DISCLAIMER: I AM NOT A LAWYER!
What is the Single Digital Gateway?
ARTICLE

What is the Online Access Act?

The Online Access Act (Onlinenzugangsgesetz, OZG) legally obligates the public administration in Germany to pro-
Compliance Manager, Audit Team, Construction Manager, User, Area Security Officer, Procurement Department, Fire Safety Officer, Data Protection Officer, Developer, Construction Company, Department, Process Owner, Building Services, ICS Information Security Officer, Chief Information Security Officer (CISO), Organisation, Top Management, IS Audit Team, IT Operation Department, Employee, BCM Officer, Operational Technology Operations, Head of OT, Human Resources Department, Planner, Tester, Supervisor, Maintenance Personnel, Central Administration
IT-Grundschutz-Compendium

Final Draft, 1 February 2022

https://bsi.bund.de/grundschutz --&gt; English
47 Elementary Threats
Fire; Unfavourable Climatic Conditions; Water; Pollution, Dust, Corrosion; Natural Disasters; Catastrophes in the Vicinity; Major Events in the Vicinity; Failure or Disruption of the Power Supply; Failure or Disruption of Communication Networks; Failure or Disruption of Supply Networks; Failure or Disruption of Service Providers; Electromagnetic Interference; Interception of Compromising Interference Signals; Interception of Information / Espionage; Eavesdropping; Theft of Devices, Storage Media and Documents; Loss of Devices, Storage Media and Documents; Poor Planning or Lack of Adaptation; Disclosure of Sensitive Information; Information or Products from an Unreliable Source; Manipulation with Hardware or Software; Manipulation of Information; Unauthorised Access to IT Systems; Destruction of Devices or Storage Media; Failure of Devices or Systems; Malfunction of Devices or Systems; Lack of Resources; Software Vulnerabilities or Errors; Violations of Laws or Regulations; Unauthorised Use or Administration of Devices and Systems; Incorrect Use or Administration of Devices and Systems; Misuse of Authorisation; Shortage of Personnel; Assault; Coercion, Blackmail or Corruption; Identity theft; Repudiation of Actions; Misuse of Personal Information; Malware; Denial of Service; Sabotage; Social Engineering; Attack with Specially Crafted Messages; Unauthorised Entry to Premises; Data Loss; Loss of Integrity of Sensitive Information; Harmful Side Effects of IT-Supported Attacks
BSI Standard 200-1 defines the general requirements for an ISMS

BSI Standard 200-2 explains how an ISMS can be built based on one of three different approaches

BSI Standard 200-3 contains all risk-related tasks

BSI Standard 100-4 covers Business Continuity Management (BCM)
Initiating of the security process
- Management commitment
- Designing and planning the security process
- Provision of financial resources, personnel and necessary time
- Selecting an approach

Drawing up an information security policy

Suitable organisational structure
- Drawing up a security concept
- Implementing the security concept

Maintenance and continuous improvement
- Improving the ISMS
- Extending the selected approach
WHAT IS YOUR STORY?
Holy Trinity

- Loss of Availability
- Loss of Confidentiality of Information
- Loss of Integrity (Correctness of Information)
- Basic Requirement
- Standard Requirement
- Requirement in Case of Increased Protection Needs
### ISMS

**Process-oriented modules**
- ORP
- CON
- OPS

**System-oriented modules**
- APP
- SYS
- IND
- NET
- INF

### DER
<table>
<thead>
<tr>
<th>Modules / Layer</th>
<th>(104 in 2022)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISMS</td>
<td>Security Management (1)</td>
</tr>
<tr>
<td>ORP</td>
<td>organisational &amp; personnel (5)</td>
</tr>
<tr>
<td>CON</td>
<td>concepts and methodologies (8)</td>
</tr>
<tr>
<td>OPS</td>
<td>operational (13)</td>
</tr>
<tr>
<td>APP</td>
<td>applications &amp; services (19)</td>
</tr>
<tr>
<td>SYS</td>
<td>IT systems (22)</td>
</tr>
<tr>
<td>IND</td>
<td>industrial IT (6)</td>
</tr>
<tr>
<td>NET</td>
<td>networking (10)</td>
</tr>
<tr>
<td>INF</td>
<td>infrastructure (12)</td>
</tr>
<tr>
<td>DER</td>
<td>detecting, incidents, continuity, ... (7)</td>
</tr>
</tbody>
</table>
• **R1**: These modules should be implemented with priority because they are the basis for an effective security process.

• **R2**: These modules should be implemented next because they are required to achieve sustainable security in essential parts of an information domain.

• **R3**: These modules are also needed to achieve the desired security level and must be implemented. The BSI recommends considering these after the other modules.
ISMS – 1 Sublayer – 17 Requirements

ORP.1 Organisation
ORP.2 Personnel
ORP.3 Awareness and Training in Information Security
ORP.4 Identity and Access Management
ORP.5 Compliance Management

CON.1 Crypto Concept
CON.2 Data Protection
CON.3 Backup Concept
CON.6 Deleting and Destroying Data and Devices
CON.7 Information Security on Trips Abroad
CON.8 Software Development
CON.9 Information Exchange
CON.10 Development of Web Applications
DER.1 Detecting Security-Relevant Events
DER.2.1 Security Incident Handling
DER.2.2 Provisions for IT Forensics
DER.2.3 Clean-Up of Extensive Security Incidents
DER.3.1 Audits and Revisions
DER.3.2 Audits Based on the BSI “Guideline for IS Audits”
DER.4 Business Continuity Management
APP.1.1 Office Products
APP.1.2 Web Browsers
APP.1.4 Mobile Applications (Apps)
APP.2.1 General Directory Service
APP.2.2 Active Directory
APP.2.3 OpenLDAP
APP.3.1 Web Applications and Web Services
APP.3.2 Web Servers
APP.3.3 File Servers
APP.3.4 Samba
APP.3.6 DNS Servers
APP.4.2 SAP ERP Systems
APP.4.3 Relational Database Systems
APP.4.4 Kubernetes
APP.4.6 SAP ABAP Programming
APP.5.2 Microsoft Exchange and Outlook
APP.5.3 General E-Mail Clients and Servers
APP.6 General Software
APP.7 Development of Individual Software (10)
APP.7 Development of Individual Software
APP.7.A1 Including Aspects of Individual Software in Software Deployment Planning (B)
APP.7.A2 Defining Security Requirements for the Software Development Process (B)
APP.7.A3 Specification of Security Functions for System Integration [IT Operation Department] (B)
APP.7.A4 Commissioning in Line with Requirements [Procurement Department] (B)
---
APP.7.A5 Appropriate Control of Application Development (S)
APP.7.A6 Documentation of Individual Software Requirements (S)
APP.7.A7 Secure Acquisition of Individual Software (S)
APP.7.A8 Early Involvement of the Process Owner in Development-Related Software Tests (S)

(B) "Basic Requirement"
(S) "Standard Requirement"
(H) "Requirement in Case of Increased Protection Needs"
Requirements in Case of Increased Protection Needs

APP.7.A9 Trusted Storage (H)

APP.7.A10 Commissioning Certified Software Development Companies (H)
Pre-SDL Requirements:
- Security Training

Phase 1: Requirements

Phase 2: Design

Phase 3: Implementation

Phase 4: Verification

Phase 5: Release

Post-SDL Requirement:
- Response
YOUR STORY
To Do

Doing

Done
PRIORITIZE
Executive Order on Improving the Nation’s Cybersecurity

(j) the term “Software Bill of Materials” or “SBOM” means a formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product. It is analogous to a list of ingredients on food packaging. An SBOM is useful to those who develop or manufacture software, those who select or purchase software, and those who operate software. Developers often use available open source and third-party software components to create a product; an SBOM allows the builder to make sure those components are up to date and to respond quickly to new vulnerabilities. Buyers can use an SBOM to perform
```python
33 self.fingerprints = set()
34 self.logdupes = True
35 self.debug = debug
36 self.logger = logging.getLogger(__name__)
37
38 if path:
39     self.file = open(os.path.join(path,),
40         self.file.seek(0)
41         self.fingerprints.update(x, os.linesep)
42 for x in self.fingerprints:
43     if x in self.fingerprints:
44         return True
45
46 @classmethod
47 def from_settings(cls, settings):
48     debug = settings.getbool("DEBUGFILTER_DEBUG")
49     return cls(job_dir(settings), debug)
50
51 def request_seen(self, request):
52     fp = self.request_fingerprint(request)
53     if fp in self.fingerprints:
54         return True
55     self.fingerprints.add(fp)
56     self.file.write(fp + os.linesep)
```
Crisis
To do
Testing
Done
FINISH
OWN YOUR ERROR
Change
HAPPY NEW YEAR
NEW YEAR
Resolutions
TO DO LIST
Thank you!