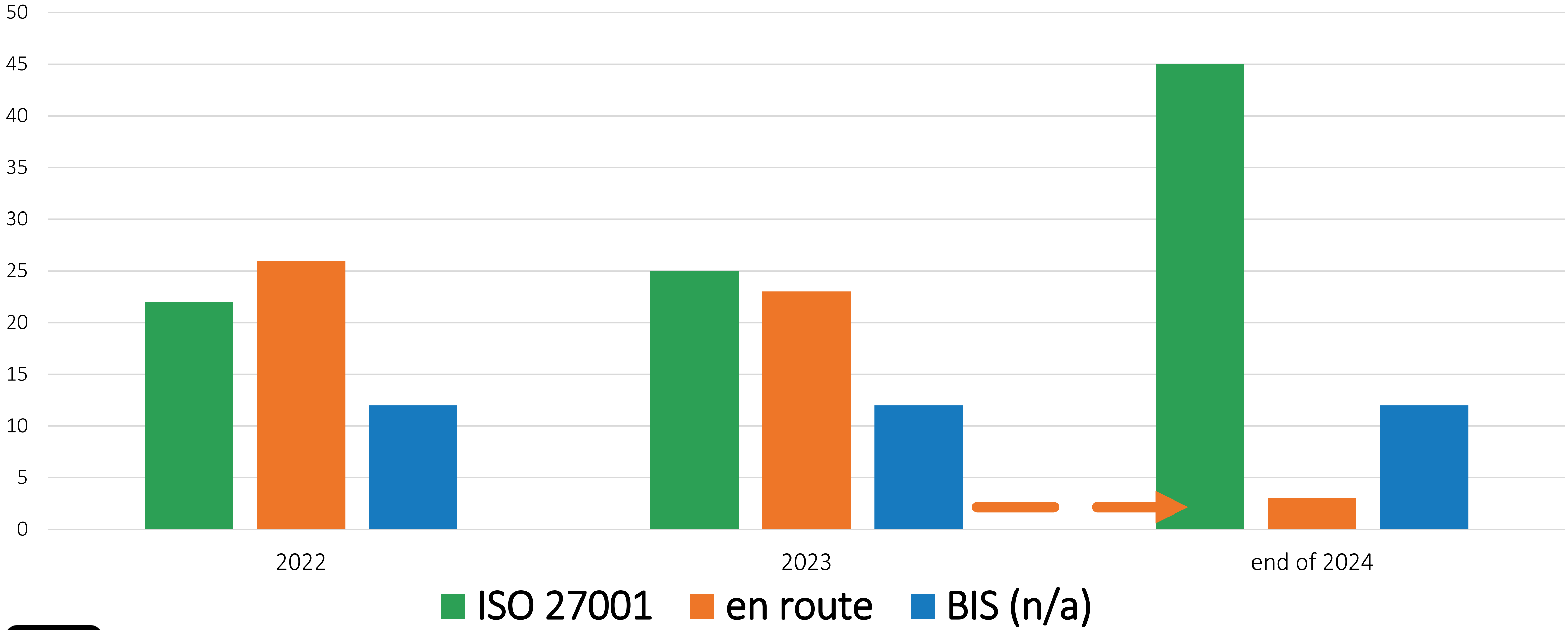
# We actually aim to improve ☺

MY CYBERSECURITY PROGRAM
OUTDATED CERTIFICATES
IMPROPERLY ENCRYPTED DATA
WEAK PASSWORDS
Balbix

# To prevent

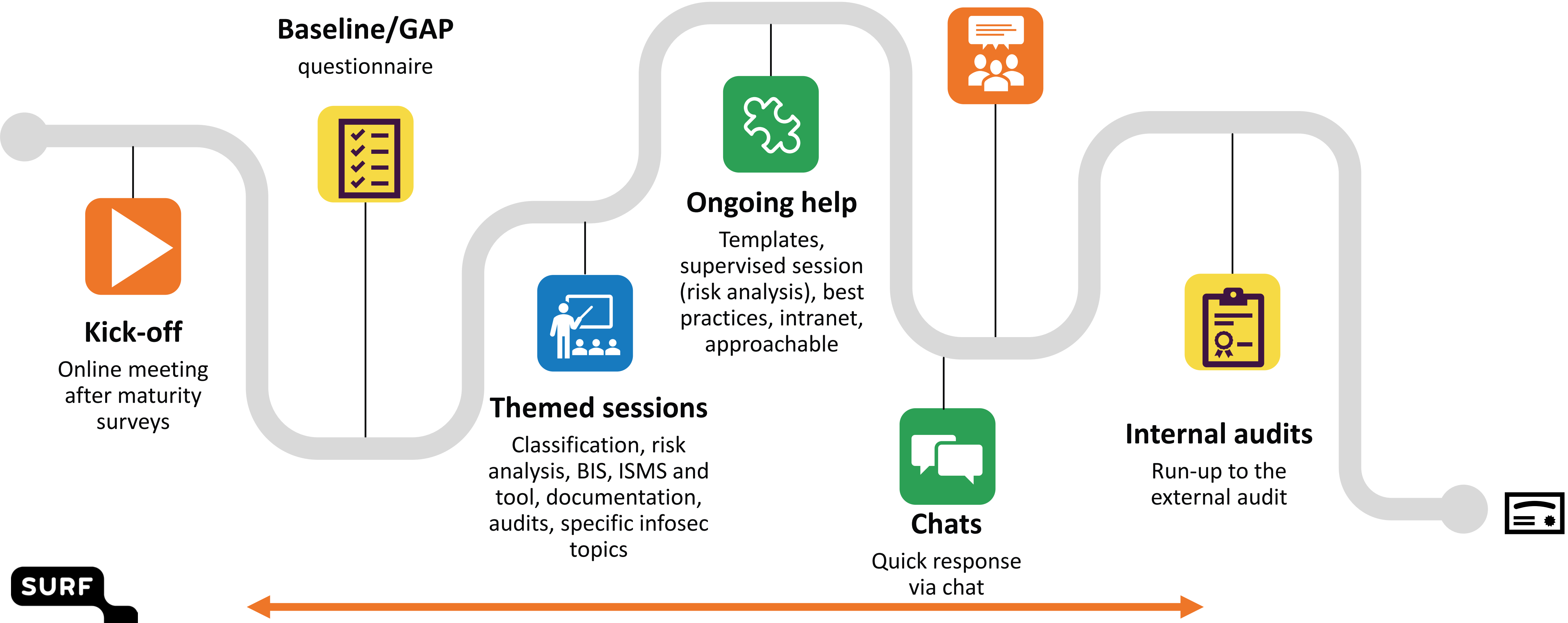


# ISO 27001 certification where relevant (48 services of 60)



BIS = Baseline Information security SURF

# ISO certification roadmap



**Kick-off**

Online meeting after maturity surveys

**Baseline/GAP**

questionnaire

**Themed sessions**

Classification, risk analysis, BIS, ISMS and tool, documentation, audits, specific infosec topics

**Ongoing help**

Templates, supervised session (risk analysis), best practices, intranet, approachable

**Walk-in clinics**

After themed sessions, also for helping/sharing

**Chats**

Quick response via chat

**Internal audits**

Run-up to the external audit

12 to 15 months

SURF

# Keeping collegues motivated

If we’re not drowning in our work,

we’ll drown in regulations on top of the work

How not to drown?

# Help, support, advice from the CISO team

kind
understanding
witty
helpful
tailored

**Programme**

Clear roadmap

**Themed sessions**

All topics covered

**Online collaboration**

Teams, intranet

**Documentation**

Documentation, recorded sessions, Q&A, explanations

**ISMS tool/GAP**

Clear focus when you know what you need

**Online walk-in sessions**

Questions, questions, help

**Tailored help**

Help for the team in guided sessions

**Chats, quick response**

Quick help, …. and off you go

SURF

# Roadmap

**7 steps in 7 months**

In between: walk-in clinics

Most important:
risk analysis and classification

Most difficult:
change management, IAM, supplier assessment

| Online sessions | Lorem ipsum |
|---|---|
| Run-up | Determining maturity level |
| 1 – Kick off | ISO 27001, H4-H10: ISMS & governance and discuss results baseline measurement |
| 2 – Classification (CIA) & risk analysis | After this session, we will schedule risk workshops to get you started (where required) |
| 3 – Baseline | Best practices, how to use, on what to focus |
| *Time* | *GAP, risk analyses, getting things in order, individual help teams* |
| 4 – Base27 | Explanation on our ISMS tool |
| 5 - Documentation | What documentation do you need, where do you find policies, procedures, templates |
| 6 – internal and external audits | How to go about audits, what to expect, why you must not worry |
| 7 – concluding session | Last questions, panic, help |

Next up:

_____________________

internal audit

+ 3 to 4 months:

external audit 🏅

# Baseline Information Security SURF (BIS)

# Protection level, example: exam results

*Guideline: the protection level '**Basic**' at SURF is approximately appropriate for information with confidentiality labels 'public', 'internal' and 'confidential'*

| Score | Confidentiality | Integrity | Availability |
|---|---|---|---|
| | | | |
| Basic | X | | X |
| High | | X | |
| | basic | high | basic |
| Result | B | H | B |

*Same measures*

H

*This CIA score is for the service as a whole*

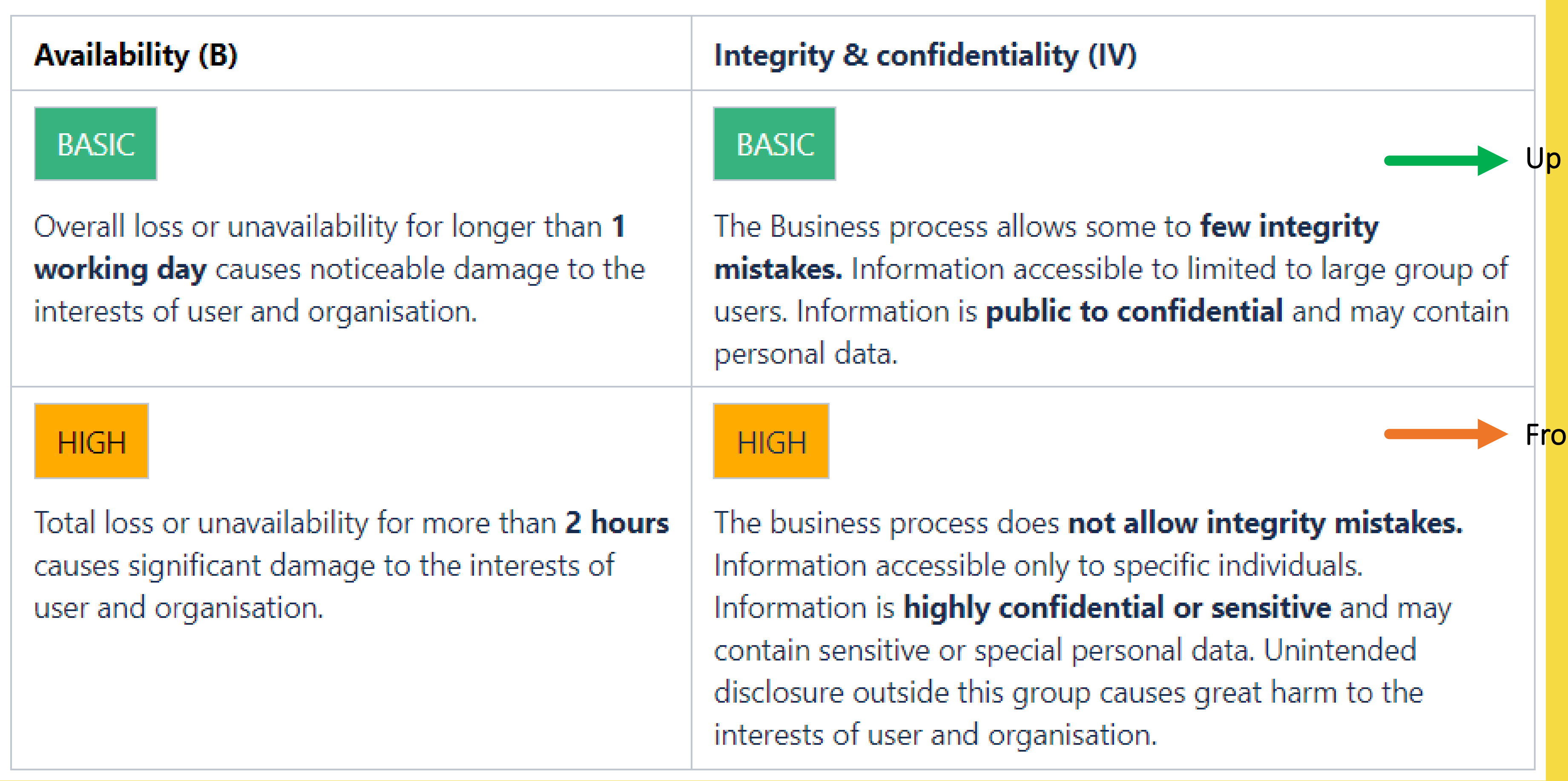
*Tools:*

- *Excel-template CIA score*
- *Business Impact Criteria (risk based, monetary damage)*

So: →

CI = High
A = Basic

# Easiest approach to determine the protection level

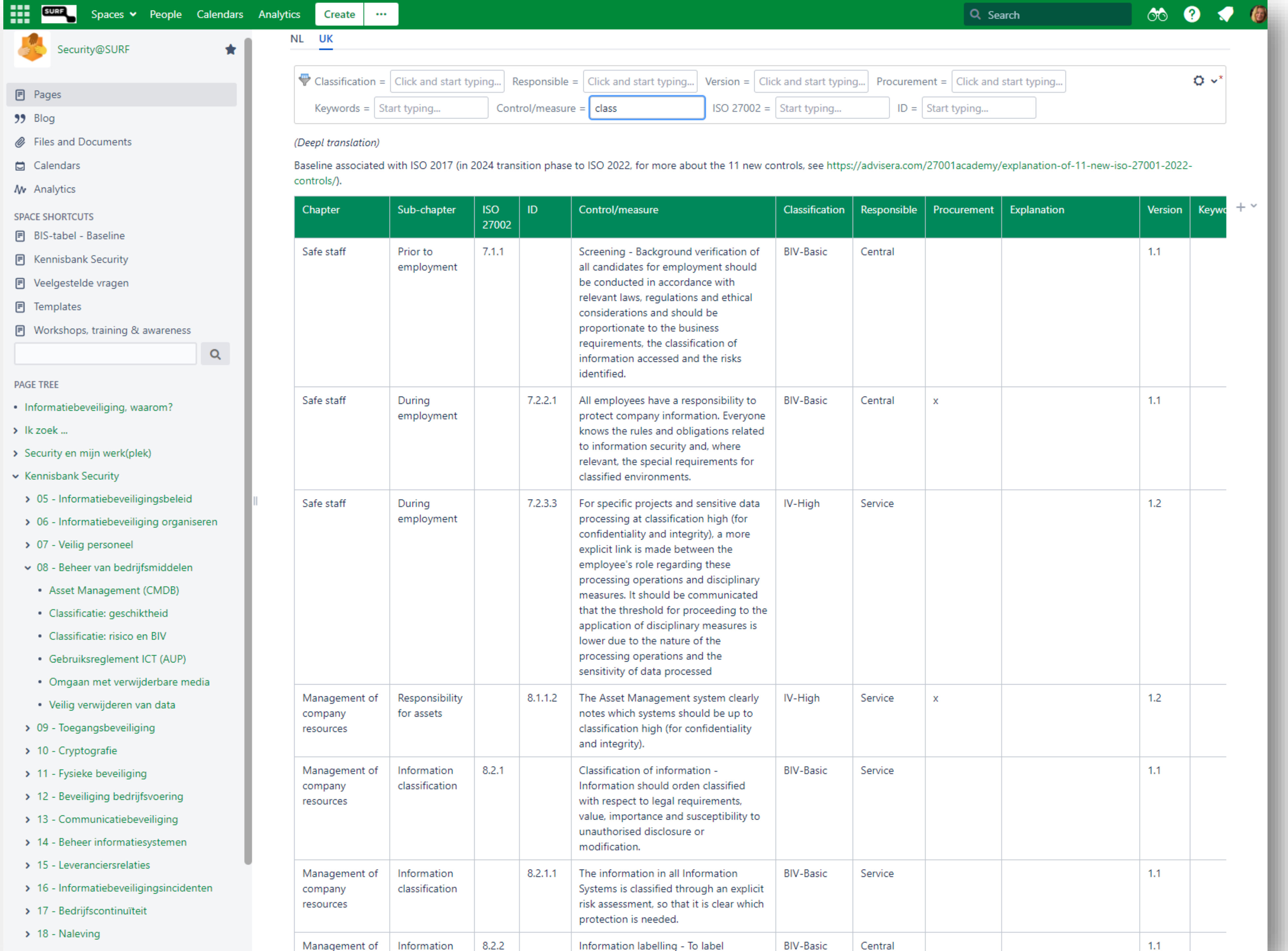


| Availability (B) | Integrity & confidentiality (IV) |
|---|---|
| BASIC<br>Overall loss or unavailability for longer than **1 working day** causes noticeable damage to the interests of user and organisation. | BASIC<br>The Business process allows some to **few integrity mistakes.** Information accessible to limited to large group of users. Information is **public to confidential** and may contain personal data. |
| HIGH<br>Total loss or unavailability for more than **2 hours** causes significant damage to the interests of user and organisation. | HIGH<br>The business process does **not allow integrity mistakes.** Information accessible only to specific individuals. Information is **highly confidential or sensitive** and may contain sensitive or special personal data. Unintended disclosure outside this group causes great harm to the interests of user and organisation. |

Up to € <amount>

From € <amount>

What is applicable in your situation?



Spaces
People
Calendars
Analytics
Create
···
Search
Security@SURF
Pages
Blog
Files and Documents
Calendars
Analytics
SPACE SHORTCUTS
BIS-tabel - Baseline
Kennisbank Security
Veelgestelde vragen
Templates
Workshops, training & awareness
PAGE TREE
Informatiebeveiliging, waarom?
Ik zoek ...
Security en mijn werk(plek)
Kennisbank Security
05 - Informatiebeveiligingsbeleid
06 - Informatiebeveiliging organiseren
07 - Veilig personeel
08 - Beheer van bedrijfsmiddelen
Asset Management (CMDB)
Classificatie: geschiktheid
Classificatie: risico en BIV
Gebruiksreglement ICT (AUP)
Omgaan met verwijderbare media
Veilig verwijderen van data
09 - Toegangsbeveiliging
10 - Cryptografie
11 - Fysieke beveiliging
12 - Beveiliging bedrijfsvoering
13 - Communicatiebeveiliging
14 - Beheer informatiesystemen
15 - Leveranciersrelaties
16 - Informatiebeveiligingsincidenten
17 - Bedrijfscontinuïteit
18 - Naleving
NL
UK

Classification = Click and start typing... Responsible = Click and start typing... Version = Click and start typing... Procurement = Click and start typing...

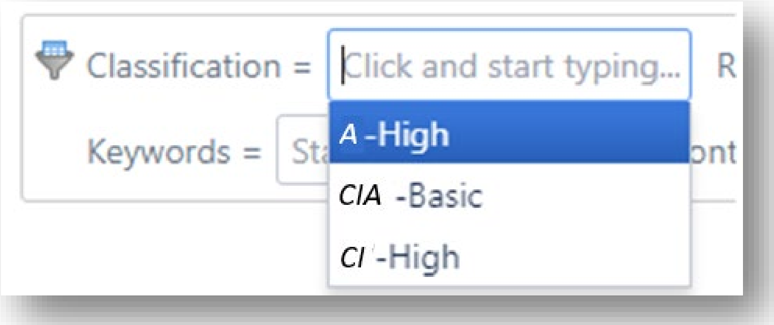
Keywords = Start typing... Control/measure = class ISO 27002 = Start typing... ID = Start typing...

*(Deepl translation)*

Baseline associated with ISO 2017 (in 2024 transition phase to ISO 2022, for more about the 11 new controls, see https://advisera.com/27001academy/explanation-of-11-new-iso-27001-2022-controls/).

| Chapter | Sub-chapter | ISO 27002 | ID | Control/measure | Classification | Responsible | Procurement | Explanation | Version | Keywo |
|---|---|---|---|---|---|---|---|---|---|---|
| Safe staff | Prior to employment | 7.1.1 | | Screening - Background verification of all candidates for employment should be conducted in accordance with relevant laws, regulations and ethical considerations and should be proportionate to the business requirements, the classification of information accessed and the risks identified. | BIV-Basic | Central | | | 1.1 | |
| Safe staff | During employment | | 7.2.2.1 | All employees have a responsibility to protect company information. Everyone knows the rules and obligations related to information security and, where relevant, the special requirements for classified environments. | BIV-Basic | Central | x | | 1.1 | |
| Safe staff | During employment | | 7.2.3.3 | For specific projects and sensitive data processing at classification high (for confidentiality and integrity), a more explicit link is made between the employee's role regarding these processing operations and disciplinary measures. It should be communicated that the threshold for proceeding to the application of disciplinary measures is lower due to the nature of the processing operations and the sensitivity of data processed | IV-High | Service | | | 1.2 | |
| Management of company resources | Responsibility for assets | | 8.1.1.2 | The Asset Management system clearly notes which systems should be up to classification high (for confidentiality and integrity). | IV-High | Service | x | | 1.2 | |
| Management of company resources | Information classification | 8.2.1 | | Classification of information - Information should orden classified with respect to legal requirements, value, importance and susceptibility to unauthorised disclosure or modification. | BIV-Basic | Service | | | 1.1 | |
| Management of company resources | Information classification | | 8.2.1.1 | The information in all Information Systems is classified through an explicit risk assessment, so that it is clear which protection is needed. | BIV-Basic | Service | | | 1.1 | |
| Management of | Information | 8.2.2 | | Information labelling - To label | BIV-Basic | Central | | | 1.1 | |

# Baseline Information Security SURF (BIS)



Classification = Click and start typing...

Keywords =

| Chapter | Sub-chapter | ISO 27002 | ID | Control/measure | Classification | Responsible | Procurement? | Explanation | Version | Keywords |
|---|---|---|---|---|---|---|---|---|---|---|
| Management of company resources | Information classification | 8.2.1 | 8.2.1.1 | The information in all Information Systems is classified through an explicit risk assessment, so that it is clear which protection is needed. | CIA Basic | Service | | | 1.1 | classification |

# Suitability Classification

# Suitability classification

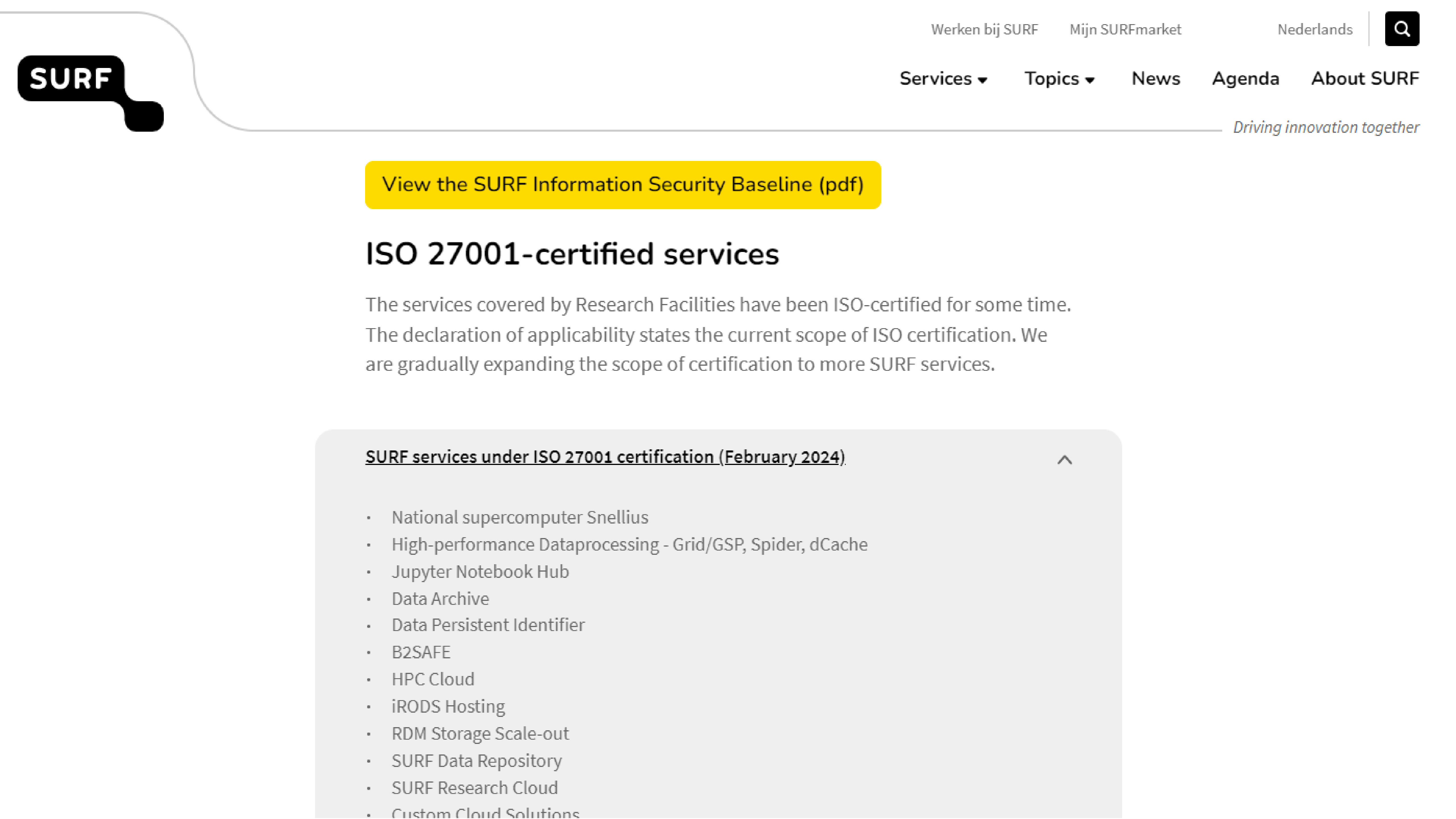
- Is derived from the CIA score, i.e. the level of protection.
- Is a tool for the purchasing institutions.
- We publish the Baseline related to the score, so security professionals can look up what to expect
- All rights reserved (it is an aid, a tool, not a contract).

Designation at SURF service:

*Service X is suitable*
*for data/information with a classification*
*CI: B/H and A: B/H*

*Tip: The lowest protection in a chain usually determines the overall suitability rating.*

# Communication: our website



## ISO 27001-certified services

The services covered by Research Facilities have been ISO-certified for some time. The declaration of applicability states the current scope of ISO certification. We are gradually expanding the scope of certification to more SURF services.

**SURF services under ISO 27001 certification (February 2024)**

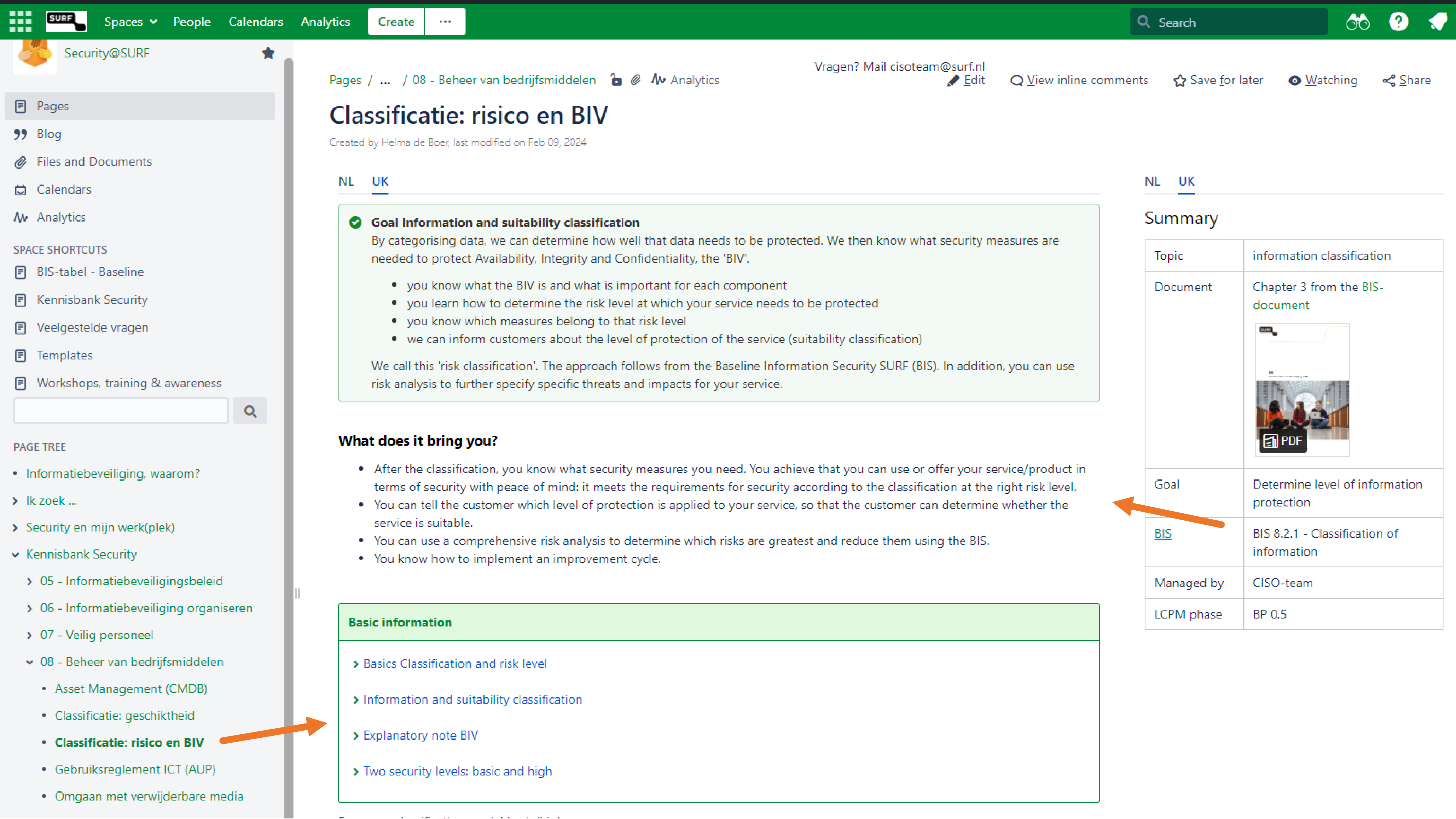
- National supercomputer Snellius
- High-performance Dataprocessing - Grid/GSP, Spider, dCache
- Jupyter Notebook Hub
- Data Archive
- Data Persistent Identifier
- B2SAFE
- HPC Cloud
- iRODS Hosting
- RDM Storage Scale-out
- SURF Data Repository
- SURF Research Cloud
- Custom Cloud Solutions

# New situation website

| **Service** | **ISO 27001 certified?** | **Availability** | **Integrity & confidentiality** |
|---|---|---|---|
| Domeinen | | Basic | Basic |
| SURFcertificaten | ✓ | Basic | Basic |
| SURFsoc | | Basic* | Basic* |
| iRODS Hosting | ✓ | Basic | Basic* |
| RDM Storage Scale-out | ✓ | basic | Basic* |

***** ***Under evaluation for the protection level ‘high; for availability or integrity/confidentiality***

# Tools … making things easier


Spaces
People
Calendars
Analytics
Create
Search
Security@SURF
Pages
Blog
Files and Documents
Calendars
Analytics
SPACE SHORTCUTS
BIS-tabel - Baseline
Kennisbank Security
Veelgestelde vragen
Templates
Workshops, training & awareness
PAGE TREE
Informatiebeveiliging, waarom?
Ik zoek ...
Security en mijn werk(plek)
Kennisbank Security
05 - Informatiebeveiligingsbeleid
06 - Informatiebeveiliging organiseren
07 - Veilig personeel
08 - Beheer van bedrijfsmiddelen
Asset Management (CMDB)
Classificatie: geschiktheid
Classificatie: risico en BIV
Gebruiksreglement ICT (AUP)
Omgaan met verwijderbare media
Pages / ... / 08 - Beheer van bedrijfsmiddelen
Analytics
Vragen? Mail cisoteam@surf.nl
Edit
View inline comments
Save for later
Watching
Share
NL
UK
PDF

# Classificatie: risico en BIV

Created by Helma de Boer, last modified on Feb 09, 2024

NL UK

**Goal Information and suitability classification**

By categorising data, we can determine how well that data needs to be protected. We then know what security measures are needed to protect Availability, Integrity and Confidentiality, the 'BIV'.

- you know what the BIV is and what is important for each component
- you learn how to determine the risk level at which your service needs to be protected
- you know which measures belong to that risk level
- we can inform customers about the level of protection of the service (suitability classification)

We call this 'risk classification'. The approach follows from the Baseline Information Security SURF (BIS). In addition, you can use risk analysis to further specify specific threats and impacts for your service.

### What does it bring you?

- After the classification, you know what security measures you need. You achieve that you can use or offer your service/product in terms of security with peace of mind: it meets the requirements for security according to the classification at the right risk level.
- You can tell the customer which level of protection is applied to your service, so that the customer can determine whether the service is suitable.
- You can use a comprehensive risk analysis to determine which risks are greatest and reduce them using the BIS.
- You know how to implement an improvement cycle.

**Basic information**

› Basics Classification and risk level

› Information and suitability classification

› Explanatory note BIV

› Two security levels: basic and high

NL UK

## Summary

| | |
|---|---|
| Topic | information classification |
| Document | Chapter 3 from the BIS-document |
| Goal | Determine level of information protection |
| BIS | BIS 8.2.1 - Classification of information |
| Managed by | CISO-team |
| LCPM phase | BP 0.5 |

# Information confidentiality labels

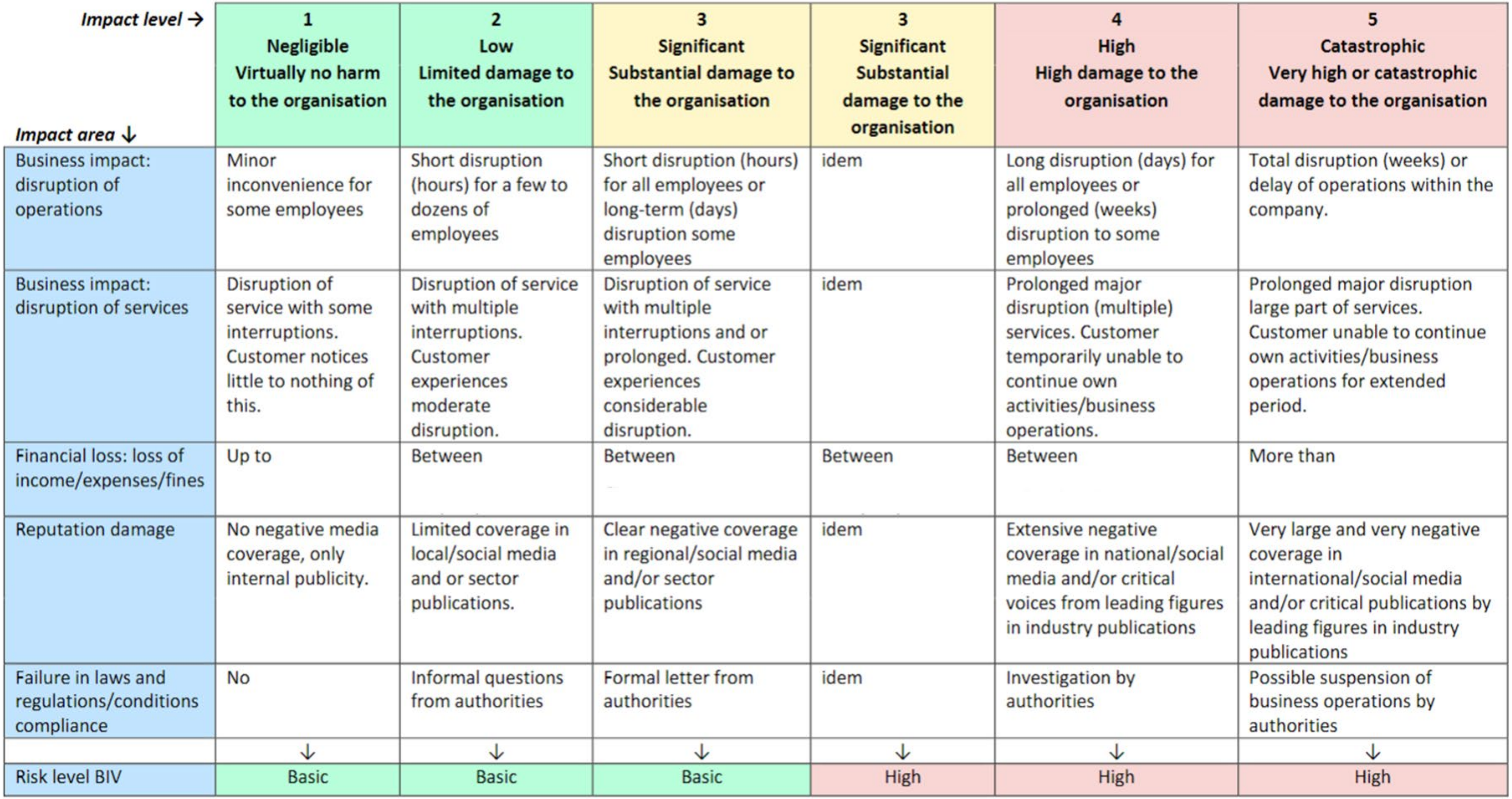
| Which information |
|---|
| Financial data |
| Technical information |
| Personal data |
| Special categories of personal data |
| Strategic information |
| Commercial information |
| Research data |

| Confidentiality (sensitivity) label |
|---|
| Public |
| Internal |
| Confidential |
| Strictly confidential/secret |

*Guideline: the protection level '**Basic**' at SURF is approximately appropriate for information with confidentiality labels 'public', 'internal' and 'confidential'*

*Note: institutions determine this for themselves*

# BIC – Business Impact Criteria



| *Impact level →*<br>*Impact area ↓* | **1**<br>**Negligible**<br>**Virtually no harm to the organisation** | **2**<br>**Low**<br>**Limited damage to the organisation** | **3**<br>**Significant**<br>**Substantial damage to the organisation** | **3**<br>**Significant**<br>**Substantial damage to the organisation** | **4**<br>**High**<br>**High damage to the organisation** | **5**<br>**Catastrophic**<br>**Very high or catastrophic damage to the organisation** |
|---|---|---|---|---|---|---|
| Business impact: disruption of operations | Minor inconvenience for some employees | Short disruption (hours) for a few to dozens of employees | Short disruption (hours) for all employees or long-term (days) disruption some employees | idem | Long disruption (days) for all employees or prolonged (weeks) disruption to some employees | Total disruption (weeks) or delay of operations within the company. |
| Business impact: disruption of services | Disruption of service with some interruptions. Customer notices little to nothing of this. | Disruption of service with multiple interruptions. Customer experiences moderate disruption. | Disruption of service with multiple interruptions and or prolonged. Customer experiences considerable disruption. | idem | Prolonged major disruption (multiple) services. Customer temporarily unable to continue own activities/business operations. | Prolonged major disruption large part of services. Customer unable to continue own activities/business operations for extended period. |
| Financial loss: loss of income/expenses/fines | Up to | Between | Between | Between | Between | More than |
| Reputation damage | No negative media coverage, only internal publicity. | Limited coverage in local/social media and or sector publications. | Clear negative coverage in regional/social media and/or sector publications | idem | Extensive negative coverage in national/social media and/or critical voices from leading figures in industry publications | Very large and very negative coverage in international/social media and/or critical publications by leading figures in industry publications |
| Failure in laws and regulations/conditions compliance | No | Informal questions from authorities | Formal letter from authorities | idem | Investigation by authorities | Possible suspension of business operations by authorities |
| | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ |
| Risk level BIV | Basic | Basic | Basic | High | High | High |

# You express availability in a a percentage. But what exactly does it mean?

| | |
|---|---|
| 99,00 percent | 3,65 days |
| 99,50 percent | 1,83 days |
| 99,80 percent | 17,52 hour |
| 99,90 percent | 8,76 hour |
| 99,99 percent | 52,56 minutes |
| 99,999 percent | 5,26 minutes |
| 99,9999 percent | 31,5 seconds |
| 99,99999 percent | 3,15 seconds |

Availability from 'high' translates at SURF into approximately 99.97 to 99.98 per cent (maximum two hours).

It is important to look at the second decimal place in the procurement agreements/’SLA.

Even though 99.9% seems high, the availability percentage of this level is 'basic'.

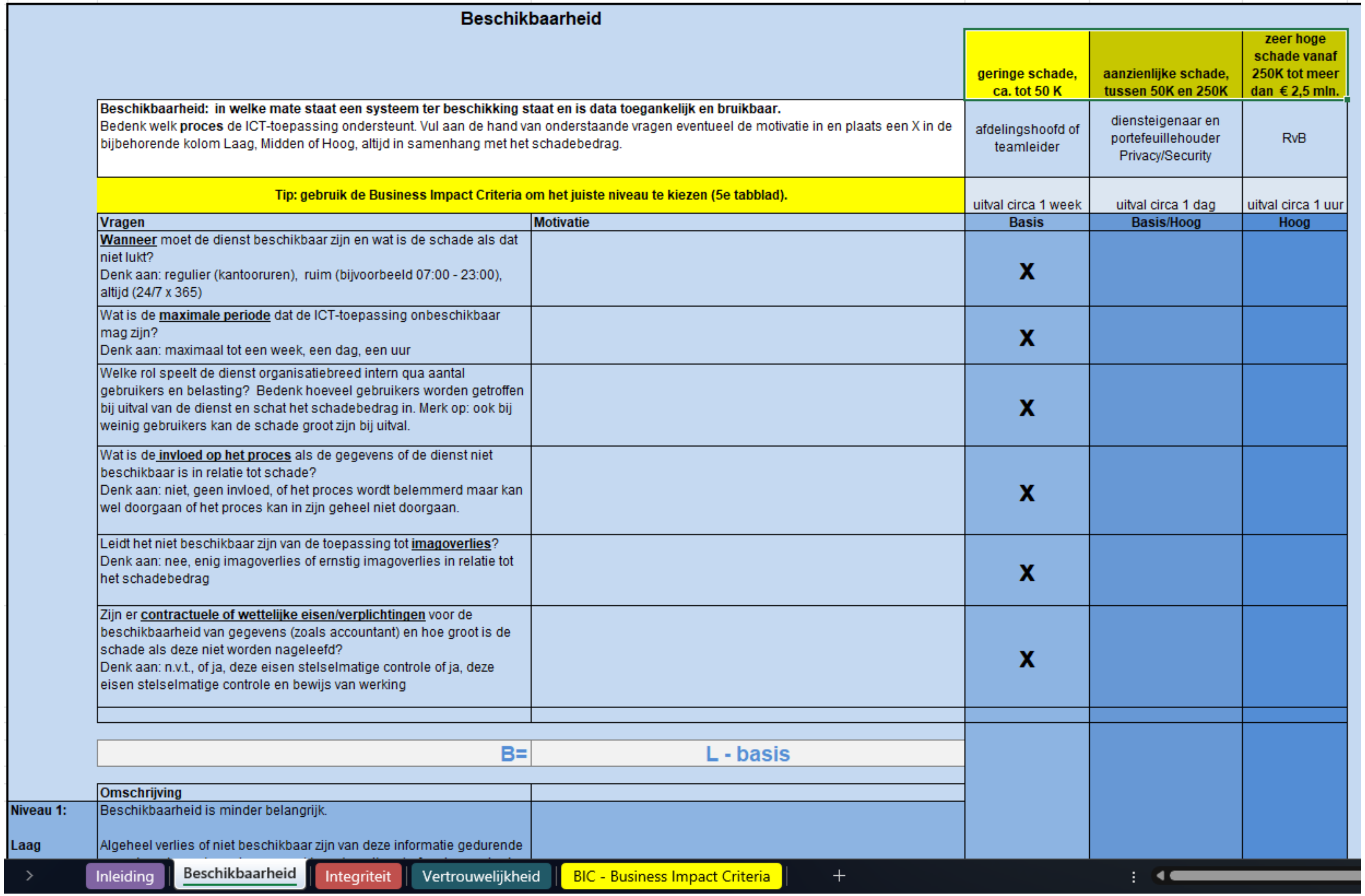
# Tool with CIA classification

## Help questions in Excel

Direct download:

Download dit Excel-template

Dutch only



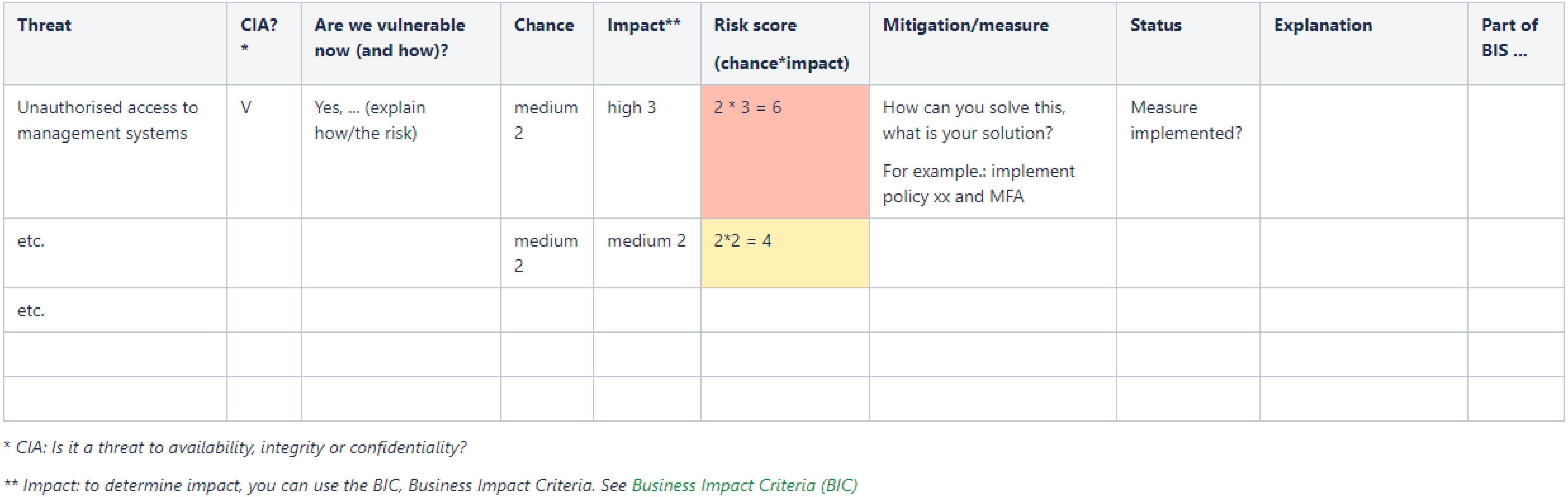
Beschikbaarheid

| | | geringe schade, ca. tot 50 K | aanzienlijke schade, tussen 50K en 250K | zeer hoge schade vanaf 250K tot meer dan € 2,5 mln. |
|---|---|---|---|---|
| **Beschikbaarheid: in welke mate staat een systeem ter beschikking staat en is data toegankelijk en bruikbaar.**<br>Bedenk welk **proces** de ICT-toepassing ondersteunt. Vul aan de hand van onderstaande vragen eventueel de motivatie in en plaats een X in de bijbehorende kolom Laag, Midden of Hoog, altijd in samenhang met het schadebedrag. | | afdelingshoofd of teamleider | diensteigenaar en portefeuillehouder Privacy/Security | RvB |
| **Tip: gebruik de Business Impact Criteria om het juiste niveau te kiezen (5e tabblad).** | | uitval circa 1 week | uitval circa 1 dag | uitval circa 1 uur |
| **Vragen** | **Motivatie** | **Basis** | **Basis/Hoog** | **Hoog** |
| **Wanneer** moet de dienst beschikbaar zijn en wat is de schade als dat niet lukt?<br>Denk aan: regulier (kantooruren), ruim (bijvoorbeeld 07:00 - 23:00), altijd (24/7 x 365) | | **X** | | |
| Wat is de **maximale periode** dat de ICT-toepassing onbeschikbaar mag zijn?<br>Denk aan: maximaal tot een week, een dag, een uur | | **X** | | |
| Welke rol speelt de dienst organisatiebreed intern qua aantal gebruikers en belasting? Bedenk hoeveel gebruikers worden getroffen bij uitval van de dienst en schat het schadebedrag in. Merk op: ook bij weinig gebruikers kan de schade groot zijn bij uitval. | | **X** | | |
| Wat is de **invloed op het proces** als de gegevens of de dienst niet beschikbaar is in relatie tot schade?<br>Denk aan: niet, geen invloed, of het proces wordt belemmerd maar kan wel doorgaan of het proces kan in zijn geheel niet doorgaan. | | **X** | | |
| Leidt het niet beschikbaar zijn van de toepassing tot **imagoverlies**?<br>Denk aan: nee, enig imagoverlies of ernstig imagoverlies in relatie tot het schadebedrag | | **X** | | |
| Zijn er **contractuele of wettelijke eisen/verplichtingen** voor de beschikbaarheid van gegevens (zoals accountant) en hoe groot is de schade als deze niet worden nageleefd?<br>Denk aan: n.v.t., of ja, deze eisen stelselmatige controle of ja, deze eisen stelselmatige controle en bewijs van werking | | **X** | | |
| | | | | |
| **B=** | **L - basis** | | | |

| | Omschrijving | |
|---|---|---|
| **Niveau 1:**<br><br>**Laag** | Beschikbaarheid is minder belangrijk.<br><br>Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende | |

# Risk analysis

1. Copy template + new Confluence page
2. Who takes notes?



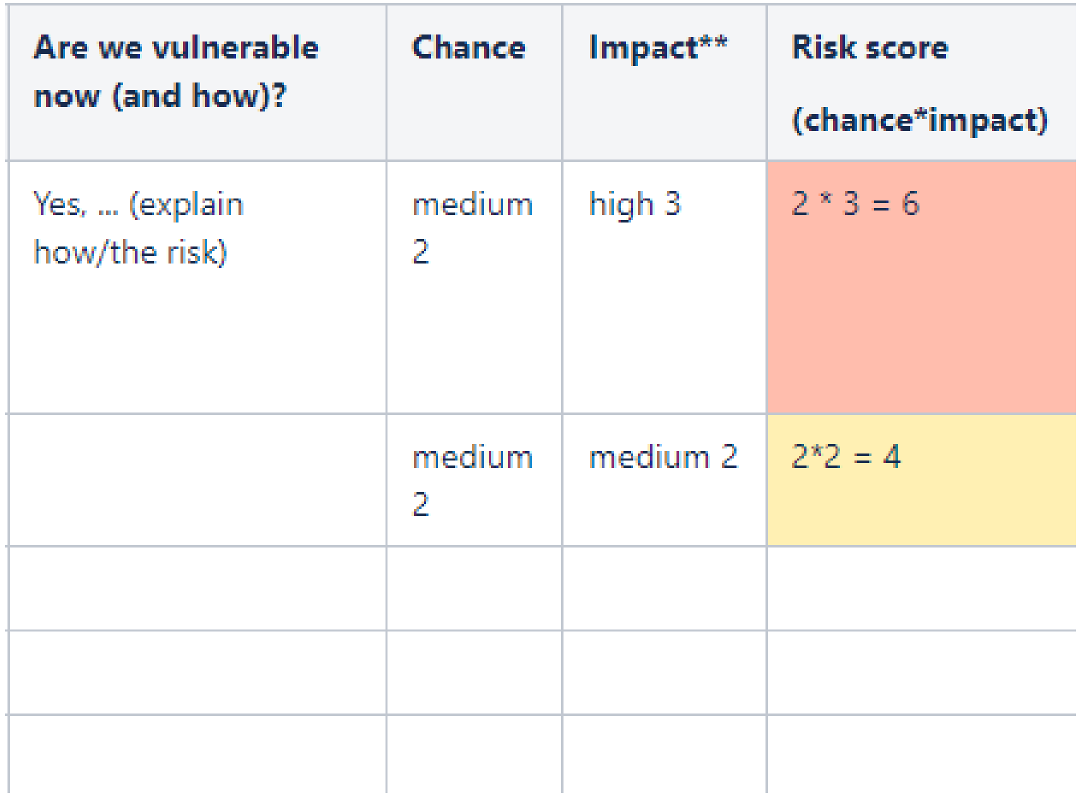
| Threat | CIA? * | Are we vulnerable now (and how)? | Chance | Impact** | Risk score<br>(chance*impact) | Mitigation/measure | Status | Explanation | Part of BIS ... |
|---|---|---|---|---|---|---|---|---|---|
| Unauthorised access to management systems | V | Yes, ... (explain how/the risk) | medium 2 | high 3 | 2 * 3 = 6 | How can you solve this, what is your solution?<br>For example.: implement policy xx and MFA | Measure implemented? | | |
| etc. | | | medium 2 | medium 2 | 2*2 = 4 | | | | |
| etc. | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

** CIA: Is it a threat to availability, integrity or confidentiality?*

*** Impact: to determine impact, you can use the BIC, Business Impact Criteria. See Business Impact Criteria (BIC)*

Hulpmiddel: RAVIB dreigingen

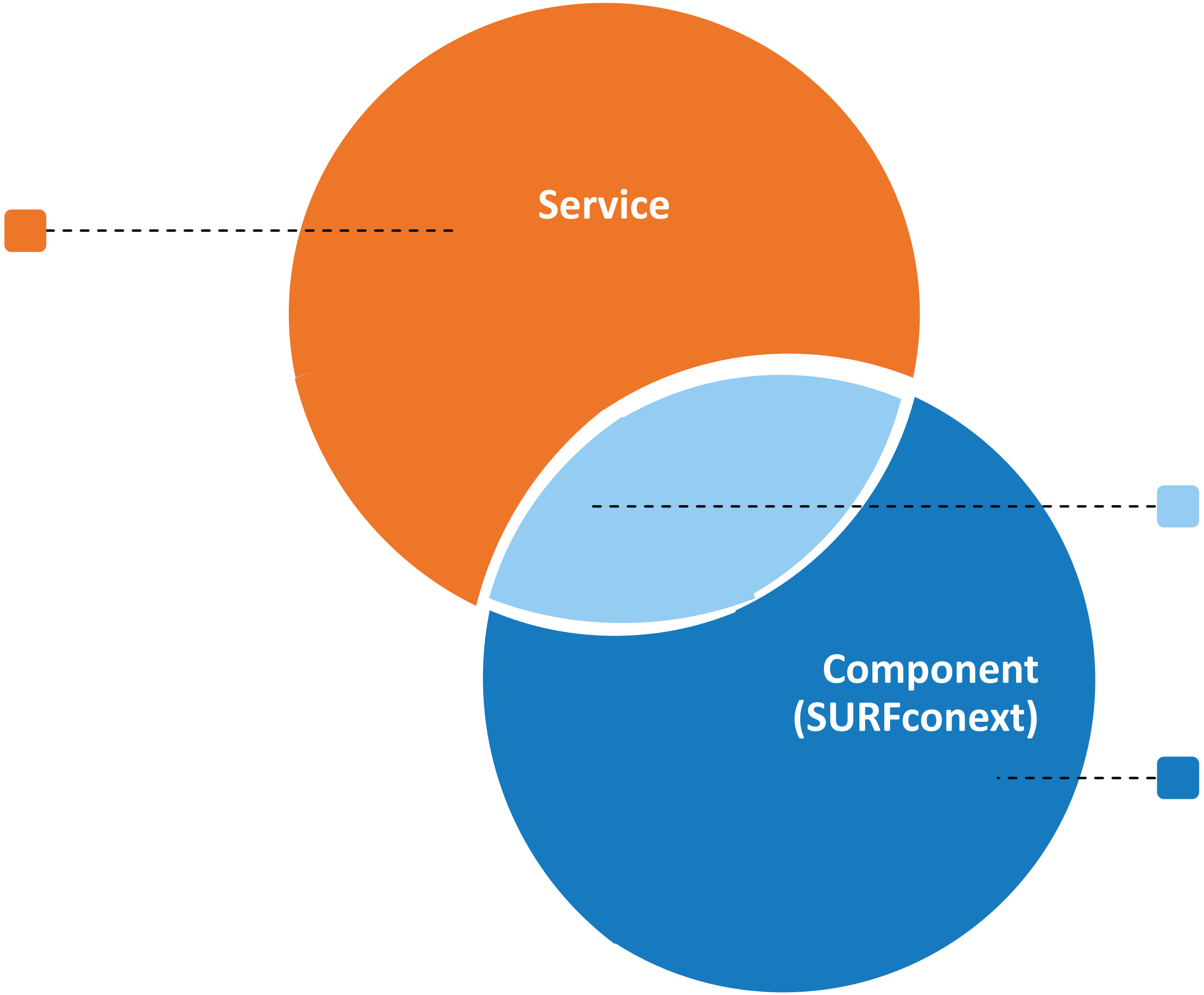
# Kans * Impact = Risicoscore



| Are we vulnerable now (and how)? | Chance | Impact** | Risk score (chance*impact) |
|---|---|---|---|
| Yes, ... (explain how/the risk) | medium 2 | high 3 | 2 * 3 = 6 |
|  | medium 2 | medium 2 | 2*2 = 4 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

| Impact * Kans | 1 | 2 | 3 |
|---|---|---|---|
| 3 | 3 | 6 | 9 |
| 2 | 2 | 4 | 6 |
| 1 | 1 | 2 | 3 |

# Risk ownership in a chain of services



**Basic/High**
Risk owner for this service

**Assess if sufficient**
Must components comply?
Know what to do if they fail
Suppliers is risk owner

**High/High**
“supplier”, risk owner of this service