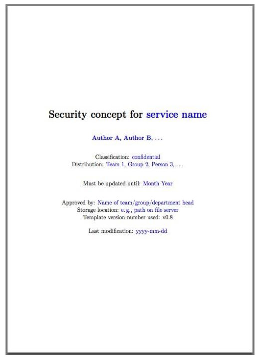
# IT security concept documentation in higher education data centers: A template-based approach


Security concept for service name

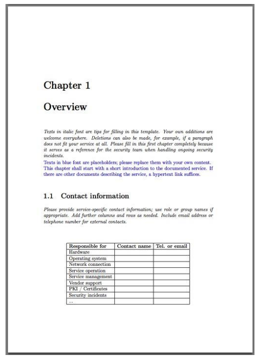
Author A, Author B, . . .

Classification: confidential
Distribution: Team 1, Group 2, Person 3, . . .

Must be updated until: Month Year

Approved by: Name of team/group/department head
Storage location: e. g., path on file server
Template version number used: v0.8

Last modification: yyyy-mm-dd


Chapter 1

Overview

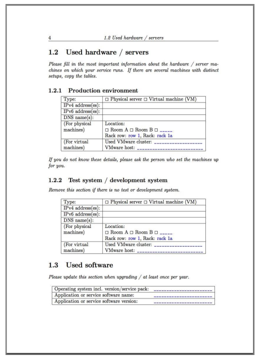
*Texts in italic font are tips for filling in this template. Your own additions are welcome everywhere. Deletions can also be made, for example, if a paragraph does not fit your service at all. Please fill in this first chapter completely because it serves as a reference for the security team when handling ongoing security incidents.*

Texts in blue font are placeholders; please replace them with your own content. This chapter shall start with a short introduction to the documented service. If there are other documents describing the service, a hypertext link suffices.

1.1 Contact information

*Please provide service-specific contact information; use role or group names if appropriate. Add further columns and rows as needed. Include email address or telephone number for external contacts.*

| Responsible for | Contact name | Tel. or email |
|---|---|---|
| Hardware | | |
| Operating system | | |
| Network connection | | |
| Service operation | | |
| Service management | | |
| Vendor support | | |
| PKI / Certificates | | |
| Security incidents | | |
| ... | | |


4 *1.2 Used hardware / servers*

1.2 Used hardware / servers

*Please fill in the most important information about the hardware / server machines on which your service runs. If there are several machines with distinct setups, copy the tables.*

1.2.1 Production environment

| | |
|---|---|
| Type: | □ Physical server □ Virtual machine (VM) |
| IPv4 address(es): | |
| IPv6 address(es): | |
| DNS name(s): | |
| (For physical machines) | Location:<br>□ Room A □ Room B □ _____<br>Rack row: row 1, Rack: rack 1a |
| (For virtual machines) | Used VMware cluster: ____________<br>VMware host: ____________ |

*If you do not know these details, please ask the person who set the machines up for you.*

1.2.2 Test system / development system

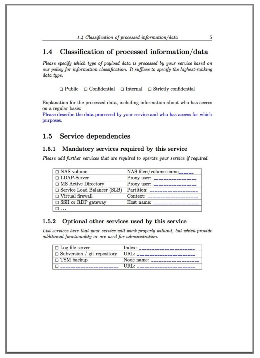
*Remove this section if there is no test or development system.*

| | |
|---|---|
| Type: | □ Physical server □ Virtual machine (VM) |
| IPv4 address(es): | |
| IPv6 address(es): | |
| DNS name(s): | |
| (For physical machines) | Location:<br>□ Room A □ Room B □ _____<br>Rack row: row 1, Rack: rack 1a |
| (For virtual machines) | Used VMware cluster: ____________<br>VMware host: ____________ |

1.3 Used software

*Please update this section when upgrading / at least once per year.*

| | |
|---|---|
| Operating system incl. version/service pack: | ____________ |
| Application or service software name: | ____________ |
| Application or service software version: | ____________ |


*1.4 Classification of processed information/data* 5

1.4 Classification of processed information/data

*Please specify which type of payload data is processed by your service based on our policy for information classification. It suffices to specify the highest-ranking data type.*

□ Public □ Confidential □ Internal □ Strictly confidential

Explanation for the processed data, including information about who has access on a regular basis:
Please describe the data processed by your service and who has access for which purposes.

1.5 Service dependencies

1.5.1 Mandatory services required by this service

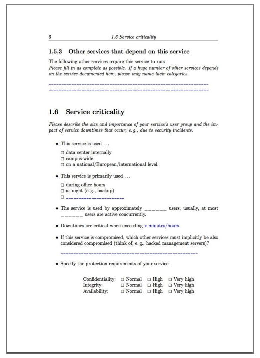
*Please add further services that are required to operate your service if required.*

| | |
|---|---|
| □ NAS volume | NAS filer:/volume-name______ |
| □ LDAP-Server | Proxy user: ____________ |
| □ MS Active Directory | Proxy user: ____________ |
| □ Service Load Balancer (SLB) | Partition: ____________ |
| □ Virtual firewall | Context: ____________ |
| □ SSH or RDP gateway | Host name: ____________ |
| □ . . . | |

1.5.2 Optional other services used by this service

*List services here that your service will work properly without, but which provide additional functionality or are used for administration.*

| | |
|---|---|
| □ Log file server | Index: ____________ |
| □ Subversion / git repository | URL: ____________ |
| □ TSM backup | Node name: ____________ |
| □ ____________ | URL: ____________ |


6 *1.6 Service criticality*

1.5.3 Other services that depend on this service

The following other services require this service to run:
*Please fill in as complete as possible. If a huge number of other services depends on the service documented here, please only name their categories.*

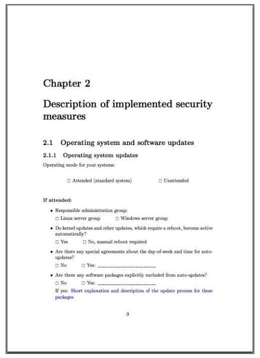
____________________________________________
____________________________________________

1.6 Service criticality

*Please describe the size and importance of your service's user group and the impact of service downtimes that occur, e. g., due to security incidents.*

- This service is used . . .
  □ data center internally
  □ campus-wide
  □ on a national/European/international level.
- This service is primarily used . . .
  □ during office hours
  □ at night (e. g., backup)
  □ ____________
- The service is used by approximately ______ users; usually, at most ______ users are active concurrently.
- Downtimes are critical when exceeding x minutes/hours.
- If this service is compromised, which other services must implicitly be also considered compromised (think of, e. g., hacked management servers)?
  ____________________________________
- Specify the protection requirements of your service:

| | | | |
|---|---|---|---|
| Confidentiality: | □ Normal | □ High | □ Very high |
| Integrity: | □ Normal | □ High | □ Very high |
| Availability: | □ Normal | □ High | □ Very high |


Chapter 2

Description of implemented security measures

2.1 Operating system and software updates

2.1.1 Operating system updates

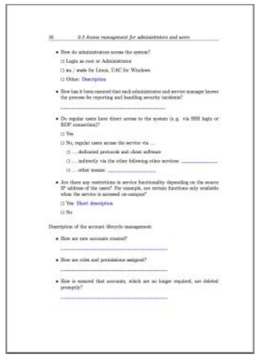
Operating mode for your systems:

□ Attended (standard system) □ Unattended

**If attended:**

- Responsible administration group:
  □ Linux server group □ Windows server group
- Do kernel updates and other updates, which require a reboot, become active automatically?
  □ Yes □ No, manual reboot required
- Are there any special agreements about the day-of-week and time for auto-updates?
  □ No □ Yes: ____________
- Are there any software packages explicitly excluded from auto-updates?
  □ No □ Yes: ____________
  If yes: Short explanation and description of the update process for these packages

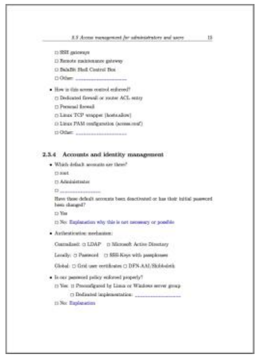
9


16 *2.3 Access management for administrators and users*

- How do administrators access the system?
  □ Login as root or Administrator
  □ su / sudo for Linux, UAC for Windows
  □ Other: Description
- How has it been ensured that each administrator and service manager knows the process for reporting and handling security incidents?
  ____________________________________
- Do regular users have direct access to the system (e. g. via SSH login or RDP connection)?
  □ Yes
  □ No, regular users access the service via . . .
    □ . . . dedicated protocols and client software
    □ . . . indirectly via the other following other services: ____________
    □ . . . other means: ____________
- Are there any restrictions in service functionality depending on the source IP address of the users? For example, are certain functions only available when the service is accessed on-campus?
  □ Yes: Short description
  □ No

Description of the account lifecycle management:

- How are new accounts created?
  ____________________________________
- How are roles and permissions assigned?
  ____________________________________
- How is ensured that accounts, which are no longer required, are deleted promptly?
  ____________________________________

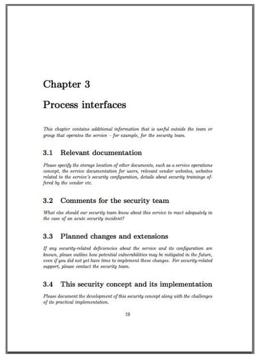

*2.3 Access management for administrators and users* 15

□ SSH gateways
□ Remote maintenance gateway
□ BalaBit Shell Control Box
□ Other: ____________

- How is this access control enforced?
  □ Dedicated firewall or router ACL entry
  □ Personal firewall
  □ Linux TCP wrapper (hosts.allow)
  □ Linux PAM configuration (access.conf)
  □ Other: ____________

2.3.4 Accounts and identity management

- Which default accounts are there?
  □ root
  □ Administrator
  □ ____________
  Have these default accounts been deactivated or has their initial password been changed?
  □ Yes
  □ No: Explanation why this is not necessary or possible
- Authentication mechanism:
  Centralized: □ LDAP □ Microsoft Active Directory
  Locally: □ Password □ SSH-Keys with passphrases
  Global: □ Grid user certificates □ DFN-AAI/Shibboleth
- Is our password policy enforced properly?
  □ Yes: □ Preconfigured by Linux or Windows server group
  □ Dedicated implementation: ____________
  □ No: Explanation


Chapter 3

Process interfaces

*This chapter contains additional information that is useful outside the team or group that operates the service – for example, for the security team.*

3.1 Relevant documentation

*Please specify the storage location of other documents, such as a service operations concept, the service documentation for users, relevant vendor websites, websites related to the service's security configuration, details about security trainings offered by the vendor etc.*

3.2 Comments for the security team

*What else should our security team know about this service to react adequately in the case of an acute security incident?*

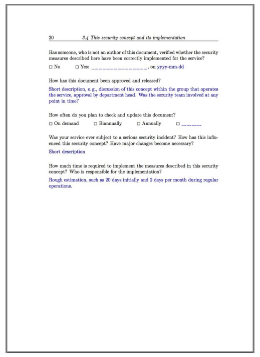
3.3 Planned changes and extensions

*If any security-related deficiencies about the service and its configuration are known, please outline how potential vulnerabilities may be mitigated in the future, even if you did not yet have time to implement these changes. For security-related support, please contact the security team.*

3.4 This security concept and its implementation

*Please document the development of this security concept along with the challenges of its practical implementation.*

19


20 *3.4 This security concept and its implementation*

Has someone, who is not an author of this document, verified whether the security measures described here have been correctly implemented for the service?

□ No □ Yes: ________________, on yyyy-mm-dd

How has this document been approved and released?

Short description, e. g., discussion of this concept within the group that operates the service, approval by department head. Was the security team involved at any point in time?

How often do you plan to check and update this document?

□ On demand □ Biannually □ Annually □ ________

Was your service ever subject to a serious security incident? How has this influenced this security concept? Have major changes become necessary?

Short description

How much time is required to implement the measures described in this security concept? Who is responsible for the implementation?

Rough estimation, such as 20 days initially and 2 days per month during regular operations.

Wolfgang Hommel
Leibniz Supercomputing Centre, Munich, Germany

EUNIS 2013

June 12th, 2013

# Leibniz Supercomputing Centre (LRZ)

Photo: Ernst A. Graf, 2012

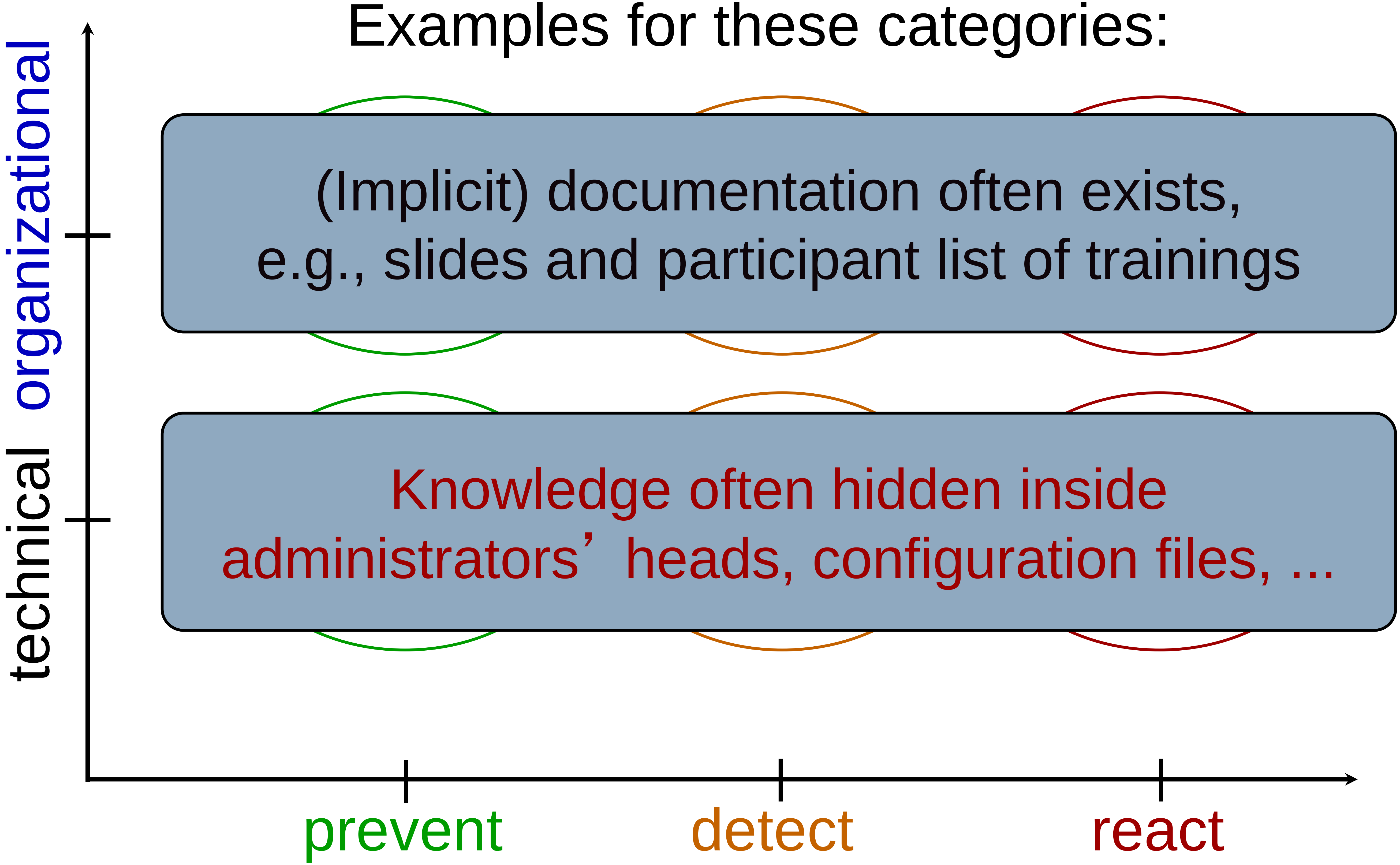
- Data center for all Munich HEIs
  - 130,000+ users
  - Comm. network spawns 550+ buildings
  - 100+ PB file servers/backup/archive
- National HPC center
  - Flagship: SuperMUC, 3 PetaFlop/s
  - Large Linux cluster (9,396 cores)
  - Gauss Computing Centre member

# Overview

- Motivation
  - for security knowledge management
  - for a template-based approach
- The LRZ security concept template
  - Design process
  - Selected content
  - Management workflow
- Ongoing work

# Categories of security controls

Examples for these categories:



organizational

technical

(Implicit) documentation often exists, e.g., slides and participant list of trainings

Knowledge often hidden inside administrators' heads, configuration files, ...

prevent

detect

react

# Documenting security is...

- ... useful for an organization as a whole:
  - Holiday replacements, employee turnover, ...
  - Supports security team in emergency cases
  - Required by industry partners, for certification, ...
  - Demonstrates security knowledge and commitment

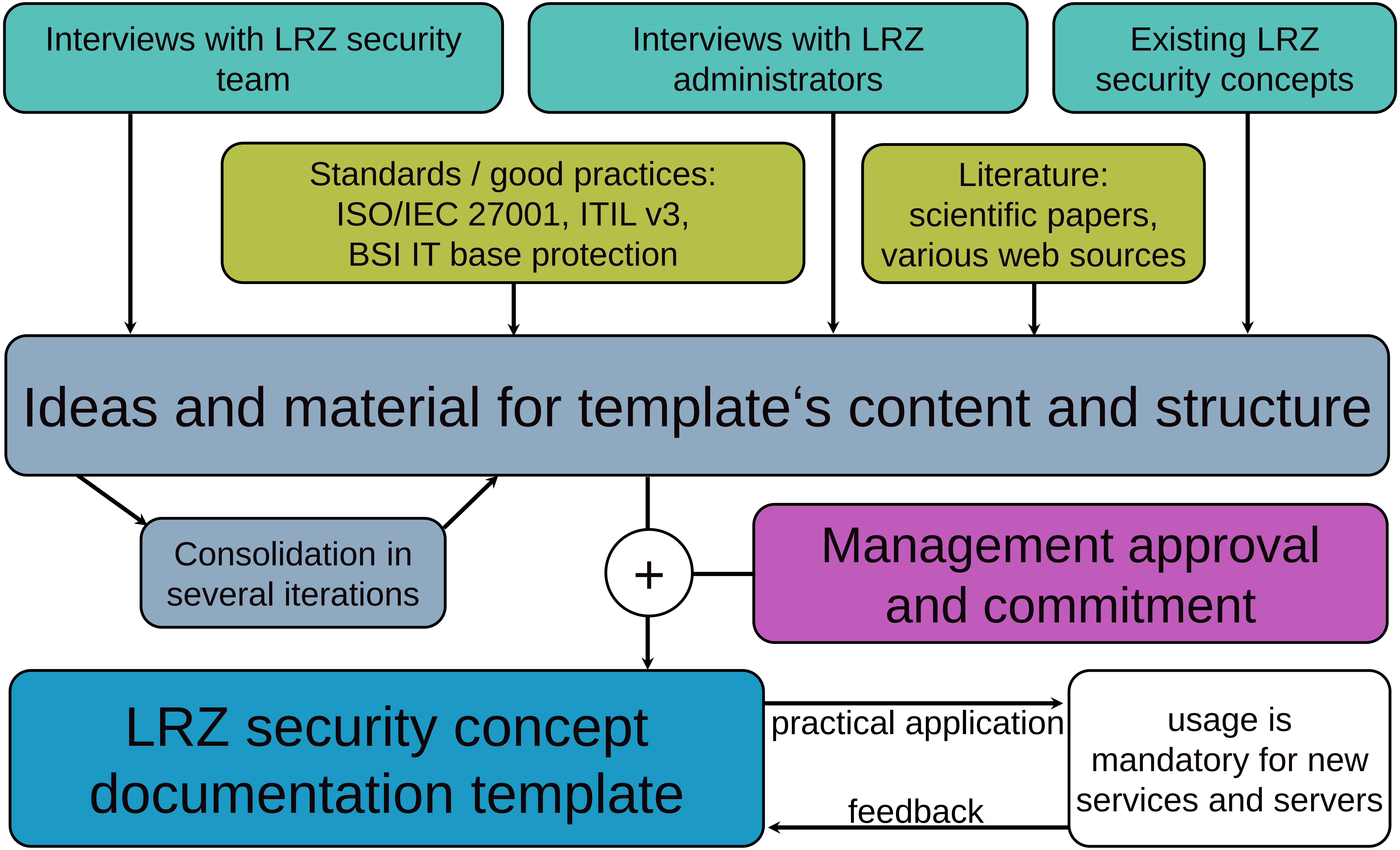
- ... often challenging:
  - Writing documentation is tedious and time-consuming
  - “Where do I start and what do I put in there?”

# A template-based approach

- Desired benefits:
  - Bidirectional knowledge transfer:
    - Make administrators think about security
    - Provide security team with necessary information
  - Efficiency:
    - Reduce the time required to write documentation
    - Uniform structure simplifies information extraction

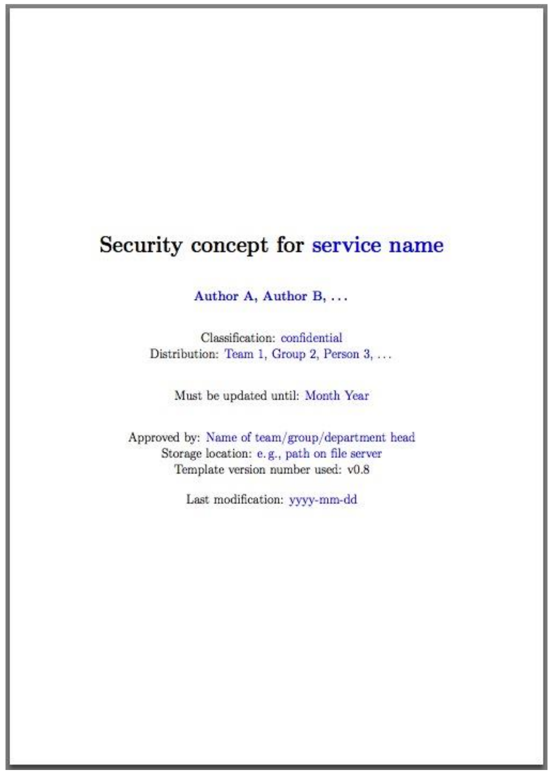
- Risks to be aware of:
  - Documentation is no replacement for security training
  - Generic templates cannot cover service-specific aspects

# How we created the template


Interviews with LRZ security team
Interviews with LRZ administrators
Existing LRZ security concepts
Standards / good practices: ISO/IEC 27001, ITIL v3, BSI IT base protection
Literature: scientific papers, various web sources
Ideas and material for template‘s content and structure
Consolidation in several iterations
+
Management approval and commitment
LRZ security concept documentation template
practical application
feedback
usage is mandatory for new services and servers

# Template content overview

- Document structure:
  - Metadata, introduction
  - Security overview
  - Implemented security controls and their configuration
  - Process interfaces



Security concept for service name

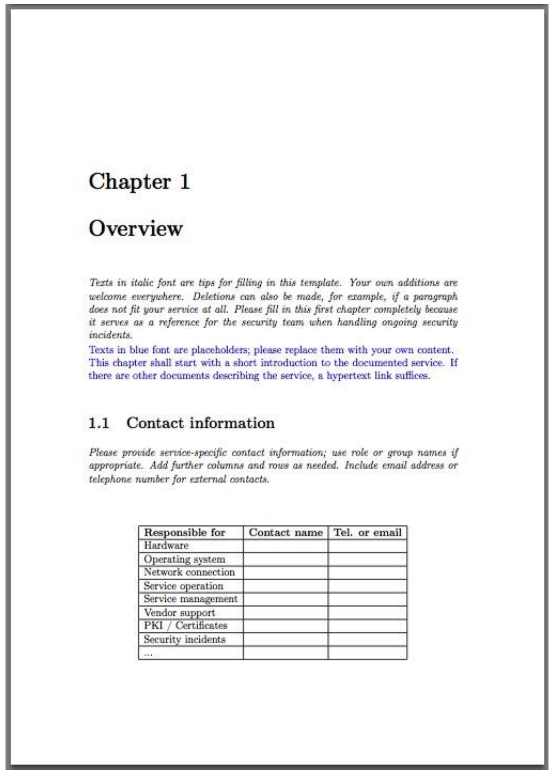
**Author A, Author B, . . .**

Classification: confidential
Distribution: Team 1, Group 2, Person 3, . . .

Must be updated until: Month Year

Approved by: Name of team/group/department head
Storage location: e. g., path on file server
Template version number used: v0.8

Last modification: yyyy-mm-dd



Chapter 1

Overview

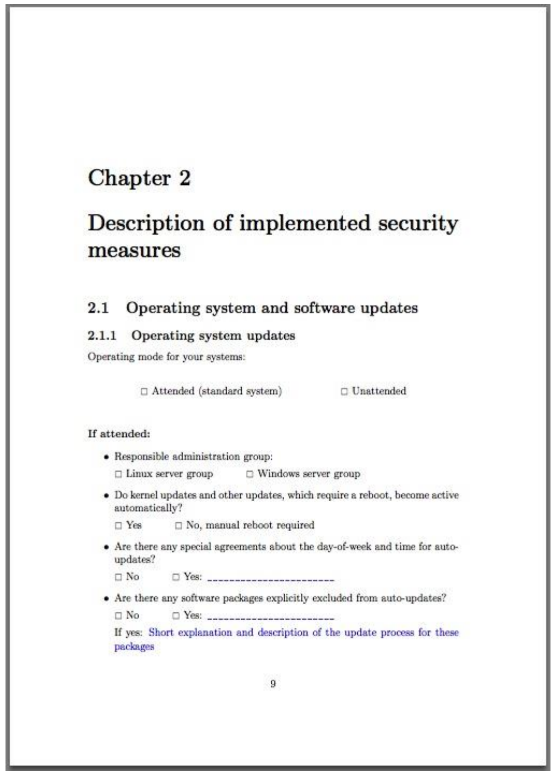
*Texts in italic font are tips for filling in this template. Your own additions are welcome everywhere. Deletions can also be made, for example, if a paragraph does not fit your service at all. Please fill in this first chapter completely because it serves as a reference for the security team when handling ongoing security incidents.*

Texts in blue font are placeholders; please replace them with your own content. This chapter shall start with a short introduction to the documented service. If there are other documents describing the service, a hypertext link suffices.

1.1 Contact information

*Please provide service-specific contact information; use role or group names if appropriate. Add further columns and rows as needed. Include email address or telephone number for external contacts.*

| Responsible for | Contact name | Tel. or email |
|---|---|---|
| Hardware | | |
| Operating system | | |
| Network connection | | |
| Service operation | | |
| Service management | | |
| Vendor support | | |
| PKI / Certificates | | |
| Security incidents | | |
| ... | | |



Chapter 2

Description of implemented security measures

2.1 Operating system and software updates

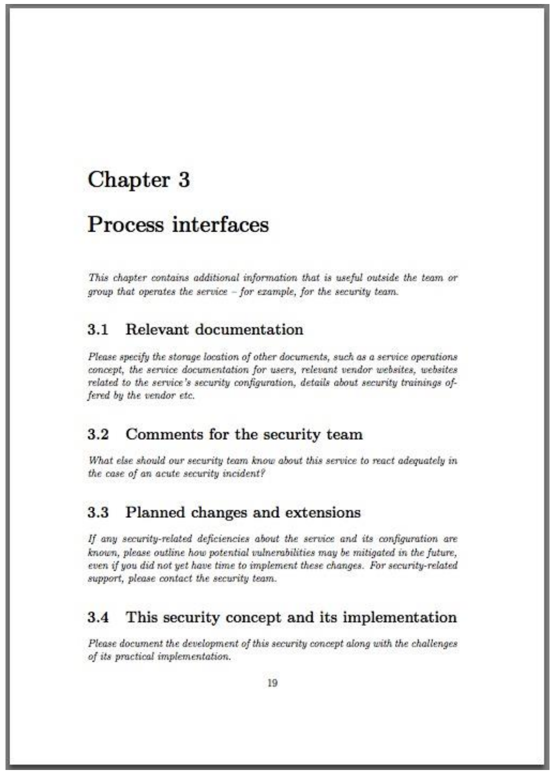
2.1.1 Operating system updates

Operating mode for your systems:

□ Attended (standard system) □ Unattended

**If attended:**

- Responsible administration group:
  □ Linux server group □ Windows server group
- Do kernel updates and other updates, which require a reboot, become active automatically?
  □ Yes □ No, manual reboot required
- Are there any special agreements about the day-of-week and time for auto-updates?
  □ No □ Yes: ______________________
- Are there any software packages explicitly excluded from auto-updates?
  □ No □ Yes: ______________________
  If yes: Short explanation and description of the update process for these packages



Chapter 3

Process interfaces

*This chapter contains additional information that is useful outside the team or group that operates the service – for example, for the security team.*

3.1 Relevant documentation

*Please specify the storage location of other documents, such as a service operations concept, the service documentation for users, relevant vendor websites, websites related to the service's security configuration, details about security trainings offered by the vendor etc.*

3.2 Comments for the security team

*What else should our security team know about this service to react adequately in the case of an acute security incident?*

3.3 Planned changes and extensions

*If any security-related deficiencies about the service and its configuration are known, please outline how potential vulnerabilities may be mitigated in the future, even if you did not yet have time to implement these changes. For security-related support, please contact the security team.*

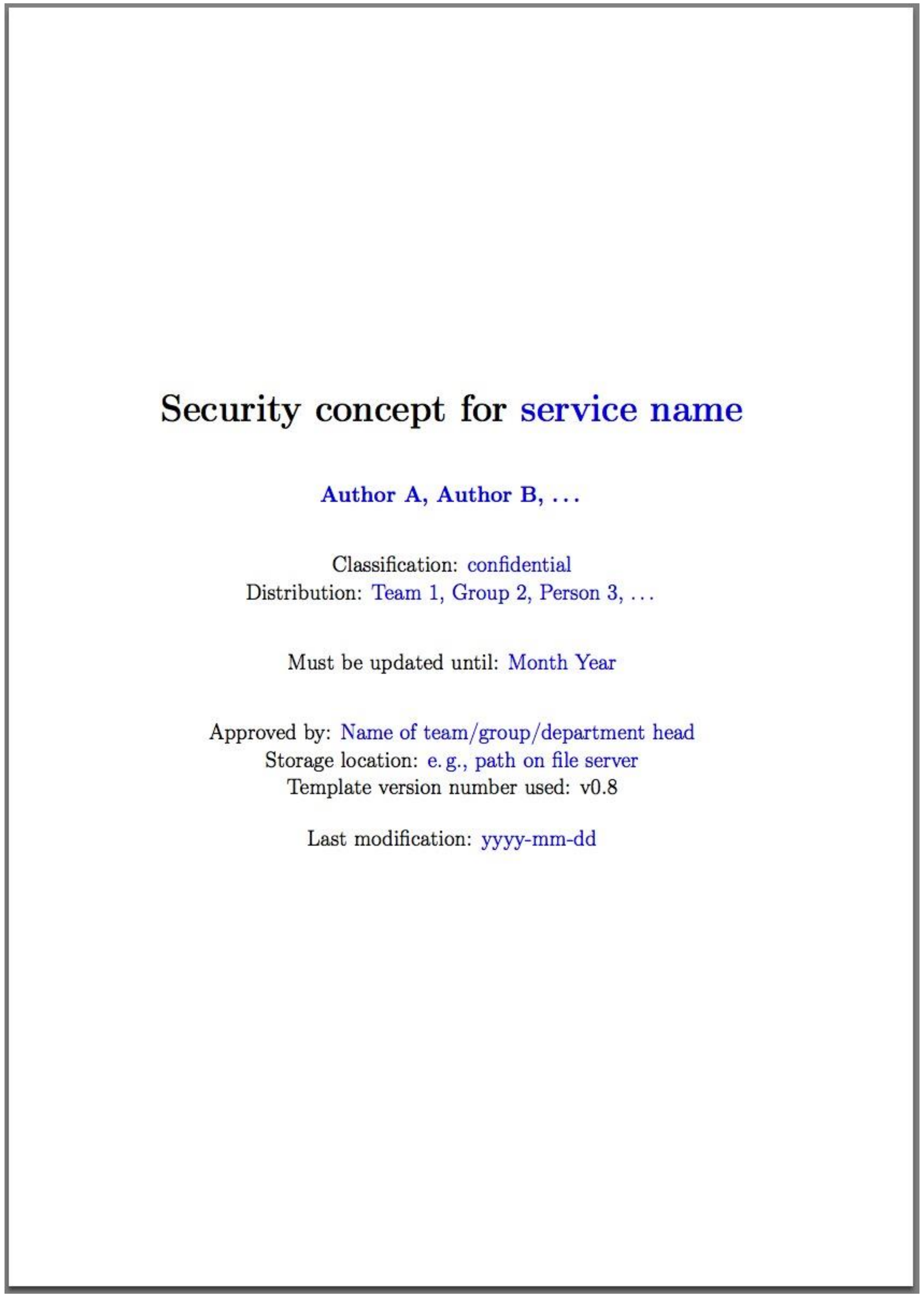
3.4 This security concept and its implementation

*Please document the development of this security concept along with the challenges of its practical implementation.*

**http://git.lrz.de/secdoc**

# Content 1/4: Metadata, introduction

- Document metadata
  - not security-specific
  - author and version information
  - authoritative storage location
- Introduction
  - purpose of the template
  - typographic conventions
  - where to extend,  
    what to skip eventually



Security concept for service name

Author A, Author B, . . .

Classification: confidential  
Distribution: Team 1, Group 2, Person 3, . . .

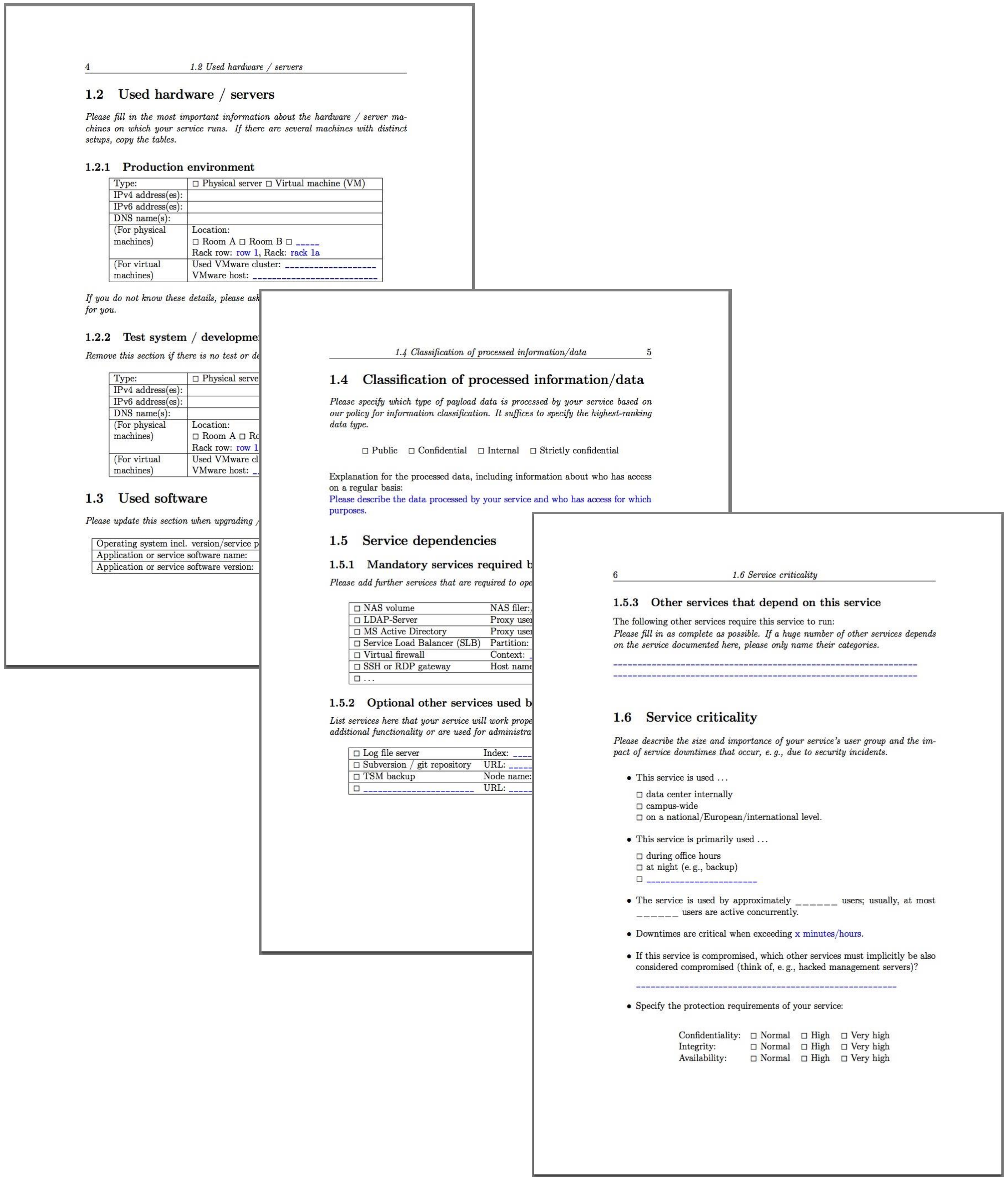
Must be updated until: Month Year

Approved by: Name of team/group/department head  
Storage location: e. g., path on file server  
Template version number used: v0.8

Last modification: yyyy-mm-dd

# Content 2/4: Security overview

- Service description
- Contact information
- Server information
- Software details
- Data classification
- Service dependencies
- Service criticality and usage
- Service-specific risks



4 *1.2 Used hardware / servers*

### 1.2 Used hardware / servers

*Please fill in the most important information about the hardware / server machines on which your service runs. If there are several machines with distinct setups, copy the tables.*

#### 1.2.1 Production environment

| | |
|---|---|
| Type: | □ Physical server □ Virtual machine (VM) |
| IPv4 address(es): | |
| IPv6 address(es): | |
| DNS name(s): | |
| (For physical machines) | Location:<br>□ Room A □ Room B □ _____<br>Rack row: row 1, Rack: rack 1a |
| (For virtual machines) | Used VMware cluster: __________________<br>VMware host: ________________________ |

*If you do not know these details, please ask*
*for you.*

#### 1.2.2 Test system / developme

*Remove this section if there is no test or de*

| | |
|---|---|
| Type: | □ Physical serve |
| IPv4 address(es): | |
| IPv6 address(es): | |
| DNS name(s): | |
| (For physical machines) | Location:<br>□ Room A □ Ro<br>Rack row: row 1 |
| (For virtual machines) | Used VMware cl<br>VMware host: _ |

### 1.3 Used software

*Please update this section when upgrading /*

| |
|---|
| Operating system incl. version/service p |
| Application or service software name: |
| Application or service software version: |

*1.4 Classification of processed information/data* 5

### 1.4 Classification of processed information/data

*Please specify which type of payload data is processed by your service based on our policy for information classification. It suffices to specify the highest-ranking data type.*

□ Public □ Confidential □ Internal □ Strictly confidential

Explanation for the processed data, including information about who has access on a regular basis:
Please describe the data processed by your service and who has access for which purposes.

### 1.5 Service dependencies

#### 1.5.1 Mandatory services required b

*Please add further services that are required to ope*

| | |
|---|---|
| □ NAS volume | NAS filer: |
| □ LDAP-Server | Proxy user |
| □ MS Active Directory | Proxy user |
| □ Service Load Balancer (SLB) | Partition: |
| □ Virtual firewall | Context: _ |
| □ SSH or RDP gateway | Host name |
| □ . . . | |

#### 1.5.2 Optional other services used b

*List services here that your service will work prope*
*additional functionality or are used for administra*

| | |
|---|---|
| □ Log file server | Index: ____ |
| □ Subversion / git repository | URL: _____ |
| □ TSM backup | Node name: |
| □ ______________________ | URL: _____ |

6 *1.6 Service criticality*

#### 1.5.3 Other services that depend on this service

The following other services require this service to run:
*Please fill in as complete as possible. If a huge number of other services depends on the service documented here, please only name their categories.*

______________________________________________________
______________________________________________________

### 1.6 Service criticality

*Please describe the size and importance of your service's user group and the impact of service downtimes that occur, e. g., due to security incidents.*

- This service is used . . .

  □ data center internally
  □ campus-wide
  □ on a national/European/international level.

- This service is primarily used . . .

  □ during office hours
  □ at night (e. g., backup)
  □ ______________________

- The service is used by approximately ______ users; usually, at most ______ users are active concurrently.
- Downtimes are critical when exceeding x minutes/hours.
- If this service is compromised, which other services must implicitly be also considered compromised (think of, e. g., hacked management servers)?

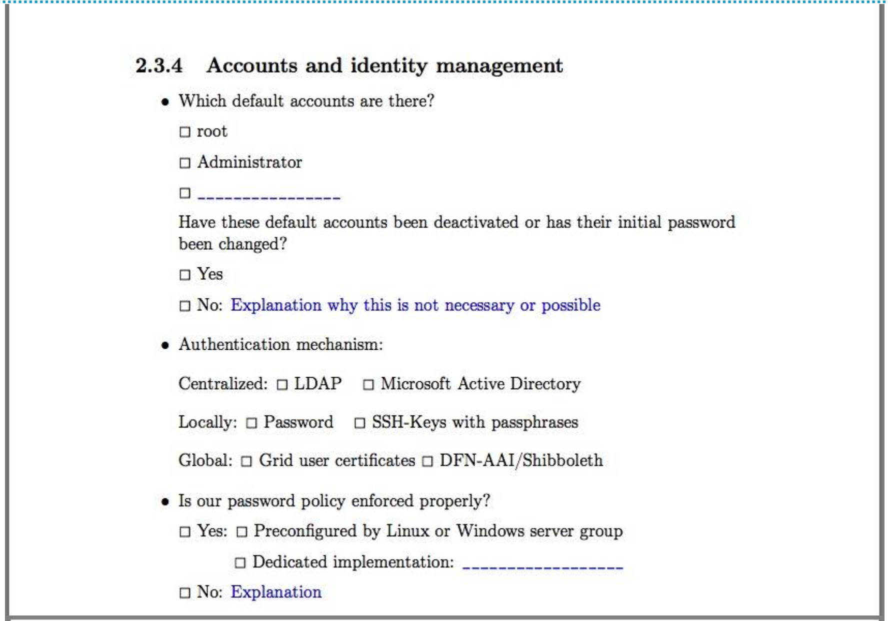
  ______________________________________________________

- Specify the protection requirements of your service:

| | | | |
|---|---|---|---|
| Confidentiality: | □ Normal | □ High | □ Very high |
| Integrity: | □ Normal | □ High | □ Very high |
| Availability: | □ Normal | □ High | □ Very high |

# Content 3/4: Security controls

- Software updates (OS/service)
- Dedicated security software, e.g.
  - anti-virus / anti-malware
  - denial of service countermeasure
- Identity & access management
- Network security, e.g., firewall
- Data availability and privacy, e.g.
  - backup and recovery plan
  - log file management



**2.3.4 Accounts and identity management**

- Which default accounts are there?

  □ root

  □ Administrator

  □ ________________

  Have these default accounts been deactivated or has their initial password been changed?

  □ Yes

  □ No: Explanation why this is not necessary or possible

- Authentication mechanism:

  Centralized: □ LDAP □ Microsoft Active Directory

  Locally: □ Password □ SSH-Keys with passphrases

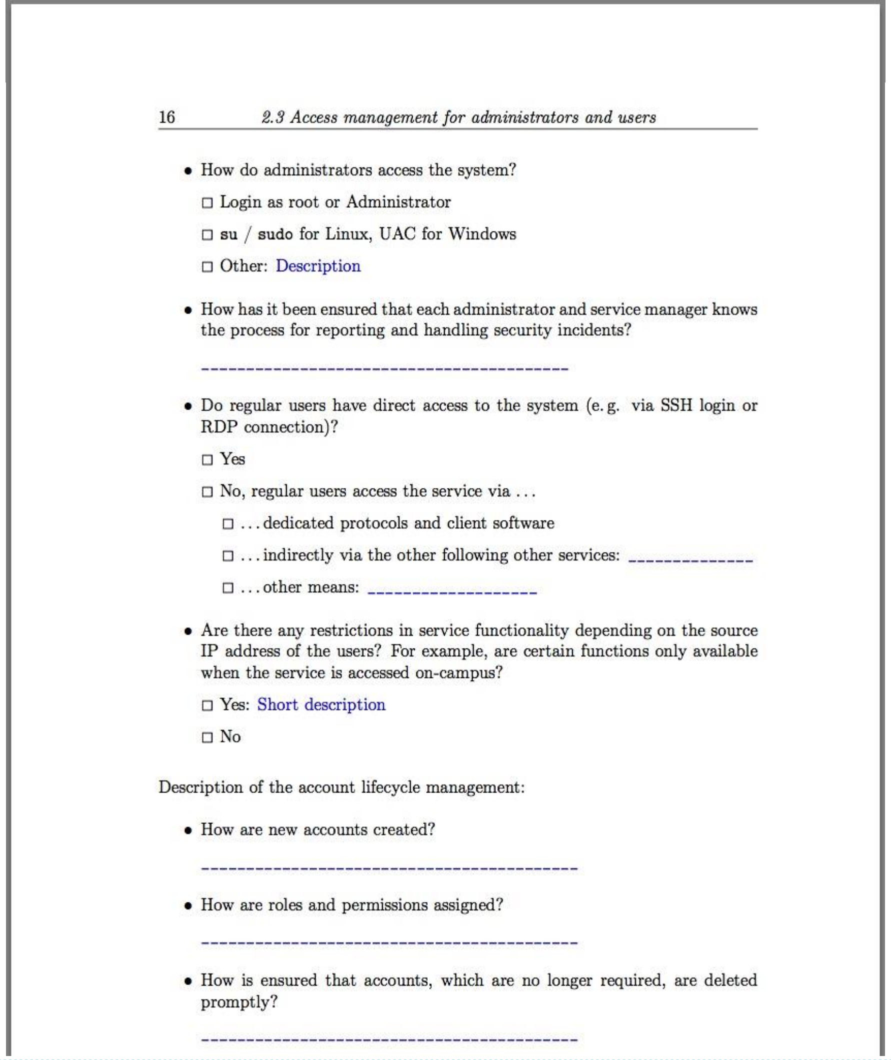
  Global: □ Grid user certificates □ DFN-AAI/Shibboleth

- Is our password policy enforced properly?

  □ Yes: □ Preconfigured by Linux or Windows server group

  □ Dedicated implementation: __________________

  □ No: Explanation



16 *2.3 Access management for administrators and users*

- How do administrators access the system?

  □ Login as root or Administrator

  □ **su** / **sudo** for Linux, UAC for Windows

  □ Other: Description

- How has it been ensured that each administrator and service manager knows the process for reporting and handling security incidents?

  ________________________________________

- Do regular users have direct access to the system (e. g. via SSH login or RDP connection)?

  □ Yes

  □ No, regular users access the service via …

  □ … dedicated protocols and client software

  □ … indirectly via the other following other services: ______________

  □ … other means: ___________________

- Are there any restrictions in service functionality depending on the source IP address of the users? For example, are certain functions only available when the service is accessed on-campus?

  □ Yes: Short description

  □ No

Description of the account lifecycle management:

- How are new accounts created?

  ________________________________________

- How are roles and permissions assigned?

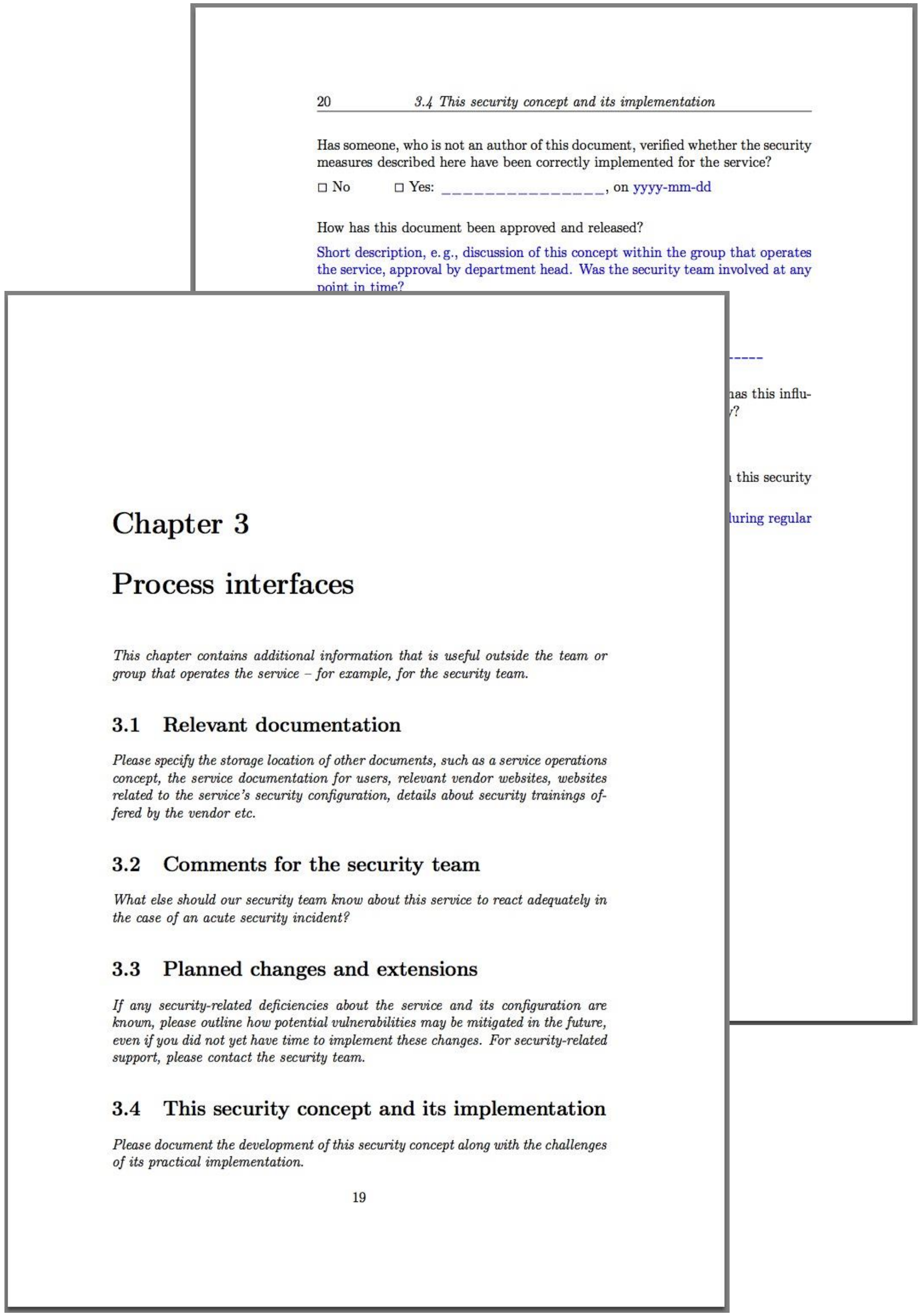
  ________________________________________

- How is ensured that accounts, which are no longer required, are deleted promptly?

  ________________________________________

# Content 4/4: Process interfaces

- Further information:
  - Related documents and relevant web links
  - Do’s and Don’ts for the security team
- Continuous improvement:
  - Past security incidents
  - Known weaknesses
  - Planned improvements
- Implementation:
  - Responsibilities
  - Required effort



20 *3.4 This security concept and its implementation*

Has someone, who is not an author of this document, verified whether the security measures described here have been correctly implemented for the service?

□ No □ Yes: ________________, on yyyy-mm-dd

How has this document been approved and released?

Short description, e. g., discussion of this concept within the group that operates the service, approval by department head. Was the security team involved at any point in time?

-----

has this influ-
?

this security

luring regular

Chapter 3

### Process interfaces

*This chapter contains additional information that is useful outside the team or group that operates the service – for example, for the security team.*

#### 3.1 Relevant documentation

*Please specify the storage location of other documents, such as a service operations concept, the service documentation for users, relevant vendor websites, websites related to the service's security configuration, details about security trainings offered by the vendor etc.*

#### 3.2 Comments for the security team

*What else should our security team know about this service to react adequately in the case of an acute security incident?*

#### 3.3 Planned changes and extensions

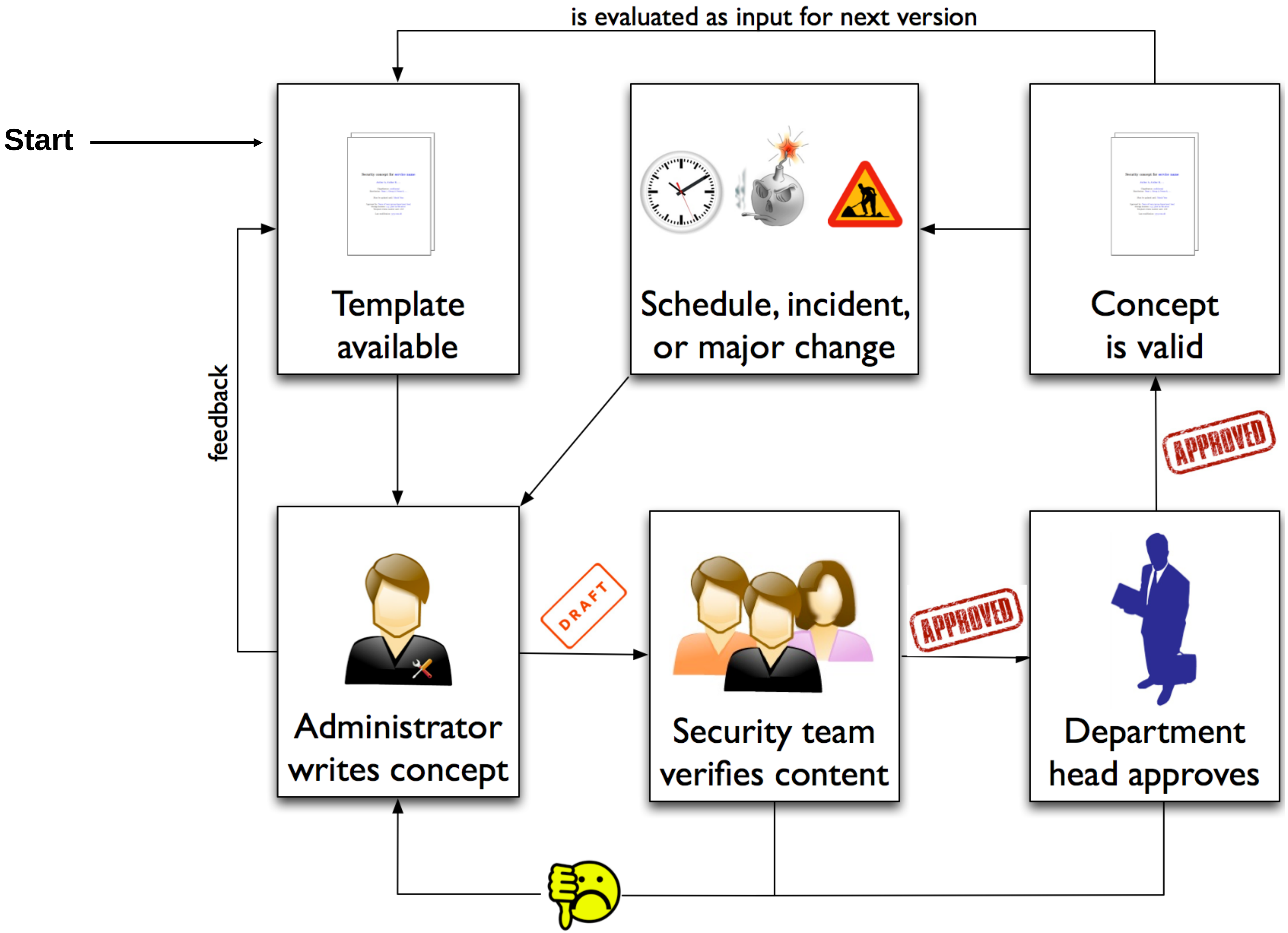
*If any security-related deficiencies about the service and its configuration are known, please outline how potential vulnerabilities may be mitigated in the future, even if you did not yet have time to implement these changes. For security-related support, please contact the security team.*

#### 3.4 This security concept and its implementation

*Please document the development of this security concept along with the challenges of its practical implementation.*

19

# Management workflow



Start

Template available

Schedule, incident, or major change

Concept is valid

Administrator writes concept

Security team verifies content

Department head approves

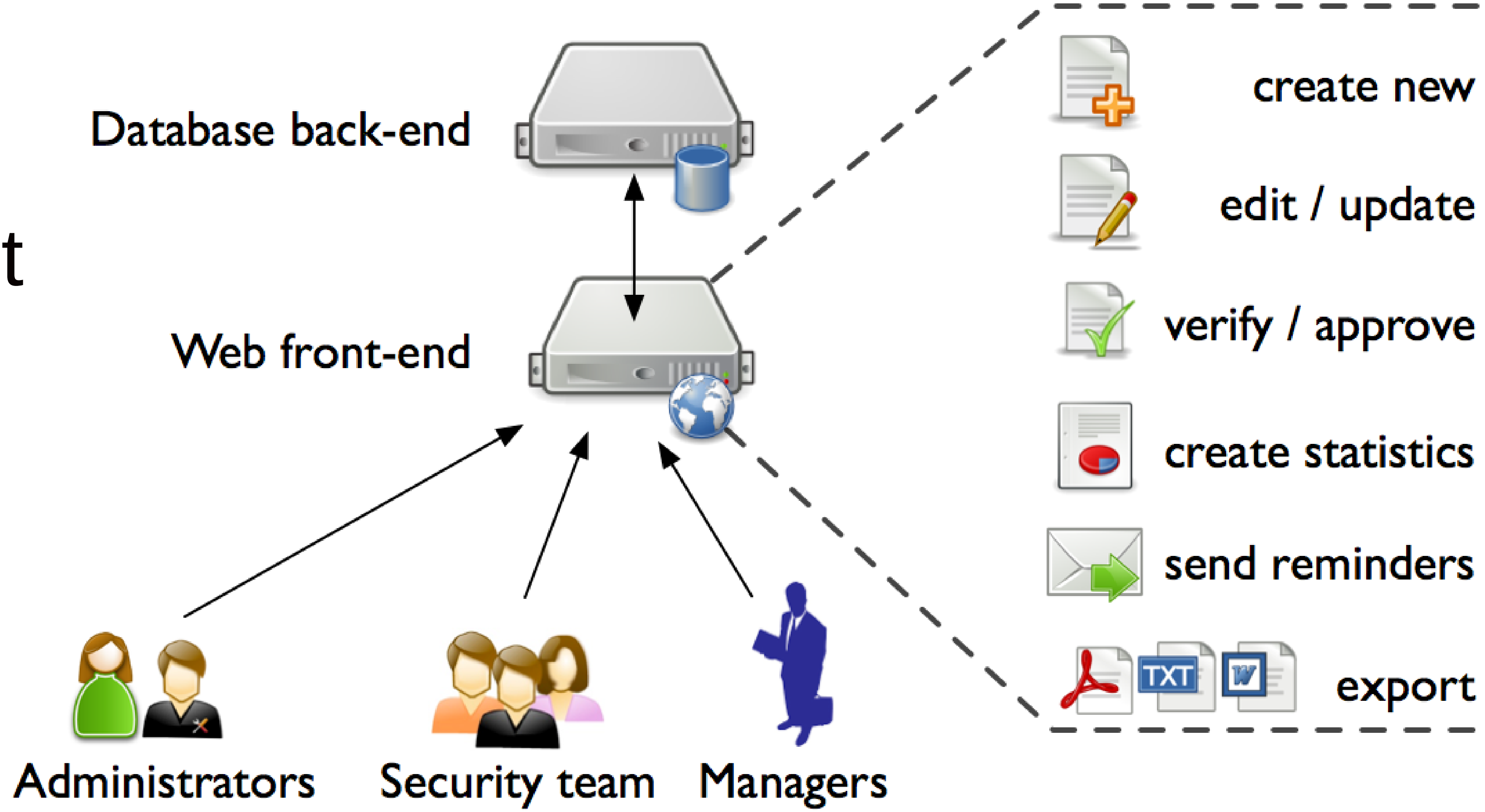
is evaluated as input for next version

feedback

# Ongoing work

- Web application
  - Central storage
  - Workflow support
  - Dynamic forms
  - Statistics
  - Export in various
    - formats
    - details

      (enable optional inter-organizational sharing)



- Discussion in regional and national working groups
- Continuous improvement based on feedback

# Conclusion

- Our security concept template is...
  - ... small but nice for security knowledge management.
  - ... by no means exhaustive, but a good start.

- PDF available at `http://git.lrz.de/secdoc`
- Web application will be released as open source

- We welcome any feedback! `secdoc@lrz.de`
  - How to make the template more intuitive the use?
  - Which additional topics should be covered?
  - Do you use a fundamentally better/different approach?