

Systementwicklung für ein Entwicklungsland

Requirements

Version: 2.0

Supervisors:

Prof. Dr. Nazir Peroz

Daniel Tippmann

Jelisaweta Kamm

Team Analysis:

Raphael Arce

Cristofer Soler

Armine Mikaelyan

Majd Hasan

Ali Agbaria

Charlie Krüger

Osama Bekfani

December 11, 2017

Contents

1. Introduction	4
2. Main Objectives	6
2.1. Overview	6
2.2. Wiki	6
2.2.1. Links	7
2.2.2. News	7
2.2.3. BSI Catalogue	8
2.2.4. Archive	9
2.2.5. Updating the BSI Catalogue	9
2.2.6. User Types	10
2.3. Text Search	12
2.4. Wizard	12
2.5. Home Page	12
2.6. Top Section	13
3. Secondary Objectives	14
3.1. API for BSI Catalog - Priority: LOW	14
3.2. FAQ - Priority: MEDIUM	14
3.3. Discussion pages - Priority: MEDIUM	14
3.3.1. Definition	14
3.3.2. Benefits	15
3.3.3. Types of discussion pages	16
3.4. Information page - Priority: MEDIUM	16
3.5. Report a Mistake - Priority: MEDIUM	17
3.6. Labels - Priority: HIGH	17
3.7. Up/Down Votes - Priority: MEDIUM	18
3.8. Reputation Points (Karma Points) - Priority: MEDIUM	19
3.9. User Access to BSI Catalogue Pages - Priority: HIGH	20
3.10. Automatically created best 10 Suggestions when linking to BSI - Priority: LOW	20
3.11. Extended Wizard (Work in Progress) - Priority: LOW	20
A. Glossar	21
B. Use Case Diagrams	22

C. BSI Pages **27**

C.1. Structure of BSI Pages 27

C.2. Linking to BSI Pages 27

1. Introduction

The requirements document contains all mandatory requirements of the platform. They define the framework conditions and main goals we strive to achieve. Their core are functional and non-functional requirements, as well as a sketch of the overall system design. The draft takes into account the future environment and infrastructure in which the system will operate.

The details of the implementation will be published later by the programming team. In fact, the current requirements do not specify any technical solutions, in order to not restrict them while designing the technical aspects of the platform.

Our requirements were created on the basis of the semester-requirements:

- Analysis of IT security in poor countries and crisis countries
- Analysis of BSI IT security catalogs
- develop and assign appropriate solutions
- Construction of the platform:
 - Dealing with increasing threats and threats / Change management / Updates
 - hardware used, software (commercial or open-source)
 - Web interface
 - Archive and search function
 - User roles
 - Design of the platform
 - Interfaces
 - Responsibilities and maintenance of data:
 - * Who is authorized or obliged to make changes to the database make?
 - * What precautions are necessary in terms of data protection?
 - * Which information may be published in which form?
- User guidance

- Documentation of the project
- Preparation of a workshop

2. Main Objectives

2.1. Overview

The goal of this project is to design, implement and provide a guidance platform for the developing country Afghanistan. Taking the circumstances in such a developing country in account, the platform should provide the users of IT-systems with the knowledge to assure the sustainability of IT-systems in their countries. Besides providing general information on IT-systems, the platform should provide, similar to the “BSI Grundschutzkatalog”, information aiming to localize and solve problems that may occur in the IT-systems as a result of a human error, technical failure or a catastrophe etc.

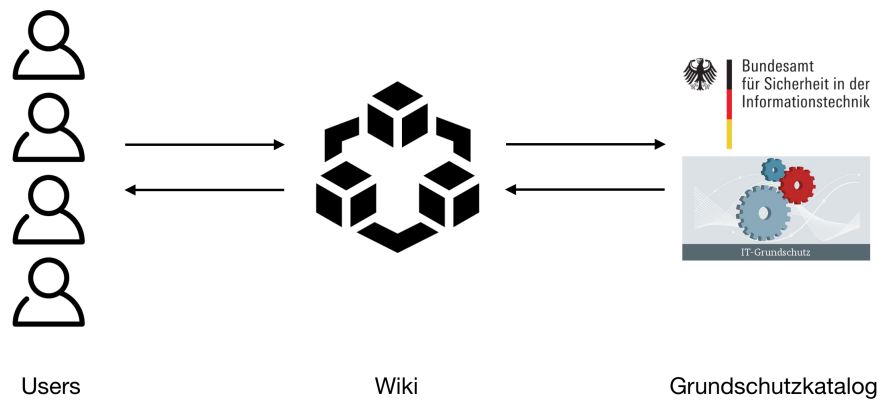


Figure 2.1.: Abstract System Design

2.2. Wiki

Considering the limited availability of IT-specialists in most of the developing countries, and after reviewing the possible ways to design and provide the platform, our team considers it convenient to create an open platform on which people can collaboratively add, edit, delete or archive content, similar to Wikipedia. This should allow the platform to constantly grow and stay relevant to current circumstances. The user created content beyond the BSI catalogue could make remarks about national peculiarities that do not play a role in Germany, aid further understanding or offer updates on more recent developments. However, this should not mean that everyone can simply write any

potentially false content for everybody to read. To assure that we have to set rules and access permission levels (see section 2.2.6). Concretely the wiki should have the following parts:

- News
- BSI catalogue
- Articles
- Archive

which will be further explained in the next subsections. In general, it should be possible to link from any page in the wiki to any other page (see Secondary Objectives 3.9 for special requirements regarding the BSI catalogue). General wiki behaviour as found on i.e. wikipedia.org applies:

- each word on any page can only link to one other page at a time,
- users who collaboratively work on the same wiki page can edit or delete each others text or links,
- each page should have a history page where different versions of the page over time can be checked,
- it is possible to retrieve a list of all users who ever worked on a given page in the wiki .

2.2.1. Links

Links are represented in two ways which slightly differ in the domains of news, articles and catalogue. A link can be:

1. ... a text link where the linked page directly comments on a word or phrase.
2. ... a bottom page link in section called 'See also' after the page content that is commenting on the wider scope of the whole page. News have no bottom page links. .

2.2.2. News

News are written by users but have to be approved by mods. If a mod approves a news article it is automatically published on the home page. The mod can decide to make a news article an important news article.

News should be implemented in the same best-practice way of Wikipedia. The figure 2.2 shows a mockup version of how it should look. One article for each month, including subsections for each day and links to previous (or future) months and years. Short sentences with links to larger articles if the news are bigger. The calendar on the right side, links each day to its section on the same page. However, news were categorized as lower priority feature by the programming group.

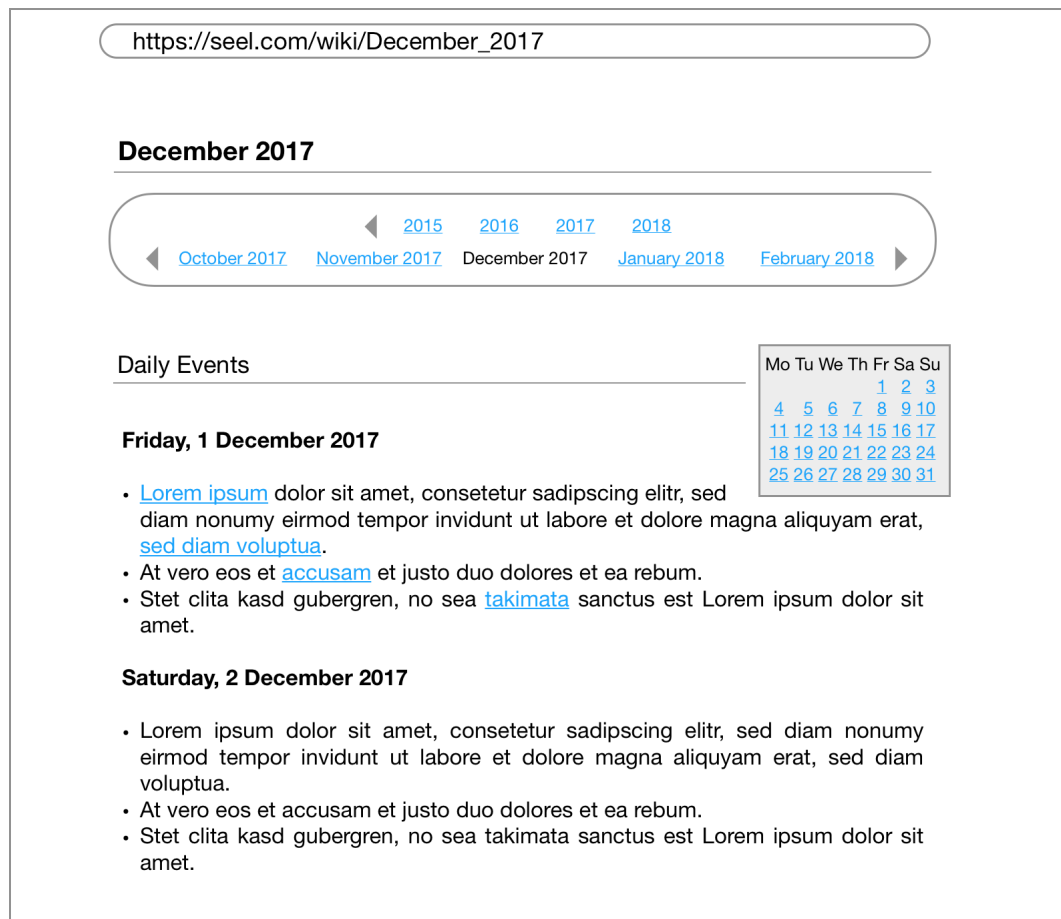


Figure 2.2.: News mockup page

2.2.3. BSI Catalogue

The BSI catalogue spans over 5000 pages which makes browsing, or even searching a specific information, a difficult task for beginners. Converting such a big text volume into wiki content by hand would be an extended task. Accordingly, a parser is needed. This parser will crawl and analyse the BSI Grundschatzkatalog website and create and sort the content automatically. The BSI catalogue is the most restrictive part in the wiki and should only be modifiable by administrators. Should users find any mistakes on the pages of the BSI, i.e. something is translated badly, the users have to inform an administrator who has to correct the text in question.

While browsing any page of the BSI catalogue a tree view of the catalogue should be displayed at the side.

The tree view adopts the structure as also found in pdf versions of the BSI catalogue. See Appendix C.1.

The tree view should not automatically expand or collapse itself without direct guest manipulation. This means for instance, that when a guest, clicks on the link of a threat

on a building block page that the tree view does not expand to show this threat. Merely the highlighted row in the tree view changes to the new item. If the item is hidden in a collapsed level the highlighted row should change colour.

BSI pages which show building blocks should be displayed slightly modified from their appearance in the catalogue. Instead of listing threats and measures separately in lists, it should be obvious only after a quick glance which measures corresponds to which threats. For this, cross-reference tables provided by the BSI should be used. These tables clearly assign each threat its measures. Thus, those pages show firstly the related text to the building block. Then a dropdown menu which allows the guest to sort the linked threats and measures by either threats or measures. Lastly, a tree view where the first level are layers, the second level the category by which the tree is sorted and the third level the other category. See Appendix C.1 for examples.

2.2.4. Archive

The website should always present up-to-date information for interested guests. Sometimes though a person might be interested in information on older systems which are not covered anymore in the most recent version of the BSI catalogue but in older versions. Those older versions and ideally their related wiki content should be available in the archive.

For example: if users are looking for an information on a no longer supported operating system and there are none in the wiki regarding this problem, the user could find older approaches in the archive.

Content in the archive can not be edited. It stays as it is since the moment it is moved to the archive.

2.2.5. Updating the BSI Catalogue

Updating the BSI catalogue to a newer version happens in three phases:

1. before the update: an administrator decides to update and performs the necessary action,
2. during the update: re-linking of pages,
3. after the update: the website is up-to-date again and old content is in the archive

About 1., the update can only be kicked-off by an administrator. The necessary action should be as simple as possible.

About 2., during this phase the website will be in a hybrid state. While the current catalogue is still available via 'Browse BSI' in the Top Section (see section 2.6) the new catalogue will be advertised in the news section on the landing page. It should stick to the top of the news list and be marked as important news. With the end of phase 1 of the update users get a notification that articles they worked on in the past have

to be re-linked. This means all the articles which are linked to the BSI catalogue and which therefore are to be considered outdated until proven otherwise by a user. At the same time there should be a page in the forum or wiki visible to all users that lists all the articles in question which have not been re-linked yet. The old catalogue and its articles should be locked during the update. This means that nobody should be able to edit them. New edits should be performed on the new catalogue and its articles. With the end of phase 2 all pages which link to the catalogue that gets archived are moved to the archive as well. Pages which were re-linked to the new catalogue are copied versions. This is necessary because articles in the wiki could be edited to reflect real world changes. Those edits then still apply to the new BSI catalogue but might not apply for older versions. Therefore, for every BSI catalogue version since the article was written and as long as it got re-linked the archive contains the same pages again which are not identical ones.

The news section on the landing page should also link to a change log page that informs about dropped, inserted and altered catalogue parts.

About 3., after a certain time - i.e. 30 days - the admin might choose to complete the process. The catalogue which up to now was accessible via 'Browse BSI' gets pushed into the archive including its wiki articles. The new catalogue gets linked to the top section and the important news on the landing page can slowly drop down as other news come in.

2.2.6. User Types

First of all, the platform will need one or multiple administrators (admins) who will update the platform from a technical perspective and ensure that policies are being respected. However, building a wiki-like platform about IT-Security for developing countries comes also with the big responsibility of the content it will provide. If everybody could publish and/or modify content without checks or labels for flaws, or malicious informations, it would present a major security risk for any layman reading it. Admins will have enough workload so we need another team of volunteers, like moderators (mods), who will check content and remove, modify or label it as unsafe if necessary. Moderators will be appointed by admins and will be responsible for policy enforcement for specific topics. Further, users who would like to publish and/or modify content will need to register to the platform and be logged in. All other users who are not logged in will be considered as guests and will only be able to read content. The following section will discuss the different user roles and their functions. This is illustrated in the appendix by the use case diagrams.

Guest, the guests have the possibility to browse and search in the archive and also in the wiki, which includes the BSI catalogue. The search can be refined with several options (more information about the search in the text search section 2.3) If guests are not sure how to find their problems they can use the wizard (more information in the

wizard section 2.4). The wiki contains news from different topics which guests can check out.

User, every registered user (registered by email address and a password) can write articles in the wiki and change them with the functions: create content and edit content. Created content can be linked in a certain part of the BSI catalogue. If the BSI catalogue updates, users who have linked content get a notification to transfer this link to the new BSI catalogue or to archive the linked wiki article with it. They can also edit their profile. After a User has logged in, he can still use the functions of a guest.

Moderator (mod), mods are managing the content published by the users. Managing or Moderating content means to delete wrong or inappropriate content or make checked content recognizable for guests that the content is verified. Mods manage the news which means they can show certain news on the home page to get more attention or delete/change incorrect news. Mods are also responsible, if necessary, to ban users. Mods can use all functions users can use.

Administrator (admin), the admin sets or changes permissions like banning users, assign topics and manage news. One of the most important tasks of the admin is to update the BSI catalogue as soon as a new one is available and to move the old one to the archive. There should be two admins for the website in case one is non-available. The admin can use all functions mods can use.

The table 2.2.6 shows the rights of each user.

	-Browse catalogue	-Add/edit articles/news -Link to BSI	-Moderate articles/news	-Assign roles -Update BSIC
Guest	✓	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>
Mod	✓	✓	✓	<input type="checkbox"/>
Admin	✓	✓	✓	✓

Figure 2.3.: user rights table

2.3. Text Search

A text search function allows users of the platform to make a free text search request and browse the results containing the key-words. Users should also have the opportunity to narrow down their search request by selecting a specific domain in which they would like to find results:

- "All": counts as every domain
- "News": domain where news are published
- "Module": modules of the BSI Grundschriftkatalog
- "Threats": threats of the BSI Grundschriftkatalog
- "Measures": measures of the BSI Grundschriftkatalog
- "Archive": archived content (no longer visible in the wiki)

Choices should be available as a dropdown list.

The search field should be well placed on the home page. The system should have a function "Back to the search results". The search function should have fault tolerance, as well as the ability to deal with synonyms. Fault tolerance means that the user will get the result even if he misspells a word or if he uses singular or plural. While a non-fault-tolerant search will let the visitor go nowhere, the system should nevertheless display the appropriate results. In addition, search functions which also master synonyms, do even more. For example, the system should derive results from the search input "laptop" in which the word "notebook" appears and for this purpose access an extensive database of words of the same meaning. The automatic completion of search terms is very welcome.

2.4. Wizard

Beginners who are not familiar with the terminology may have a hard time finding solutions to problems they encounter. To help them, we would like to implement a wizard, which will ask them a set of yes/no questions to filter out what problems they could have, similar to the game Akinator¹.

2.5. Home Page

The home page is the entry point to the different services offered by the website. As such its design should provide a clear overview of and a dead on target guidance to all available functions for users of all levels of experience. Firstly, the home page also displays the always present top section (see section 2.6) but no side bar to use the full

¹<http://en.akinator.com>

available space for the sections defined below and in order to not overwhelm the user with two detailed lists of items. Directly below the top section is a distinguished area for time-critical news which inform of widespread threats or important updates. Those are important to all users and should therefore be on top. In times of no imminent danger time-critical news might not be displayed but instead a few of the most recent regular news which are part of the wiki. The third area in a vertical sense is a wide and inviting search bar that allows experienced users the quick access to the BSI catalogue and other parts. Should a user not know what to search he can browse the BSI catalogue following a link in the top section (see section 2.6). The search offers the full functionality as described in section 2.3. As a last section before the always present bottom section is an overview of introductory tutorials on how to implement the guidelines of the BSI catalogue while developing, building and maintaining a basic IT system. Equally visible as the tutorials should be the offer to use the wizard to help and find security gaps and other system flaws. Both the tutorials and the wizard are aimed at users of no or little knowledge or overview of the BSI catalogue. For detailed explanations of the wizard see section 2.4. The bottom section shows links to items as contact, legal notice, possibly FAQ and copyright.

2.6. Top Section

The top section is an always present area at the top of each subpage that connects the different services and allows for quick access. It should feature the following items whose order and wording might be changed appropriately:

- Home Page
- News
- Browse the BSI catalogue
- Tutorials
- Wizard
- Search
- Login .

3. Secondary Objectives

3.1. API for BSI Catalog - Priority: LOW

The application programming interface (API) should offer straightforward REST access to read, create, edit and possibly manage the content of the wiki heeding the permission settings in place. This includes the News section, tutorials as well as the BSI catalogue itself. Such access could be used for a future integration into a mobile application. Existing wiki-frameworks might already include ready-to-use API functionalities and could be used.

3.2. FAQ - Priority: MEDIUM

The website should have an page showing Frequently Asked Questions (FAQ) and there answers. Questions should be grouped by theme and answers hidden behind expandable questions. This gives the guest a better overview on the questions that are dealt with. The FAQ should be accessible through the bottom section and should also be present on the tutorial overview page. Content will be provided by the analysis team.

3.3. Discussion pages - Priority: MEDIUM

3.3.1. Definition

- Discussion pages are pages, in form of a Tab, linked in the upper left corner of each article.
- a Discussion page doesn't exist unless a user starts a discussion about the article
 - There should be a button called "start a discussion".
- These pages consist of at least one discussion or more about the related Topic.
- All registered members, including the author of the topic, are allowed to take part in the discussion.
- The content of a discussion page is to be kept online as long as the related article is online, unless a moderator decides otherwise.
- To allow a flowing discussion, the content in the discussion page doesn't need to be approved by a moderator before being published, taking in count that users not obeying the roles of the wiki should be banned or at least get a warning.

- There are no discussion pages for BSI pages.

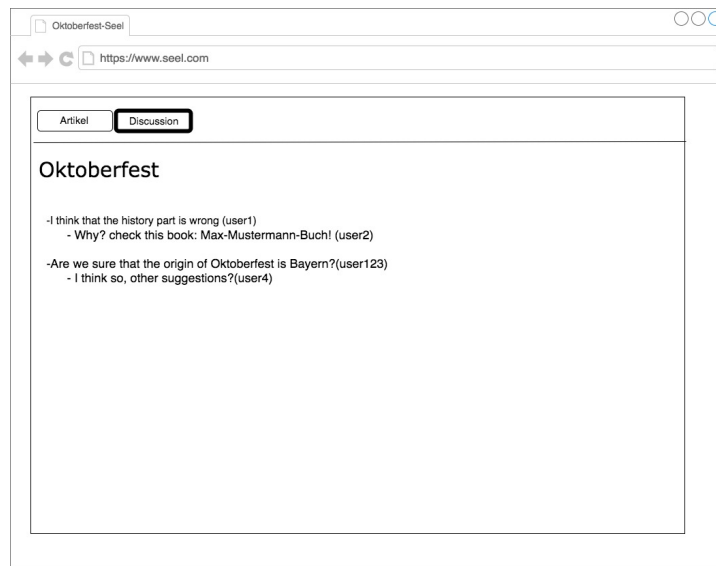


Figure 3.1.: Discussion page example

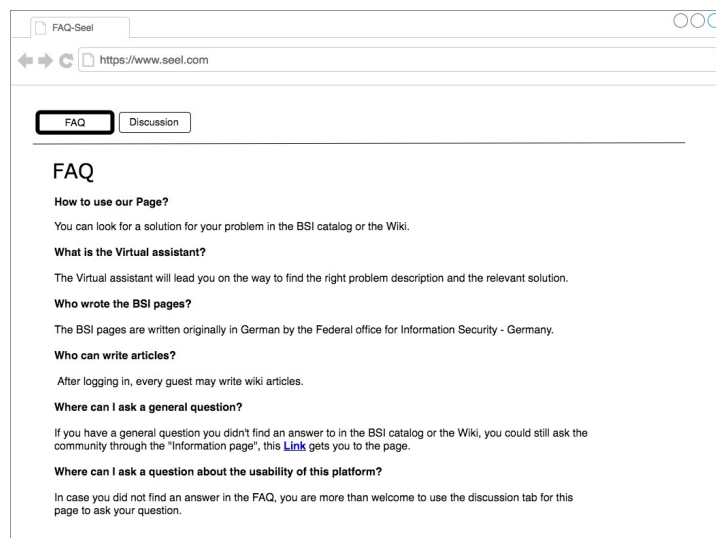


Figure 3.2.: Link to the Information page in the FAQ

3.3.2. Benefits

The main idea behind discussion pages is to allow the users to discuss about a specific article in the Wiki. Topics written by users tend often to start discussions, mostly because the authors aren't professionals in the specific fields they write about. To avoid

having multiple wiki articles about one Subject as a result of different opinions, we would allow and recommend user to discuss one article in purpose of reaching a common opinion about the subject.

3.3.3. Types of discussion pages

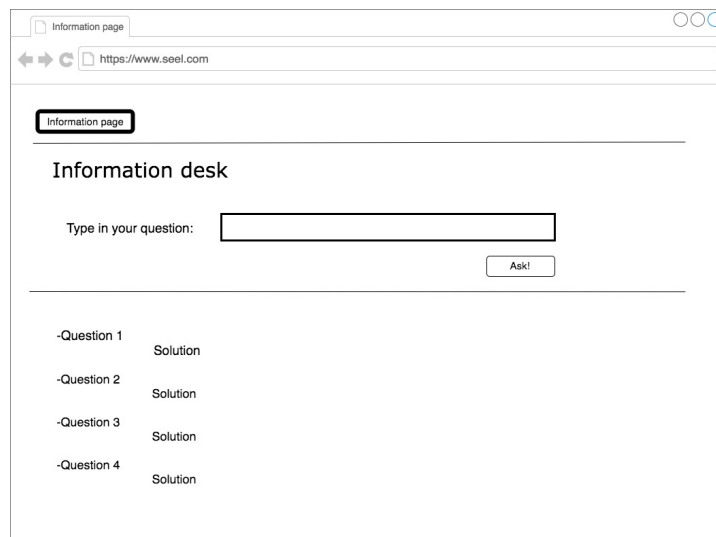
- Discussion regarding user-generated articles
- Discussion regarding BSI page: unlike user-generated articles discussion pages, these discussion pages are not aiming to improve the content of BSI pages, but just to discuss the topics and share question regarding them.
- Discussion regarding FAQ: This page will be used to enable the users of our platform to ask general questions regarding the usability of this page which was not found in the FAQ.

3.4. Information page - Priority: MEDIUM

The Information page allows EVERY guest to share and publish general questions to the community in our platform.

Since the platform main concept is to share the BSI pages and good content through Wiki to the community, we came upon a conclusion to keep it "hidden" and just link it in the FAQ page (See graphic below).

The Information page should allow every guest to write content, so unlike normal articles, there should be a text field on the top of the article, provided with a submit button.



Information page

https://www.seel.com

Information page

Information desk

Type in your question:

Ask!

-Question 1 Solution

-Question 2 Solution

-Question 3 Solution

-Question 4 Solution

Figure 3.3.: Information page structure

3.5. Report a Mistake - Priority: MEDIUM

Since the BSI pages are automatically translated, translation errors may occur quite often, and since the users can't update the pages and correct the mistakes themselves, we need a tool, in which users can inform the mods in case they find an error.

The page consists of a text field, in which the users are asked to fill in information regarding the mistake they found.

The field can't be empty, but the users are free to write description and improvement tips as they want.

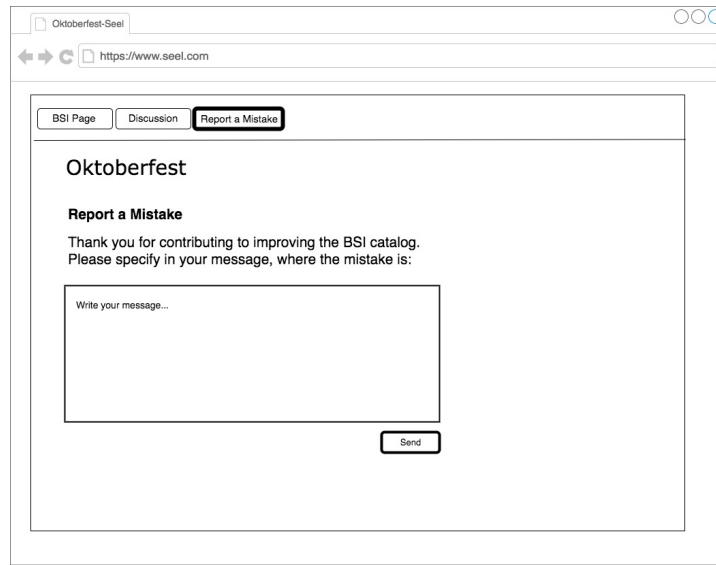
The image shows a web browser window with the address bar displaying 'https://www.seel.com'. The page has three tabs: 'BSI Page', 'Discussion', and 'Report a Mistake', with the last one being the active tab. The main content area is titled 'Oktoberfest' and contains a sub-header 'Report a Mistake'. Below this, a message reads: 'Thank you for contributing to improving the BSI catalog. Please specify in your message, where the mistake is:'. There is a large text input field with the placeholder text 'Write your message...'. At the bottom right of the input field is a 'Send' button.

Figure 3.4.: The structure of "Report a Mistake"

The moderators should check these forms and, if necessary, correct the errors.

3.6. Labels - Priority: HIGH

Labels should inform website users about the current state of content.

Types of labels:

- **creation status:** an automatically generated label which gives information about how long ago the content has been created. Formatting in hours, weeks, months and years.
- **unchecked/checked:** The default is unchecked, content read by moderators and where the content is appropriate will get a checked label. When a user edits a checked article, it will be automatically gets a unchecked label.
- **helpful label:** For a certain number of upvotes, content should get a helpful label. This should be scalable

- **content type:** use labels as a 'path'/show where the page is: news, archive, BSIc. Several content types are possible.
- **important:** The important label is mainly to draw attention to certain news.

It should be possible to label each content, articles as well as news. For the news it should be possible to put a label within an article. For example, to mark individual news with an important label. It should be possible for the admin to create a new label that he considers appropriate.

Here are some examples for label

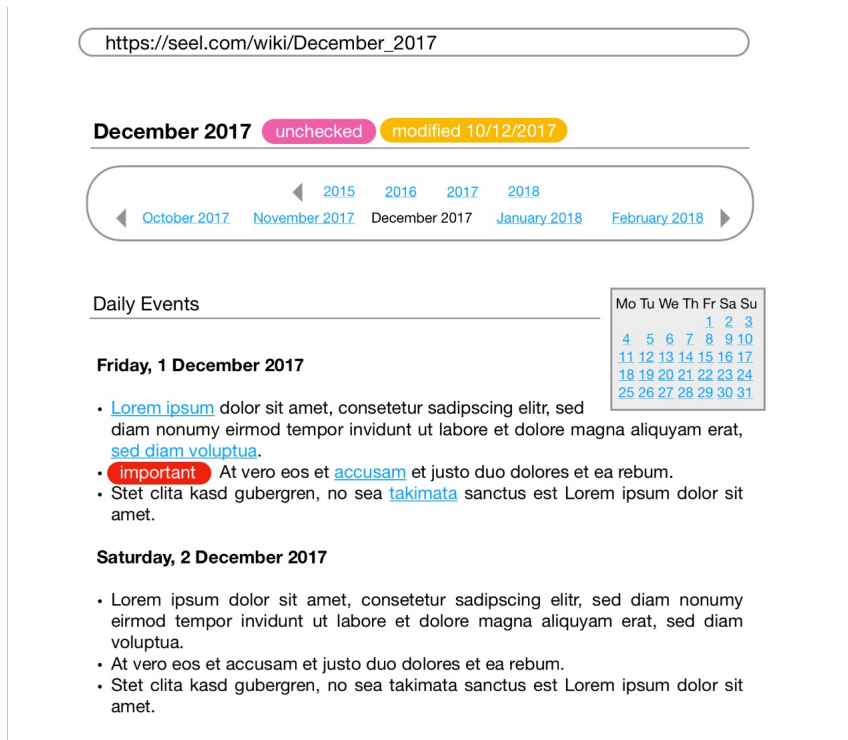


Figure 3.5.: Labels in the News section

3.7. Up/Down Votes - Priority: MEDIUM

Article votes would be nice in form of a “Is this page helpful?” Question with yes/no buttons at the end of it, which could generate after 100 yes votes a label “Helpful” or through many no votes draw the attention to revisions the article. Every website user can vote, including the guest. When an article is re-linked during an update, all the votes will remain.



Figure 3.6.: Microsoft helpful-vote example

3.8. Reputation Points (Karma Points) - Priority: MEDIUM

Reputation points should motivate users to get involved on the side and reward them for that.

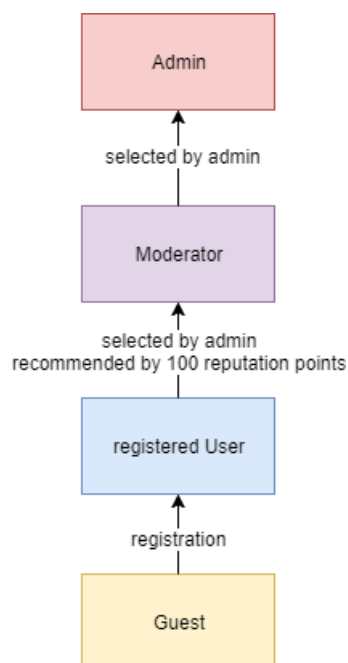


Figure 3.7.: Waffle label analyse

We would like to keep a similiar (best-practice) user structure to Wikipedia. In our system we will have admins, the “sichter” will be our “moderator”, we will also have registered user and guests.

However after intensive discussion about how Karma (or reputation points) is generated, we decided to just keep the “article upvoting” generated votes for an article only without passing it to the user, since the quality of writing / editing, perhaps only a few, article isn’t representative of the trustworthiness of a user.

Only users which have had a big number (100) of approved edits/writings are recommended to the admin as a new mod. However it remains the decision of the admin whom appoint as mod. If the admin needs help he can select a mod and add him as as

additional admin.

3.9. User Access to BSI Catalogue Pages - Priority: HIGH

While the general access to alter the pages of the BSI catalogue should be restrictive (see section 2.2.3) users who write an article should still be allowed to link their article in the pages of the BSI catalogue.

For mockups of the linking process detailed here see Appendix C.2. After or while users write their articles they are presented with the option to link it to the BSI catalogue. This option leads users to another page. Here:

- users can search for wiki content they want to link to,
- users can directly browse the BSI tree to find the page they want to link to,
- on the left users see a list of titles of wiki pages that they already have linked their article to .

There is no restriction on the number of pages an article can be linked to. So the list of linked pages should offer a scroll bar if the list exceeds the page limits. If users click on a search result, a BSI tree item or an item of the list of linked to wiki pages they are brought to the page in question. There, if users want to link to a word they click on/mark the word they want to link their article to. Alternatively, they click on/mark the “See also” section of the page. Both times the selection has to be confirmed and brings the user back to the second page which features the list of linked pages. The list of search results should be limited to ten. So that, users have to change or add to his keywords if they did not get the page they were looking for. All pages should have a “Back” or “Cancel” button.

3.10. Automatically created best 10 Suggestions when linking to BSI - Priority: LOW

For mockups of the linking process detailed here see Appendix C.2. The best 10 Suggestions are nice to have but low periorized. It would be nice if these suggestions appear automatically after writing an article. Our idea was that these suggestions would be found through the internal search. These suggestions are always updated when the user enters something again in the search field. This topic is low-periodized and does not need to be strongly considered.

3.11. Extended Wizard (Work in Progress) - Priority: LOW

A. Glossar

Guest - a visitor of the website.

User - the user type relating to the wiki permissions.

Mod - the user type relating to the wiki permissions.

Admin - the user type relating to the wiki permissions.

(Wiki) Content - a page in the wiki. Could belong to News, BSI catalogue, articles or archived versions of all of the above.

Article - a page in the wiki which was created by a user and does not belong to the News or BSI catalogue.

Threat - as defined by the BSI Grundschutzkatalog (Gefährdung).

Measure - as defined by the BSI Grundschutzkatalog (Maßnahme).

B. Use Case Diagrams

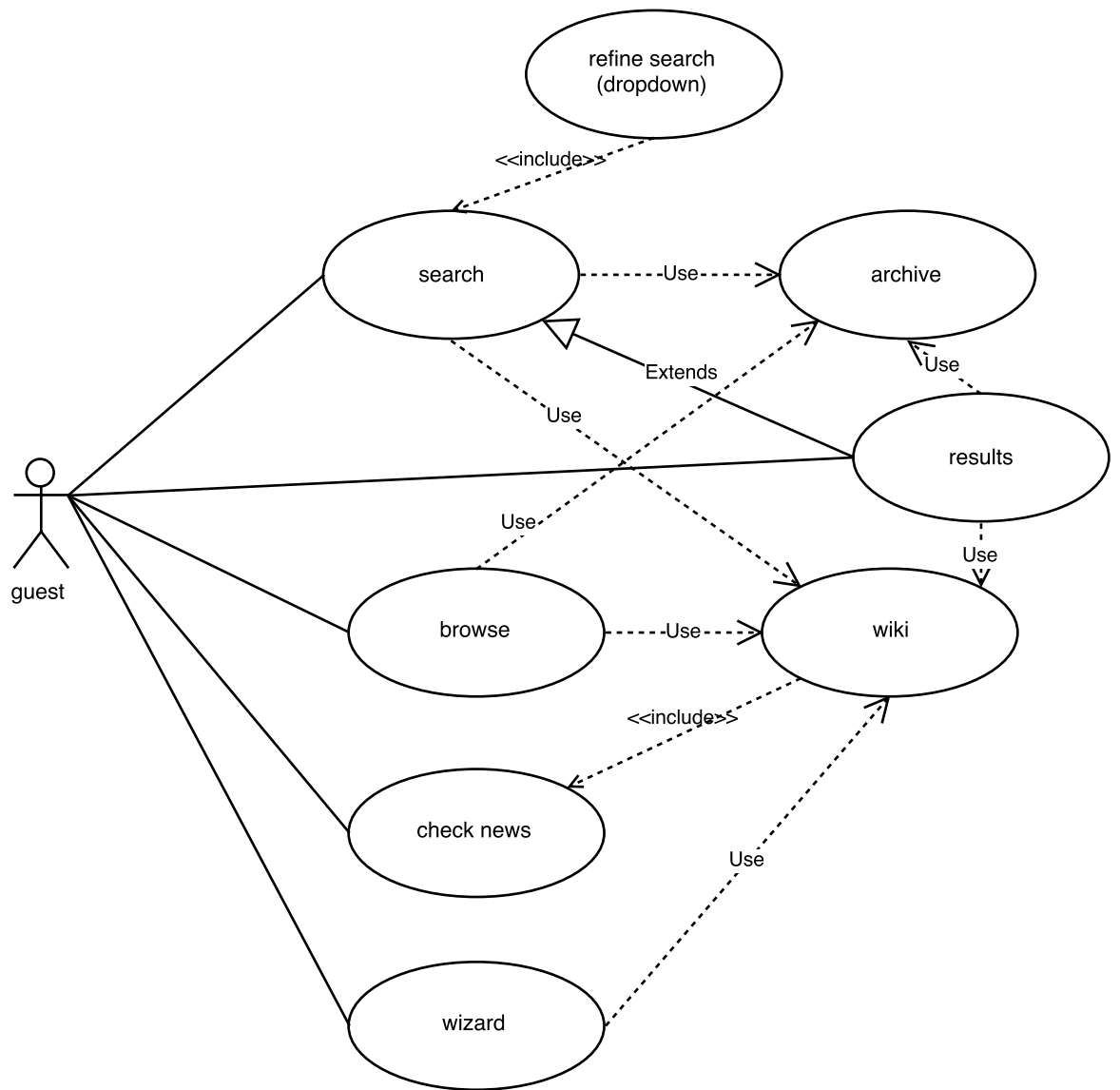


Figure B.1.: guest - use case

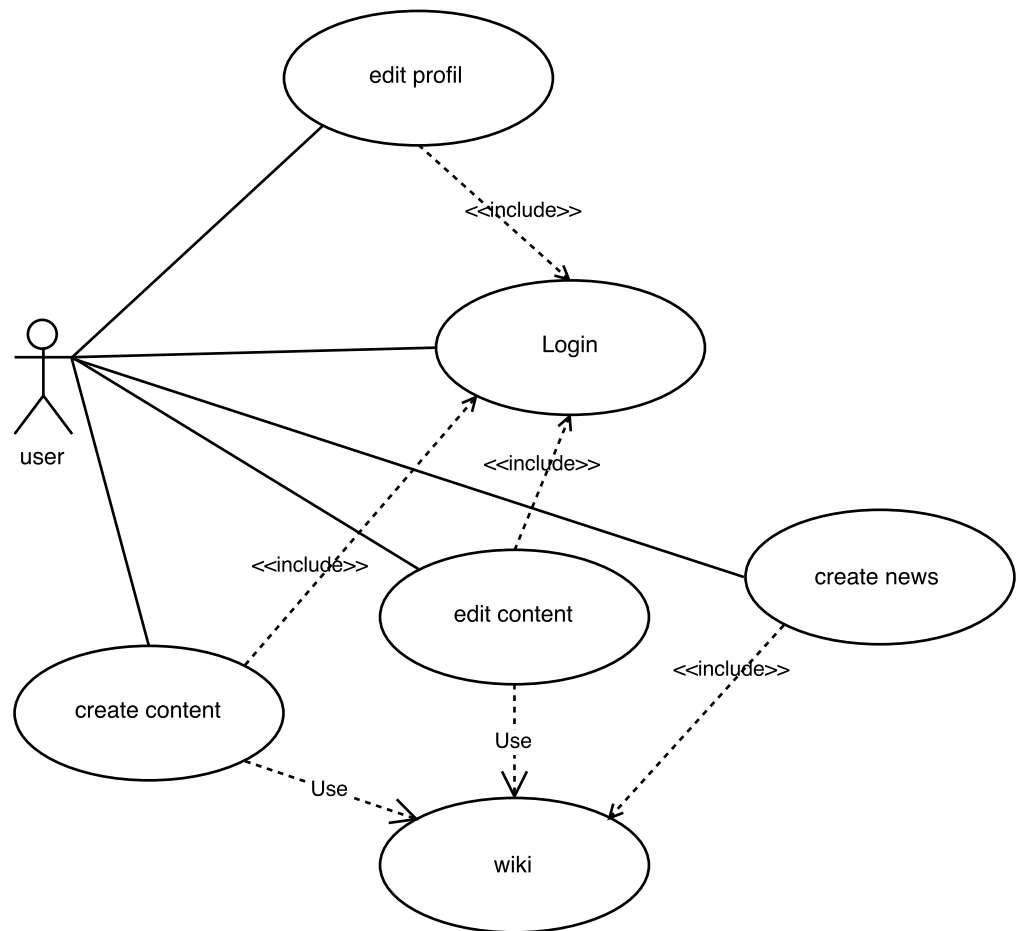
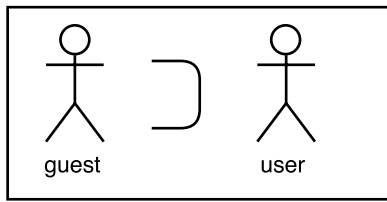


Figure B.2.: user - use case

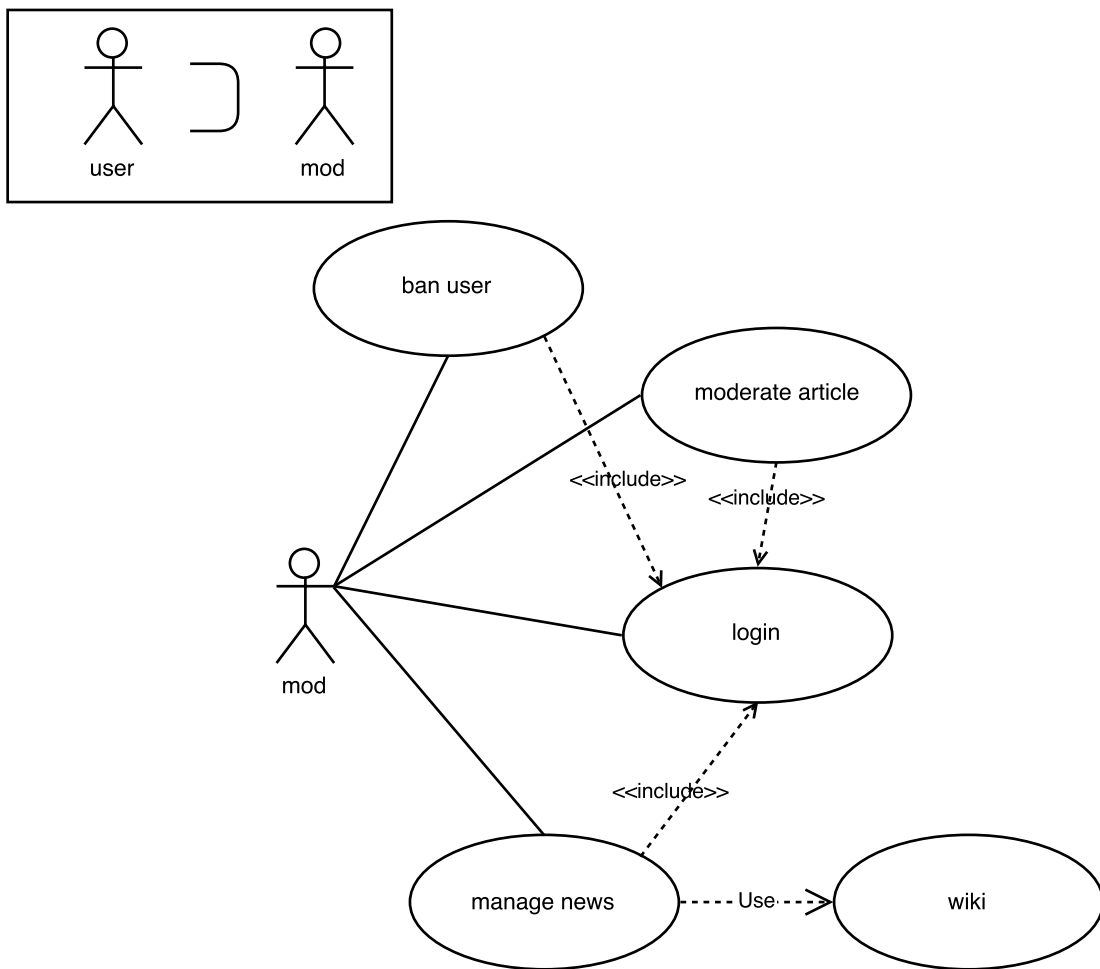


Figure B.3.: mod - use case

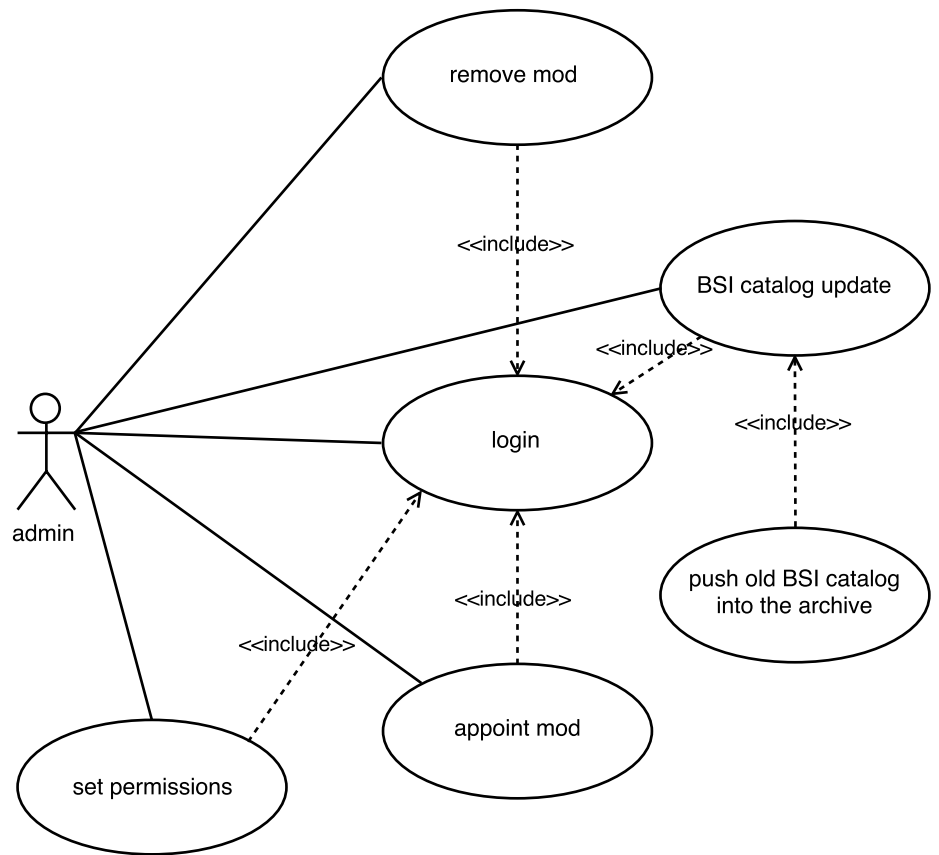
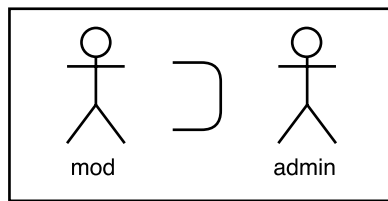


Figure B.4.: admin - use case

C. BSI Pages

C.1. Structure of BSI Pages

C.2. Linking to BSI Pages

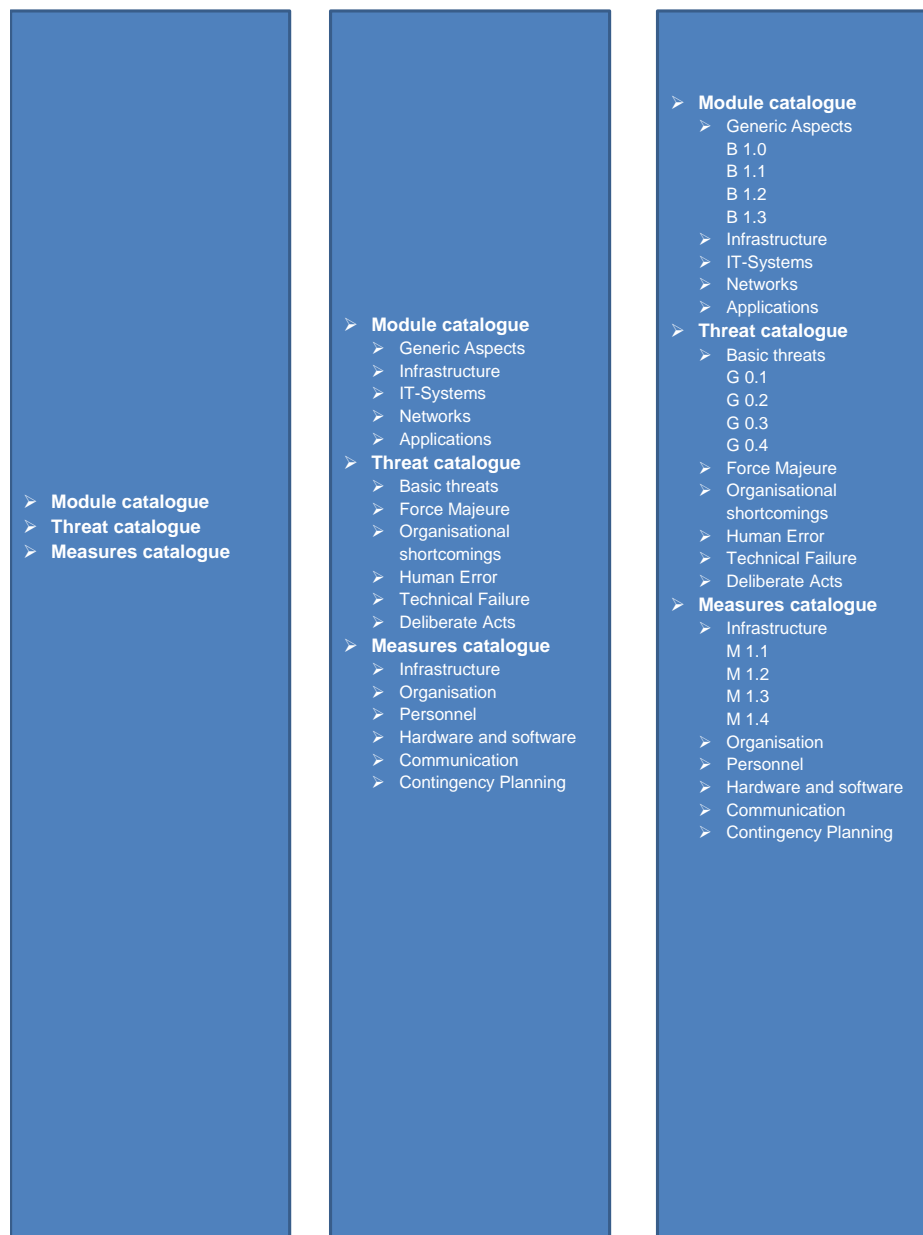


Figure C.1.: Tree view of BSI pages.

➤ **Module Catalogue**

➤ **Generic Aspects**

B 1.0

B 1.1

B 1.2

B 1.3

➤ Infrastructure

➤ IT-Systems

➤ Networks

➤ Applications

➤ **Threat catalogue**

➤ **Measures catalogue**

Sort by ▼

Threats

Measures

Threats ▼

➤ **Force majeure**

➤ G 1.1 *Loss of personnel*

- M 2.226 (A) *Procedures regarding the use of outside staff*

- M 3.51 (Z) *Appropriate concept for assignment and qualification*

➤ G 1.2 *Failure of the IT system*

➤ **Organisational shortcomings**

➤ G 2.2 *Insufficient knowledge of rules and procedures*

➤ G 2.7 *Unauthorised use of rights*

➤ **Human error**

➤ G 3.1 *Loss of data confidentiality or integrity as a result of user error*

➤ G 3.2 *Negligent destruction of equipment or data*

➤ G 3.3 *Non-compliance with IT security measures*

- M 3.4 (A) *Training before actual use of a program*

- M 3.50 (Z) *Selection of employees*

➤ G 3.8 *Improper use of the IT system*

➤ G 3.9 *Improper IT system administration*

➤ G 3.36 *Misinterpretation of events*

➤ G 3.37 *Unproductive searches*

- M 3.11 (A) *Training of maintenance and administration staff*

➤ G 3.43 *Inappropriate handling of passwords or other authentication mechanisms*

➤ G 3.44 *Carelessness in handling information*

➤ G 3.77 *Insufficient acceptance of information security*

➤ **Deliberate acts**

➤ G 5.1 *Manipulation or destruction of equipment or accessories*

➤ G 5.2 *Manipulation of information or software*

➤ G 5.20 *Misuse of administrator rights*

➤ G 5.23 *Malicious software*

➤ G 5.42 *Social Engineering*

➤ G 5.80 *Hoax*

➤ G 5.104 *Espionage*

➤ **Module Catalogue**

➤ **Generic Aspects**

B 1.0

B 1.1

B 1.2

B 1.3

➤ Infrastructure

➤ IT-Systems

➤ Networks

➤ Applications

➤ **Threat catalogue**

➤ **Measures catalogue**

➤ **Force majeure**

➤ G 1.1 *Loss of personnel*

- M 2.226 (A) *Procedures regarding the use of outside staff*

- M 3.51 (Z) *Appropriate concept for assignment and qualification*

➤ G 1.2 *Failure of the IT system*

➤ **Organisational shortcomings**

➤ G 2.2 *Insufficient knowledge of rules and procedures*

➤ G 2.7 *Unauthorised use of rights*

➤ **Human error**

➤ G 3.1 *Loss of data confidentiality or integrity as a result of user error*

➤ G 3.2 *Negligent destruction of equipment or data*

➤ G 3.3 *Non-compliance with IT security measures*

- M 3.4 (A) *Training before actual use of a program*

- M 3.50 (Z) *Selection of employees*

➤ G 3.8 *Improper use of the IT system*

➤ G 3.9 *Improper IT system administration*

➤ G 3.36 *Misinterpretation of events*

➤ G 3.37 *Unproductive searches*

- M 3.11 (A) *Training of maintenance and administration staff*

➤ G 3.43 *Inappropriate handling of passwords or other authentication mechanisms*

➤ G 3.44 *Carelessness in handling information*

➤ G 3.77 *Insufficient acceptance of information security*

➤ **Deliberate acts**

➤ G 5.1 *Manipulation or destruction of equipment or accessories*

➤ G 5.2 *Manipulation of information or software*

➤ G 5.20 *Misuse of administrator rights*

➤ G 5.23 *Malicious software*

➤ G 5.42 *Social Engineering*

➤ G 5.80 *Hoax*

➤ G 5.104 *Espionage*

Sort by ▾

Threats

Measures

Threats ▾

- Module Catalogue
- Generic Aspects
 - B 1.0
 - B 1.1
 - B 1.2**
 - B 1.3
- Infrastructure
- IT-Systems
- Networks
- Applications
- Threat catalogue
- Measures catalogue

B 1.2 Personnel

Description

This module illustrates the generic IT-Grundschutz safeguards that should be implemented as standards in the area of personnel. A number of safeguards are necessary starting from the time the employees are hired and continuing until they leave the organisation. Adequate security safeguards also need to be implemented to handle external personnel such as visitors or maintenance technicians. Personnel recommendations that are linked to a specific role such as the appointment of a system administrator for a LAN are provided in the modules dealing with the corresponding topic.

Method recommendation

To secure the information system examined, other modules will need to be implemented in addition to this module. These modules are selected based on the results of the IT - Grundschutz modelling process.

A series of safeguards need to be implemented for the personnel employed at a company or a government agency, starting with proper training for new employees and further training and continuing right up to until an employee leaves the organisation. The steps to be followed in this case as well as the safeguards to be taken into consideration in the respective steps are listed in the following.

Sort by ▼
Threats
Measures

Measures ▼

- **Planning and design**
 - M 2.226 (A) *Procedures regarding the use of outside staff*
 - G 1.1 Loss of personnel
 - M 3.51 (Z) *Appropriate concept for assignment and qualification of employees*
 - - G 1.1 Loss of personnel
 - M 3.83 (Z) *Analysis of security-relevant personnel factors*
- **Procurement**
 - M 3.50 (Z) *Selection of employees*
 - G 3.3 Non-compliance with IT security measures
- **Implementation**
 - M 3.1 (A) *Well-regulated familiarisation/training of new staff with their work*
 - M 3.10 (A) *Selection of a trustworthy administrator and his substitute*
 - M 3.33 (Z) *Security vetting of staff*
 - M 3.55 (C) *Non-disclosure agreements (NDAs)*
- **Operation**
 - M 3.3 (A) *Arrangements for substitution*
 - M 3.4 (A) *Training before actual use of a program*
 - G 3.3 Non-compliance with IT security measures
 - M 3.5 (A) *Training on security safeguards*
 - M 3.7 (Z) *Point of contact in case of personal problems*
 - M 3.8 (Z) *Avoidance of factors impairing the organisation climate*
 - M 3.11 (A) *Training of maintenance and administration staff*
 - G 3.37 Unproductive searches
- **Disposal**
 - M 3.6 (A) *Regulated procedure for when employees leave the organisation*

B 1.2 Personnel

This module illustrates the generic IT-Grundschutz safeguards that should be implemented as standards in the area of personnel. A number of safeguards are necessary starting from the time the employees are hired and continuing until they leave the organisation. Adequate security safeguards also need to be implemented to handle external personnel such as visitors or maintenance technicians. Personnel recommendations that are linked to a specific role such as the appointment of a system administrator for a LAN are provided in the modules dealing with the corresponding topic.

Method recommendation

To secure the information system examined, other modules will need to be implemented in addition to this module. These modules are selected based on the results of the IT-Grundschutz modelling process.

A series of safeguards needs to be implemented for the personnel employed at a company or a government agency, starting with proper training for new employees and further training and continuing right up to until an employee leaves the organisation. The steps to be followed in this case as well as the safeguards to be taken into consideration in the respective steps are listed in the following.

Sort by ▾

Threats

Measures

Measures ▾

- **Planning and design**
 - M 2.226 (A) *Procedures regarding the use of outside staff*
 - G 1.1 *Loss of personnel*
 - M 3.51 (Z) *Appropriate concept for assignment and qualification of employees*
 - G 1.1 *Loss of personnel*
 - M 3.83 (Z) *Analysis of security-relevant personnel factors*
- **Procurement**
 - M 3.50 (Z) *Selection of employees*
 - G 3.3 *Non-compliance with IT security measures*
- **Implementation**
 - M 3.1 (A) *Well-regulated familiarisation/training of new staff with their work*
 - M 3.10 (A) *Selection of a trustworthy administrator and his substitute*
 - M 3.33 (Z) *Security vetting of staff*
 - M 3.55 (C) *Non-disclosure agreements (NDAs)*
- **Operation**
 - M 3.3 (A) *Arrangements for substitution*
 - M 3.4 (A) *Training before actual use of a program*
 - G 3.3 *Non-compliance with IT security measures*
 - M 3.5 (A) *Training on security safeguards*
 - M 3.7 (Z) *Point of contact in case of personal problems*
 - M 3.8 (Z) *Avoidance of factors impairing the organisation climate*
 - M 3.11 (A) *Training of maintenance and administration staff*
 - G 3.37 *Unproductive searches*
- **Disposal**
 - M 3.6 (A) *Regulated procedure for when employees leave the organisation*

Figure C.3.: BSI page showing a building block page sorted by measures.

[Back](#)

Add a new Article

Write your Article...

[Link to BSIC](#) 

Save

Figure C.4.: The editing page to write an article features the option for users to link their article.

[Back](#)

Search results

search

Link 1
Link 2
Link 3
Link 4
Link 5
.....

Link 20

Best 10 Suggestions

- ☐ Option 1
- ☐ Option 2
- ☐ Option 3
- ☐ Option 4
- ☐
- ☐ Option 10

Select from catalogue

- **Module Catalogue**
 - **Generic Aspects**
 - B 1.0
 - B 1.1
 - B 1.2**
 - B 1.3
 - Infrastructure
 - IT-Systems
 - Networks
 - Applications
- **Threat catalogue**
- **Measures catalogue**

Figure C.5.: When users want to link their articles they can search for keywords or browse the catalogue. They always see their already linked pages.

[Back](#)

Example article

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum
[Lorem](#) Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

confirm selection

Figure C.6.: Users select a word on a BSI page and confirm their selection.