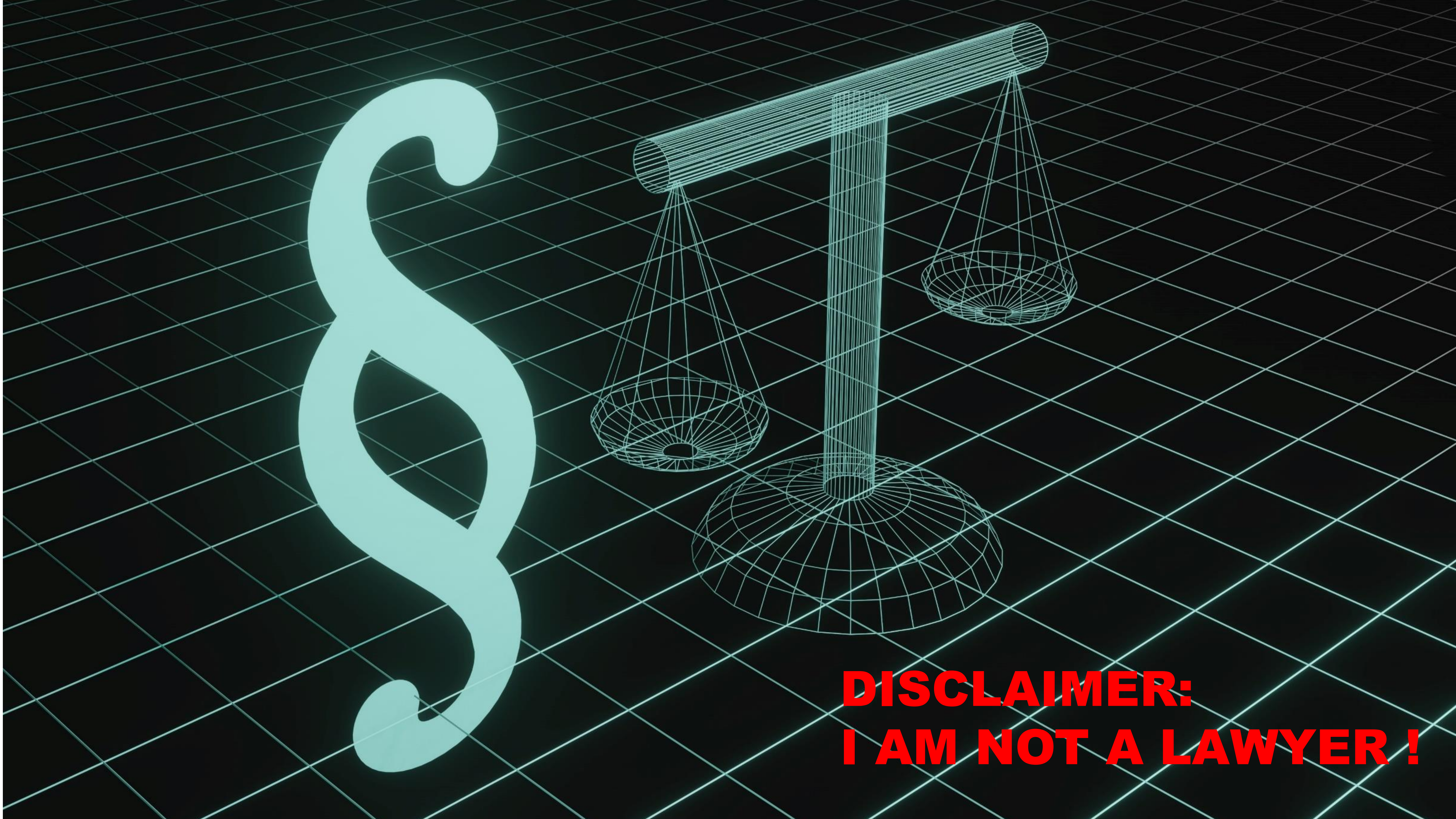
IT GRUNDSCHUTZ
AND SBOM



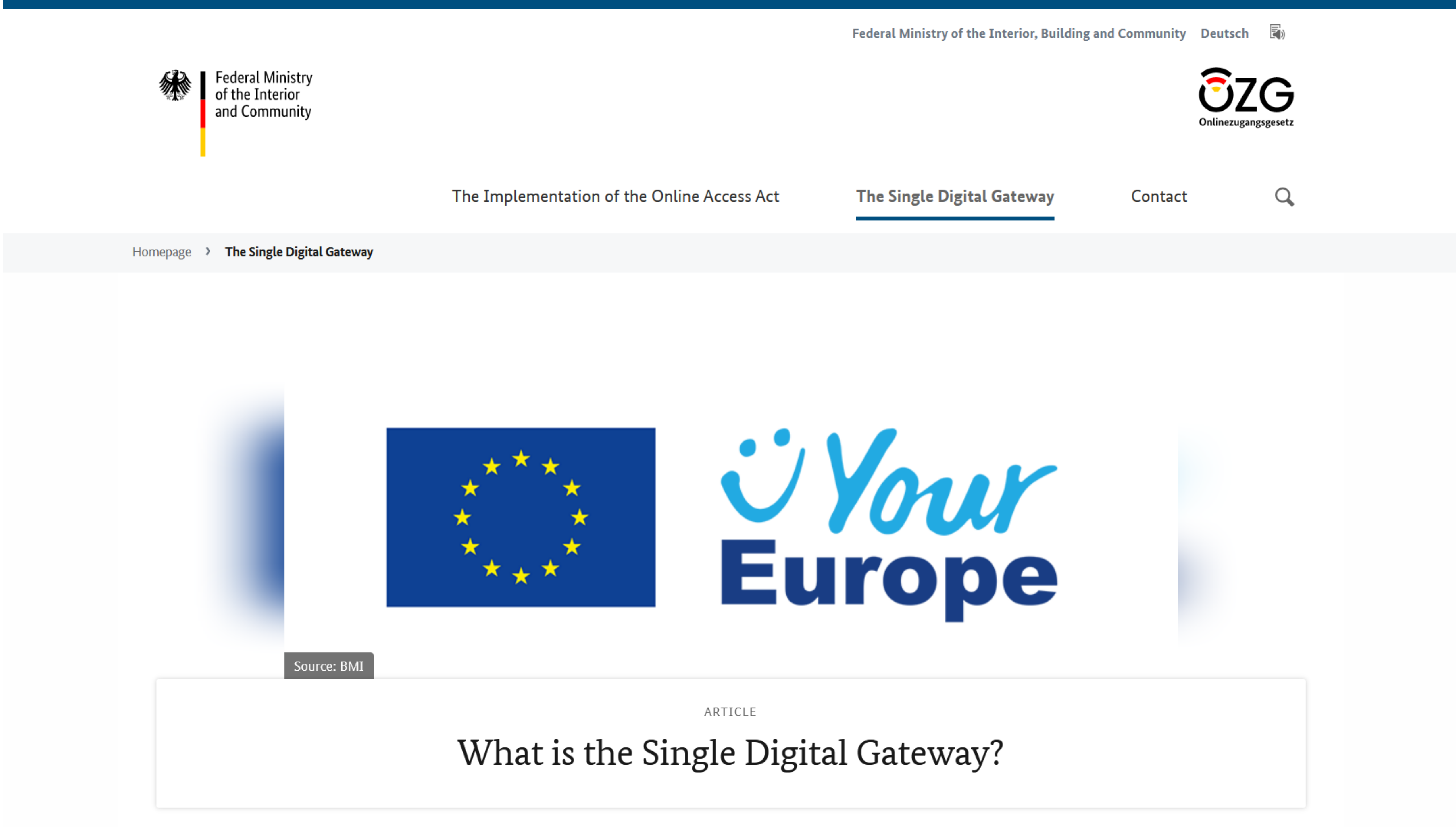
DISCLAIMER:
I AM NOT A LAWYER !

EGOVERNMENT
EJUSTICE

PD Estimate
AERIAL
Incomplete PP
Police Report
Estimate USAA
DL

MASONIC
DE
MASONIC
I-K
MASONIC
L
MASONIC
M-Ma
MASONIC
R
MASONIC
S-Sh
MASONIC
Si-Sy
GENERAL
Ar - Bar
GENERAL

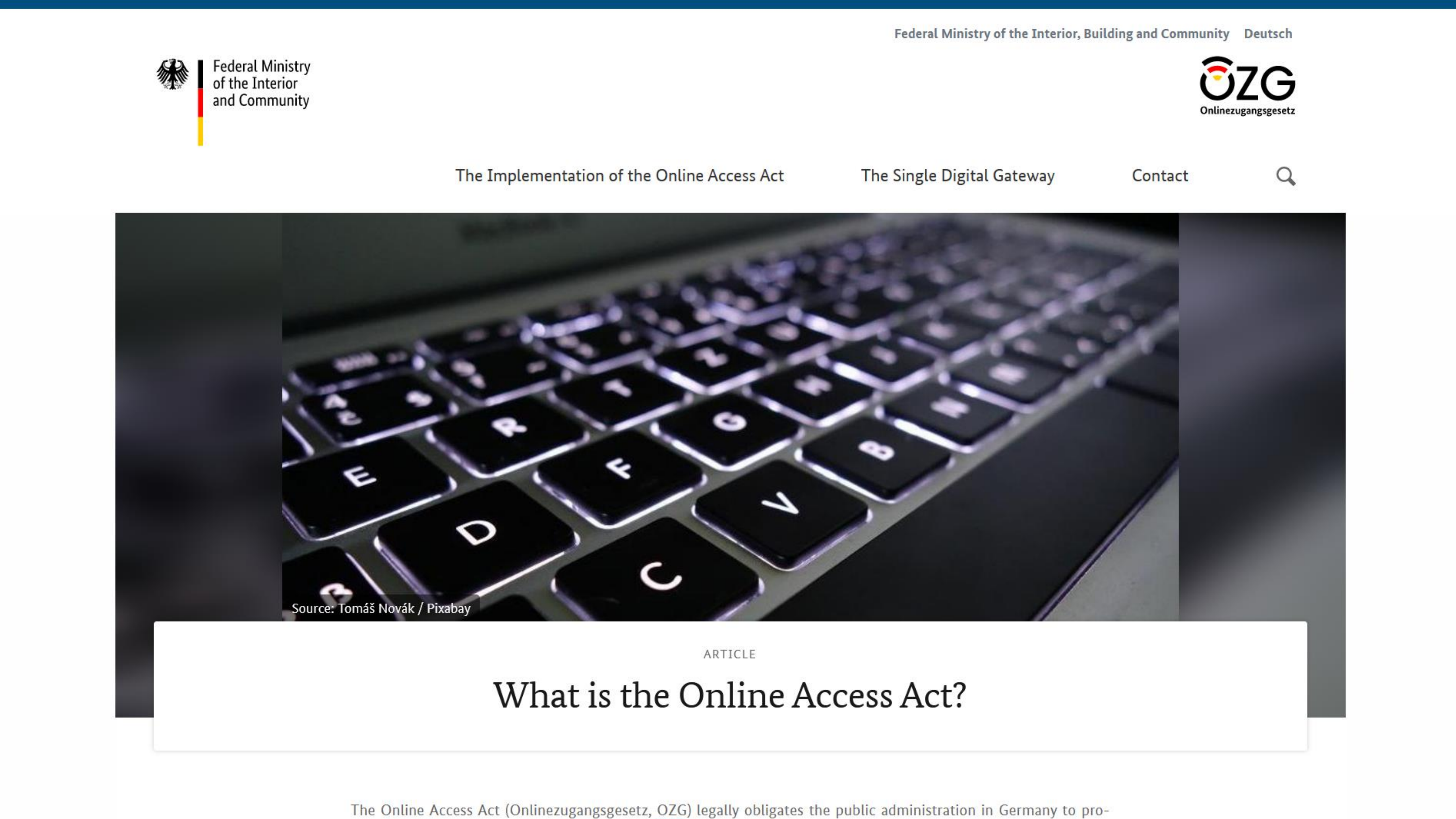
July
Mis Gortheren
Cornwall Wildlife Trust
GHTON
ROCK
GRAHAM
GREENE
ALAMEDA
Remittance Advice



Source: BMI

ARTICLE

What is the Single Digital Gateway?



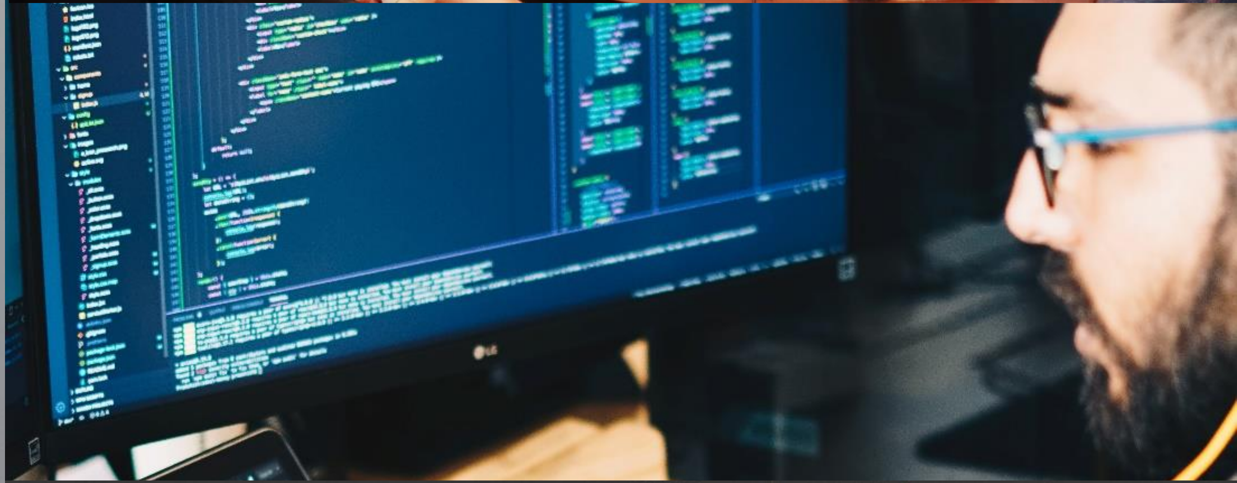
Source: Tomáš Novák / Pixabay

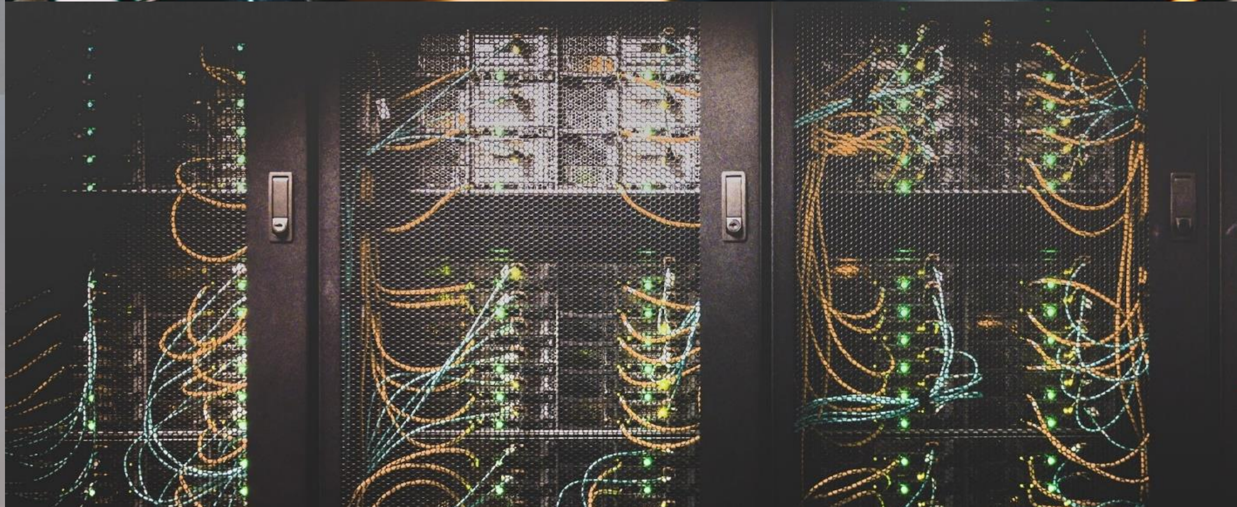
ARTICLE

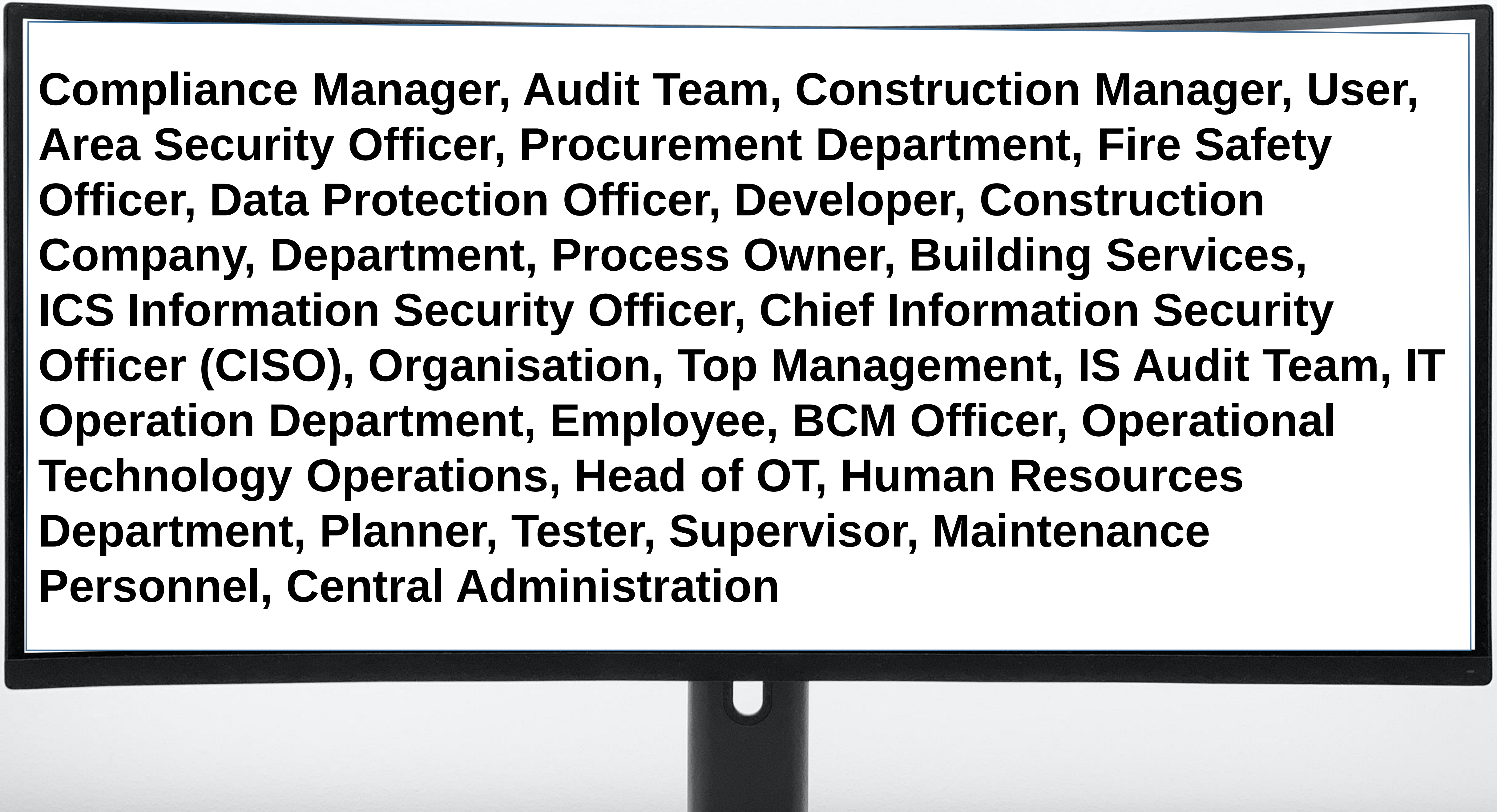
What is the Online Access Act?

The Online Access Act (Onlinezugangsgesetz, OZG) legally obligates the public administration in Germany to pro-

Q2
Activity log
Rights management
Improve in-app onboarding
Improve Trello integration
mobile App
Build NPS survey
Launch new website





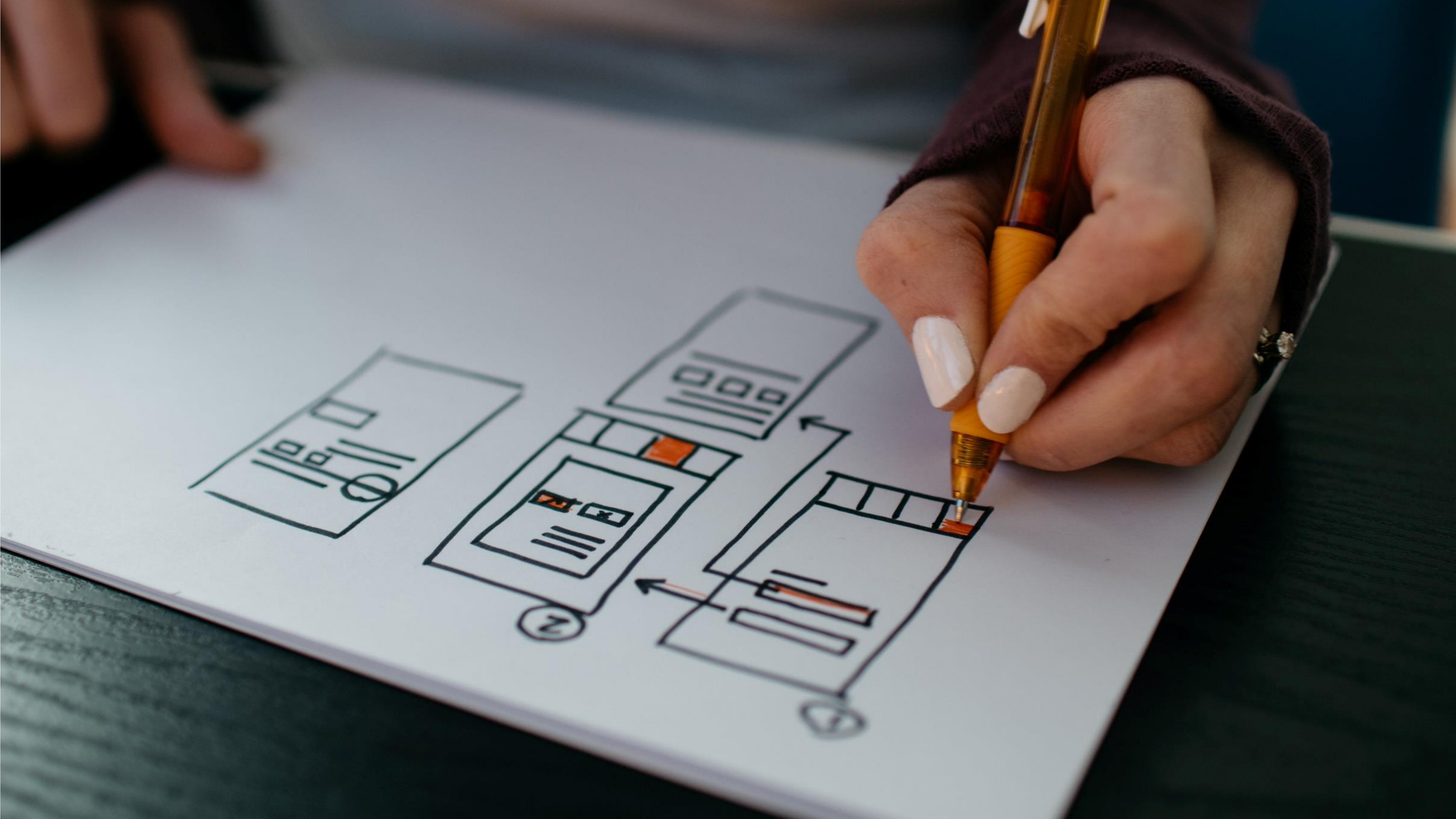


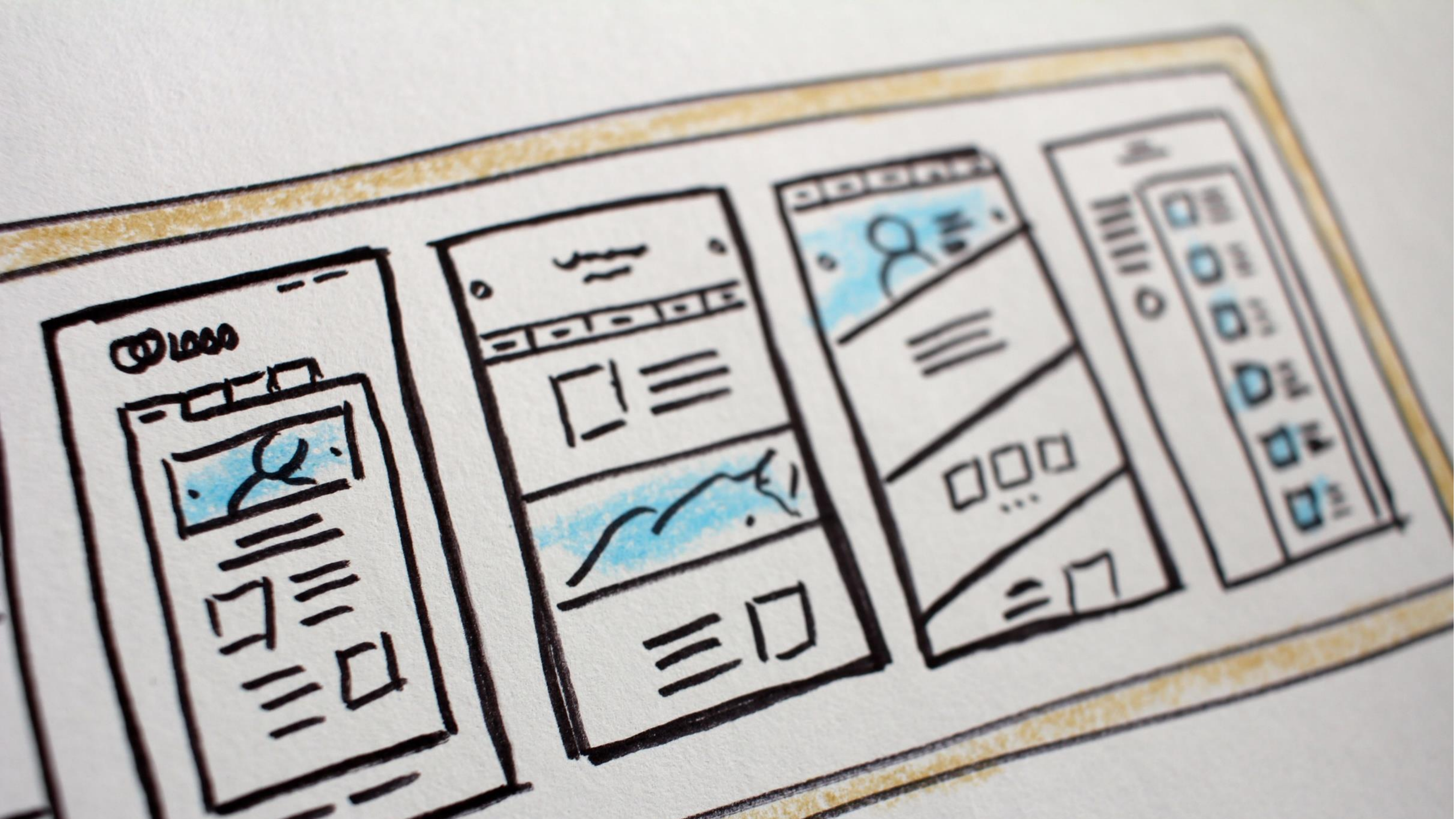
Compliance Manager, Audit Team, Construction Manager, User, Area Security Officer, Procurement Department, Fire Safety Officer, Data Protection Officer, Developer, Construction Company, Department, Process Owner, Building Services, ICS Information Security Officer, Chief Information Security Officer (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

3

Development Made Easy: HubSpot Design Tools

Story
To Do
IN Progress
Done
Goals
·Create Proof Data Mart
& Corresponding API
·MVP - Connect API to existing data to ... what we know about person today.
Backlog
MVP Data Store
CI/CD


2
1


LOGO

HARDENED

Federal Office
for Information Security

IT-Grundschutz-Compendium

Final Draft, 1 February 2022

https://bsi.bund.de/grundschutz --> English

Federal Office
for Information Security

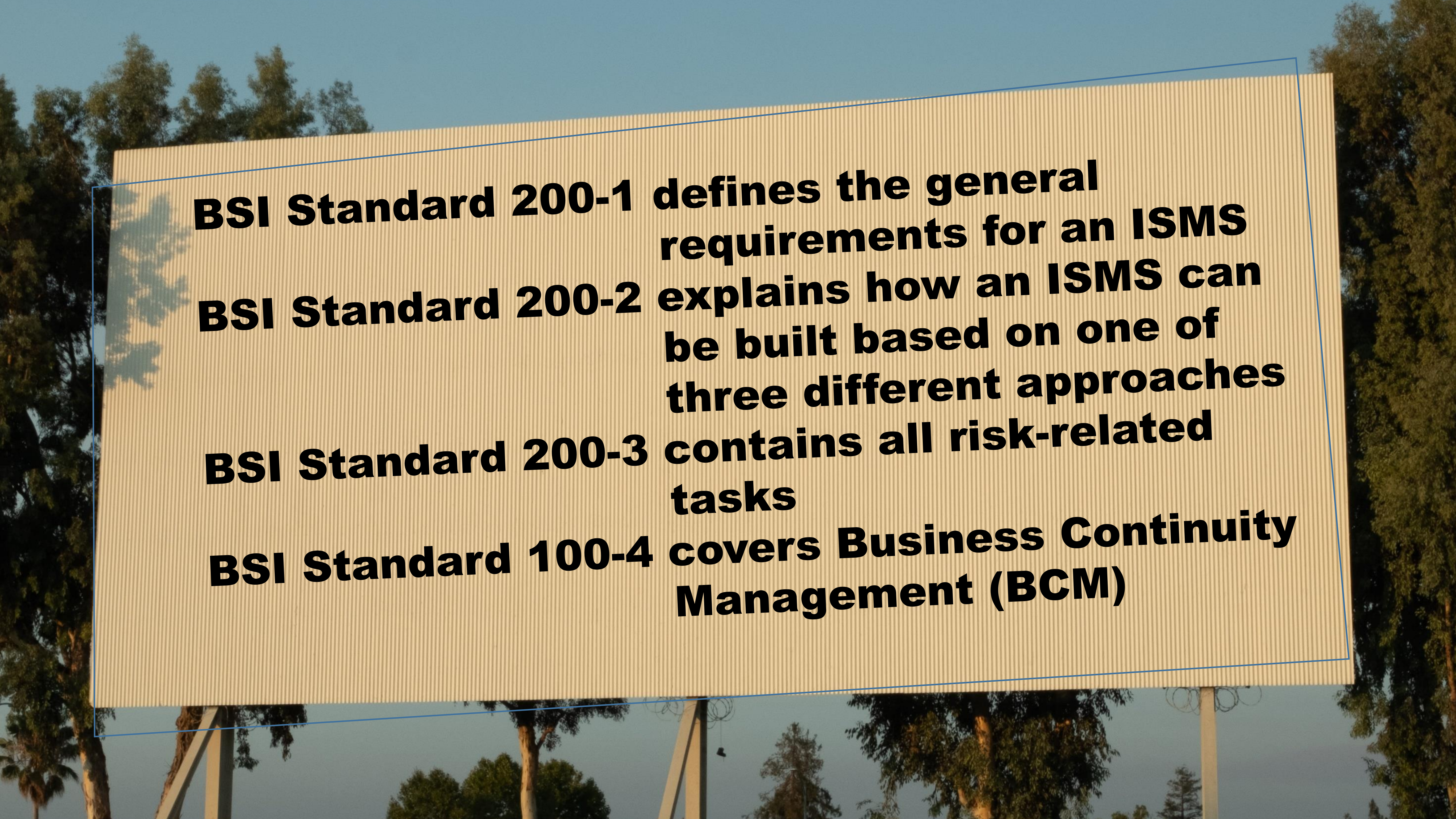
IT-Grundschutz Online Course

Print version

Last update: 07.08.2018

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

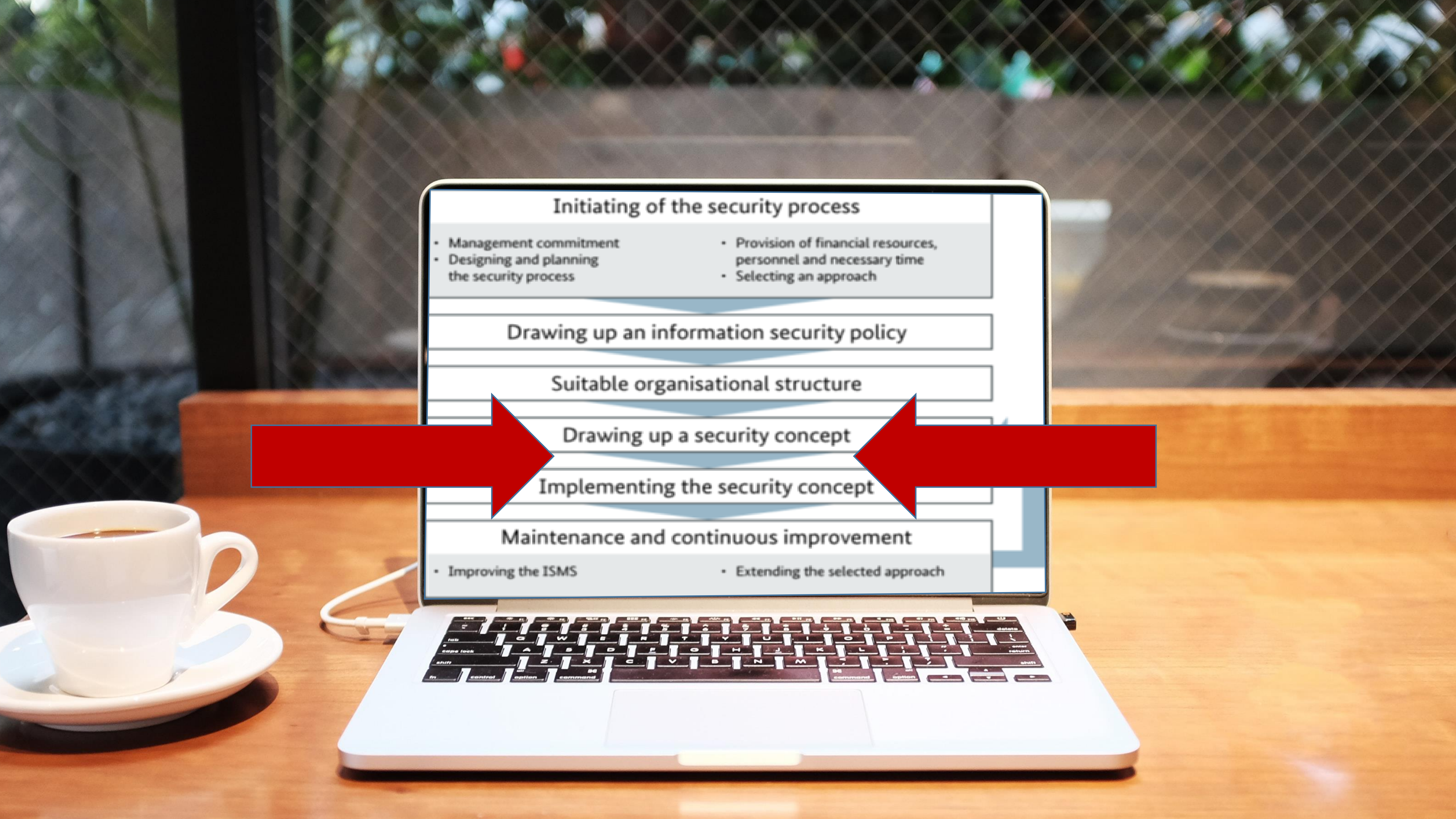


BSI Standard 200-1 defines the general requirements for an ISMS

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

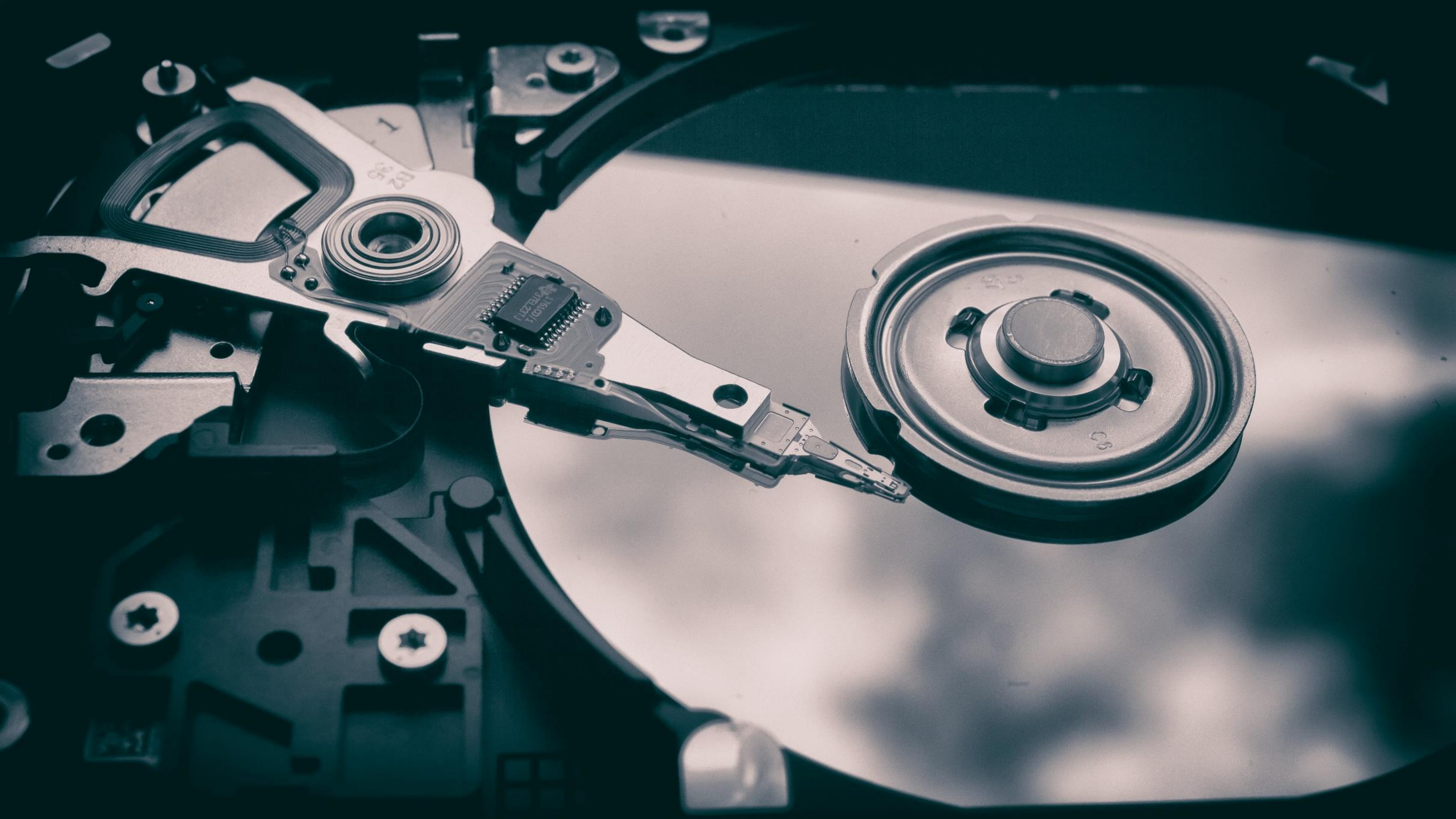
Implementing the security concept

Maintenance and continuous improvement

- Improving the ISMS
- Extending the selected approach

GOOD VIBES ONLY
WHAT IS YOUR STORY?

Feedback
Danke!
Proversion
$9⁹⁹
Kaufen
Feedback
Verkauf
Infos +



3

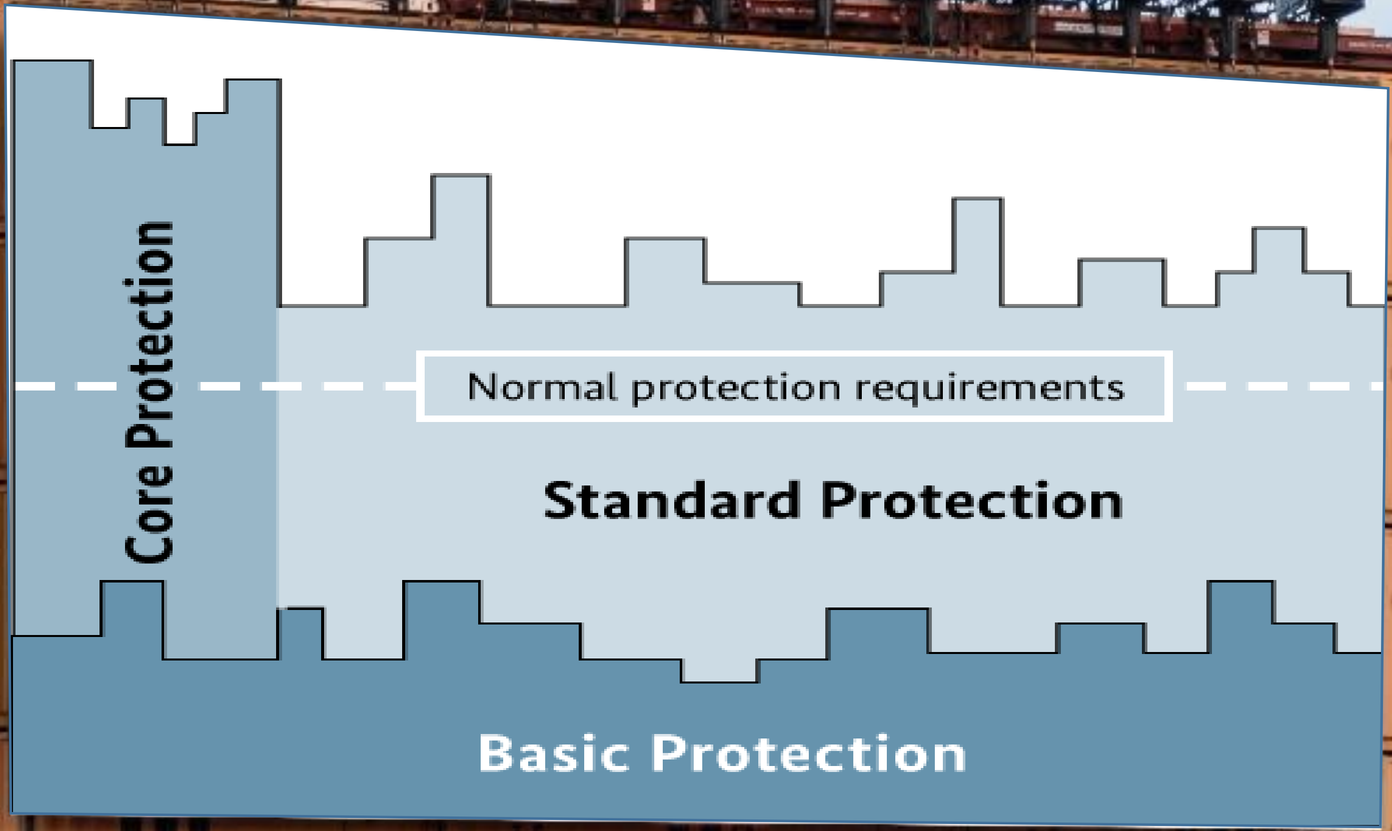
Holy Trinity

- Loss of Availability

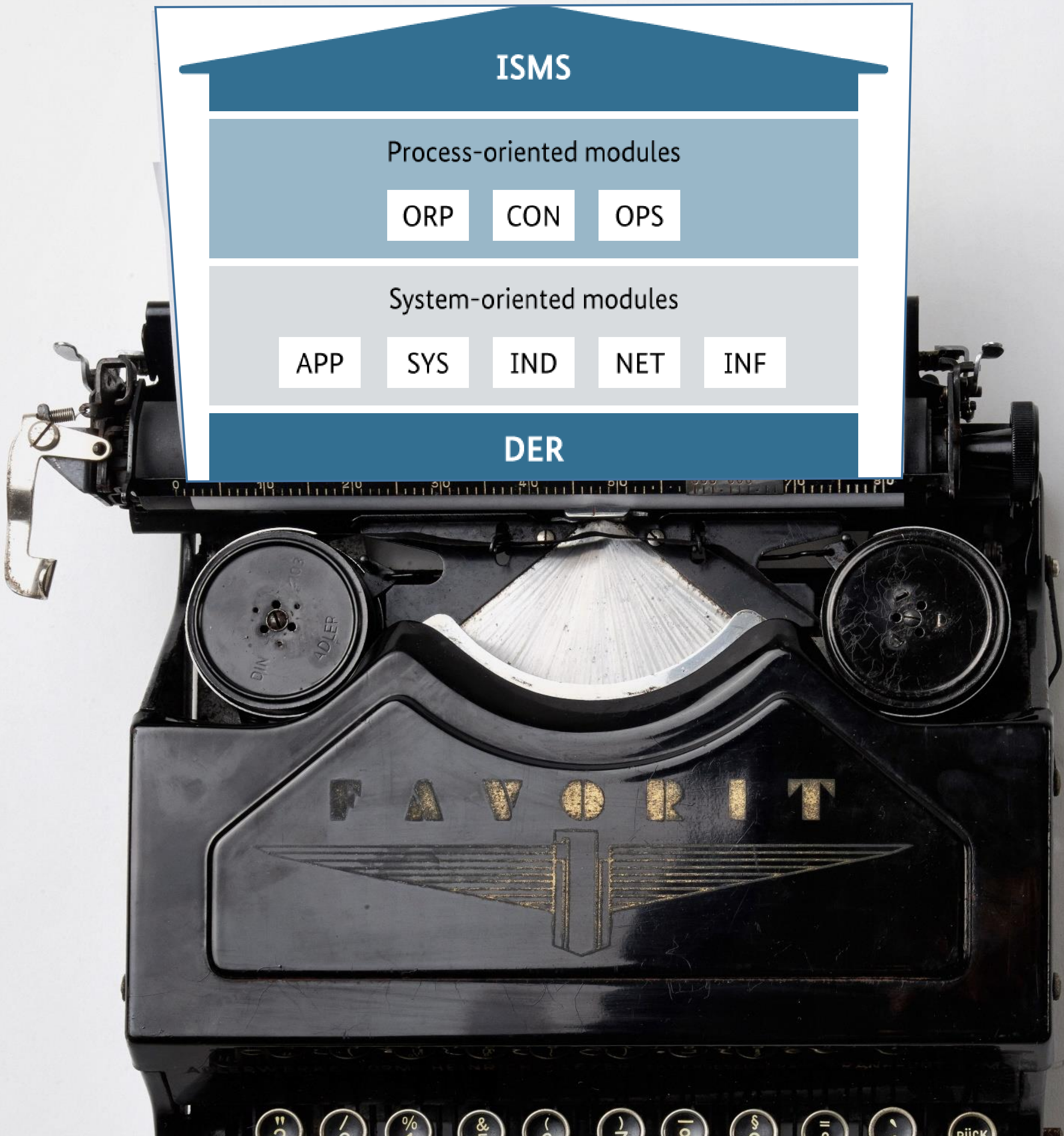
- Loss of Confidentiality of Information

- Loss of Integrity
  (Correctness of Information)

d's first major Nudie
achelor
rom
eping
3



- Basic Requirement
- Standard Requirement
- Requirement in Case of Increased Protection Needs



ISMS

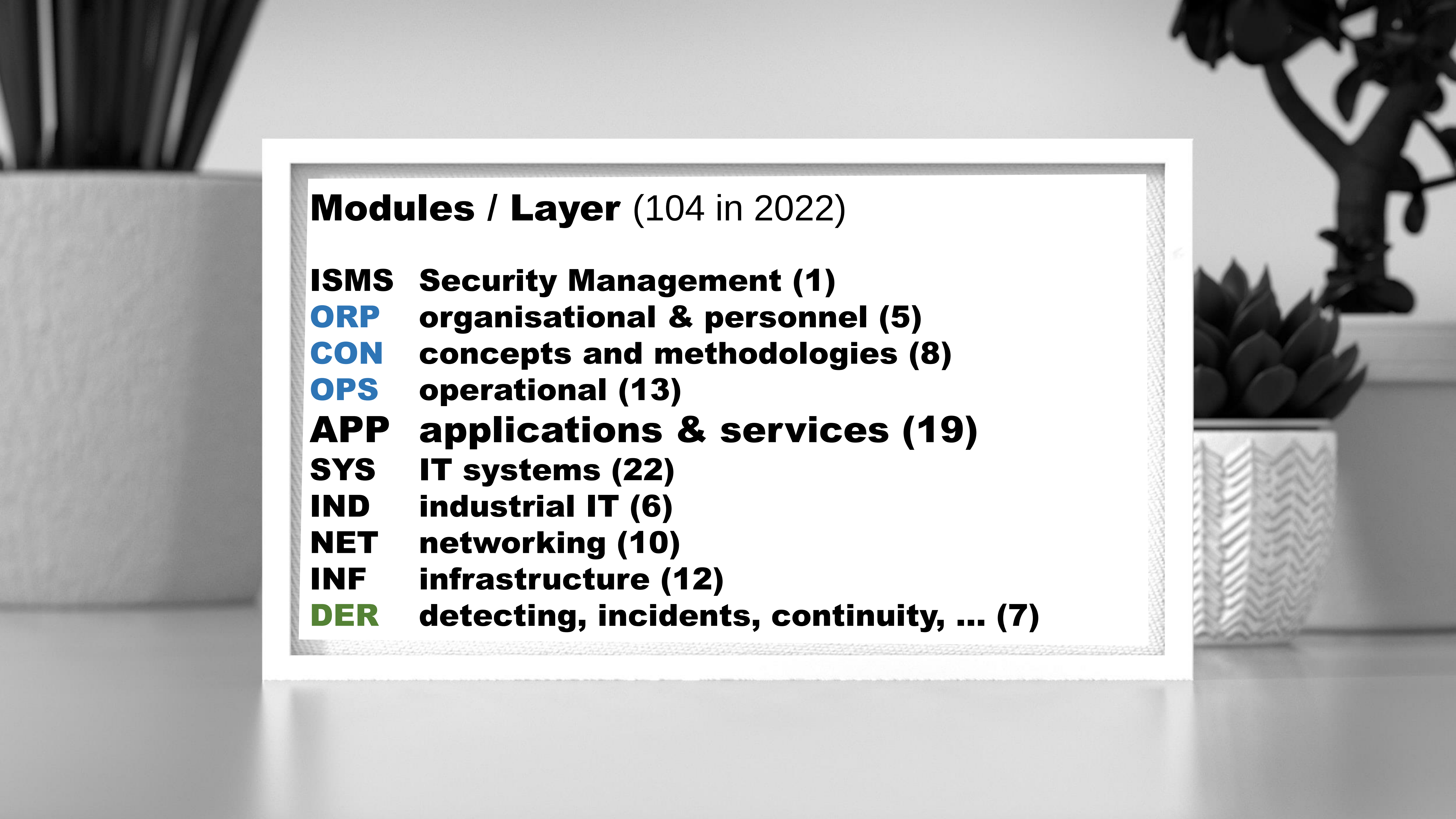
Process-oriented modules

ORP CON OPS

System-oriented modules

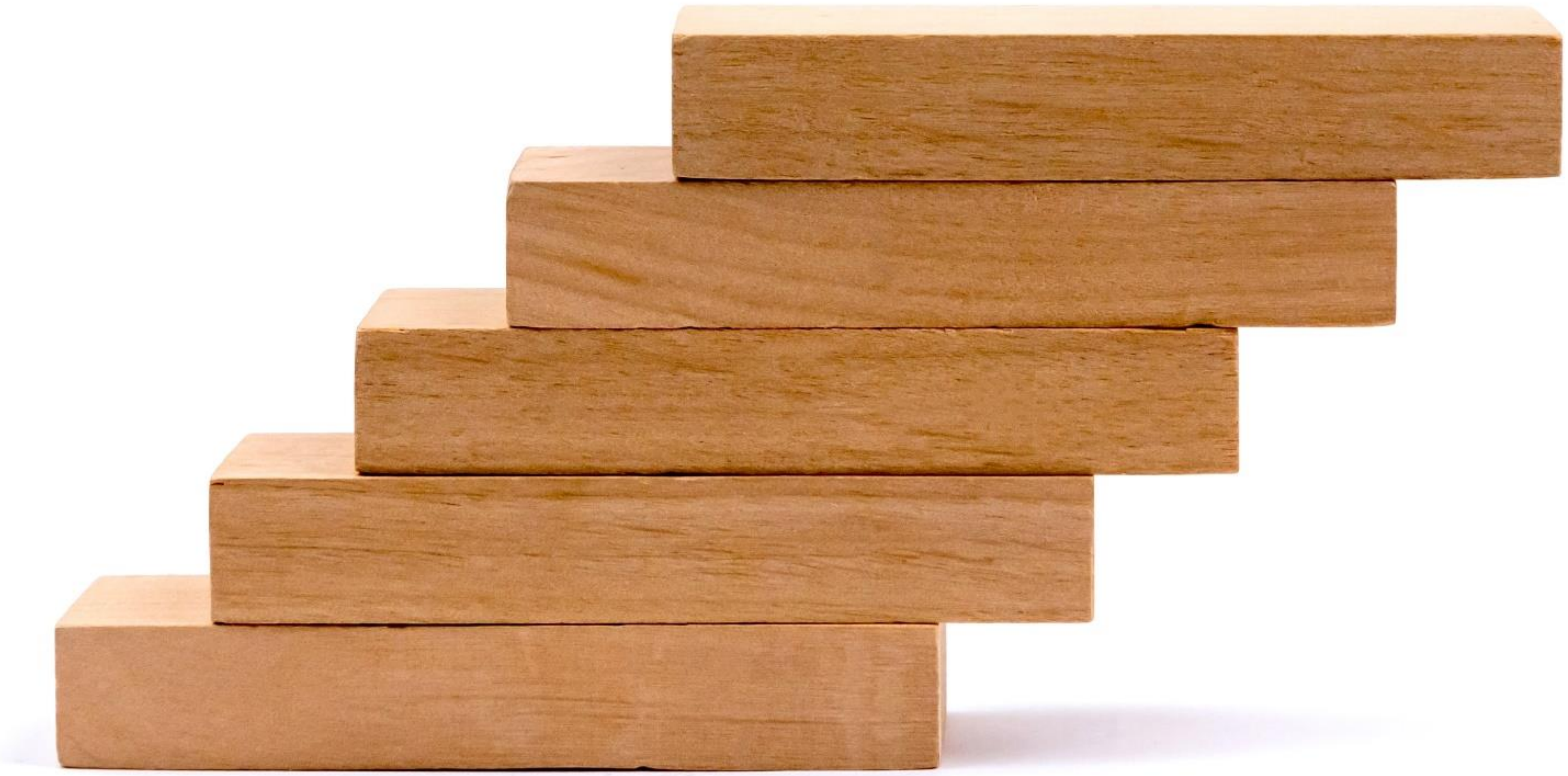
APP SYS IND NET INF

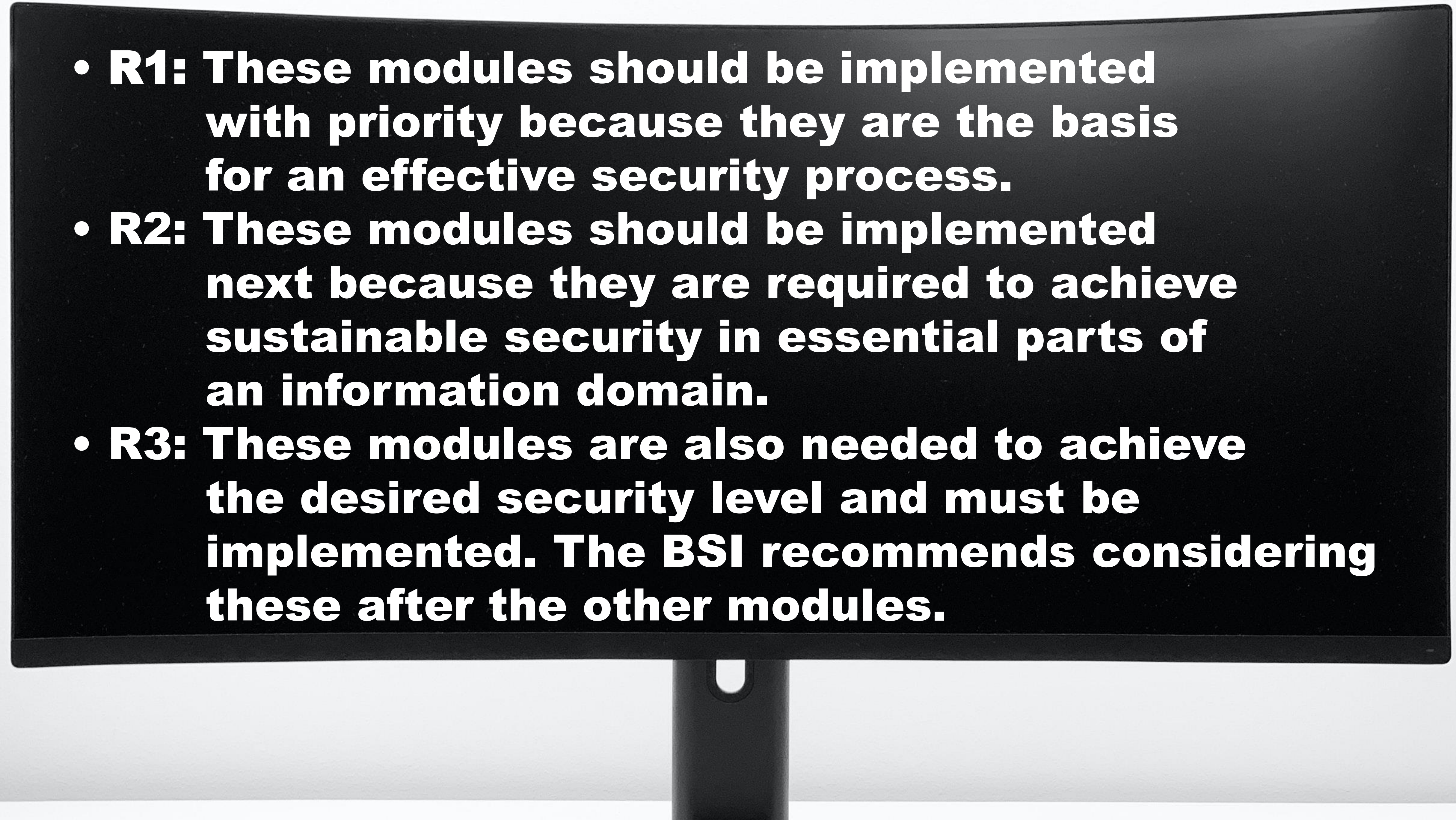
DER



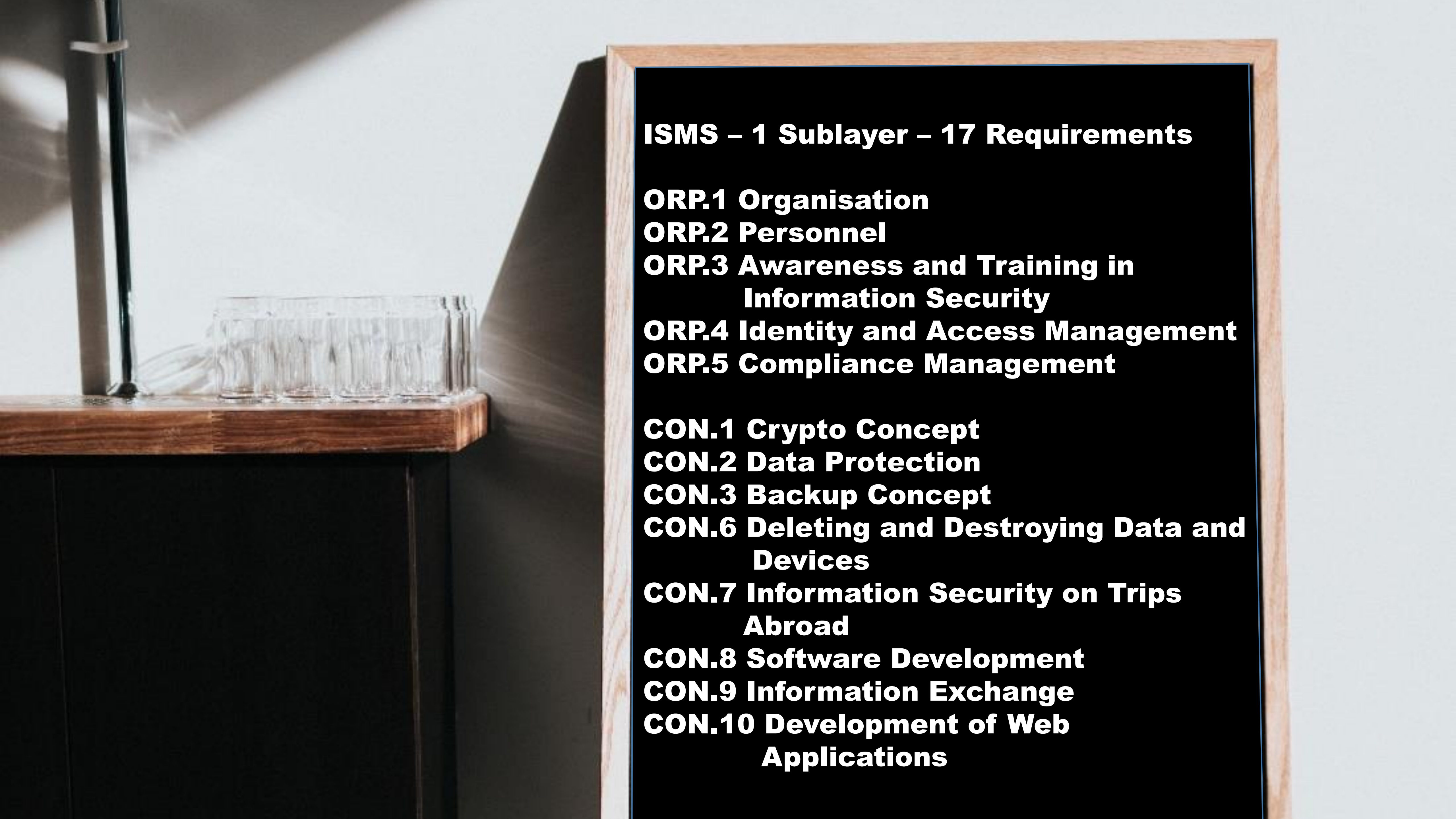
Modules / Layer (104 in 2022)

ISMS	**Security Management (1)**
ORP	**organisational & personnel (5)**
CON	**concepts and methodologies (8)**
OPS	**operational (13)**
APP	**applications & services (19)**
SYS	**IT systems (22)**
IND	**industrial IT (6)**
NET	**networking (10)**
INF	**infrastructure (12)**
DER	**detecting, incidents, continuity, … (7)**





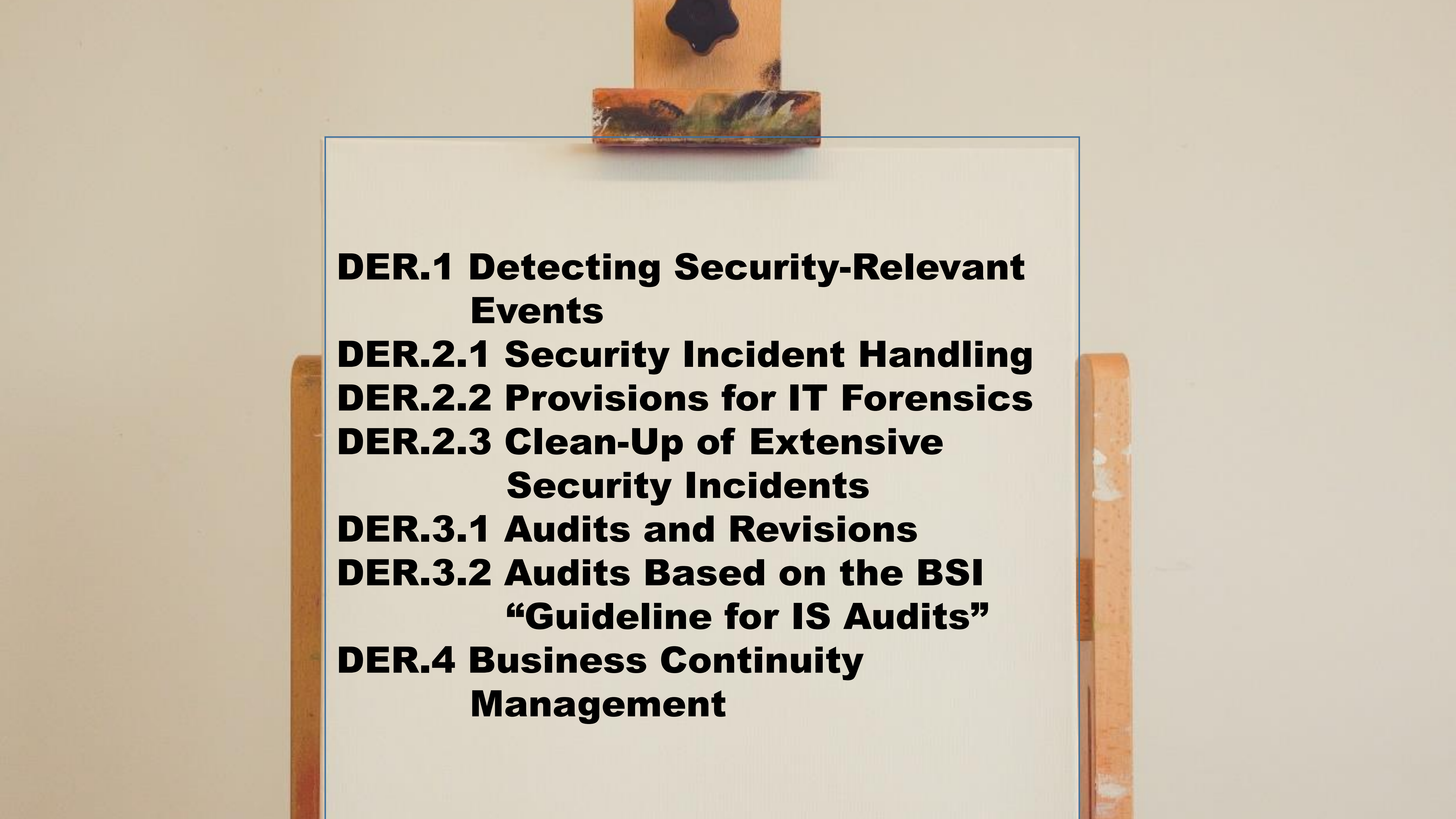
- R1: These modules should be implemented with priority because they are the basis for an effective security process.
- R2: These modules should be implemented next because they are required to achieve sustainable security in essential parts of an information domain.
- R3: These modules are also needed 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

Sublayer

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)

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

Requirements

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)

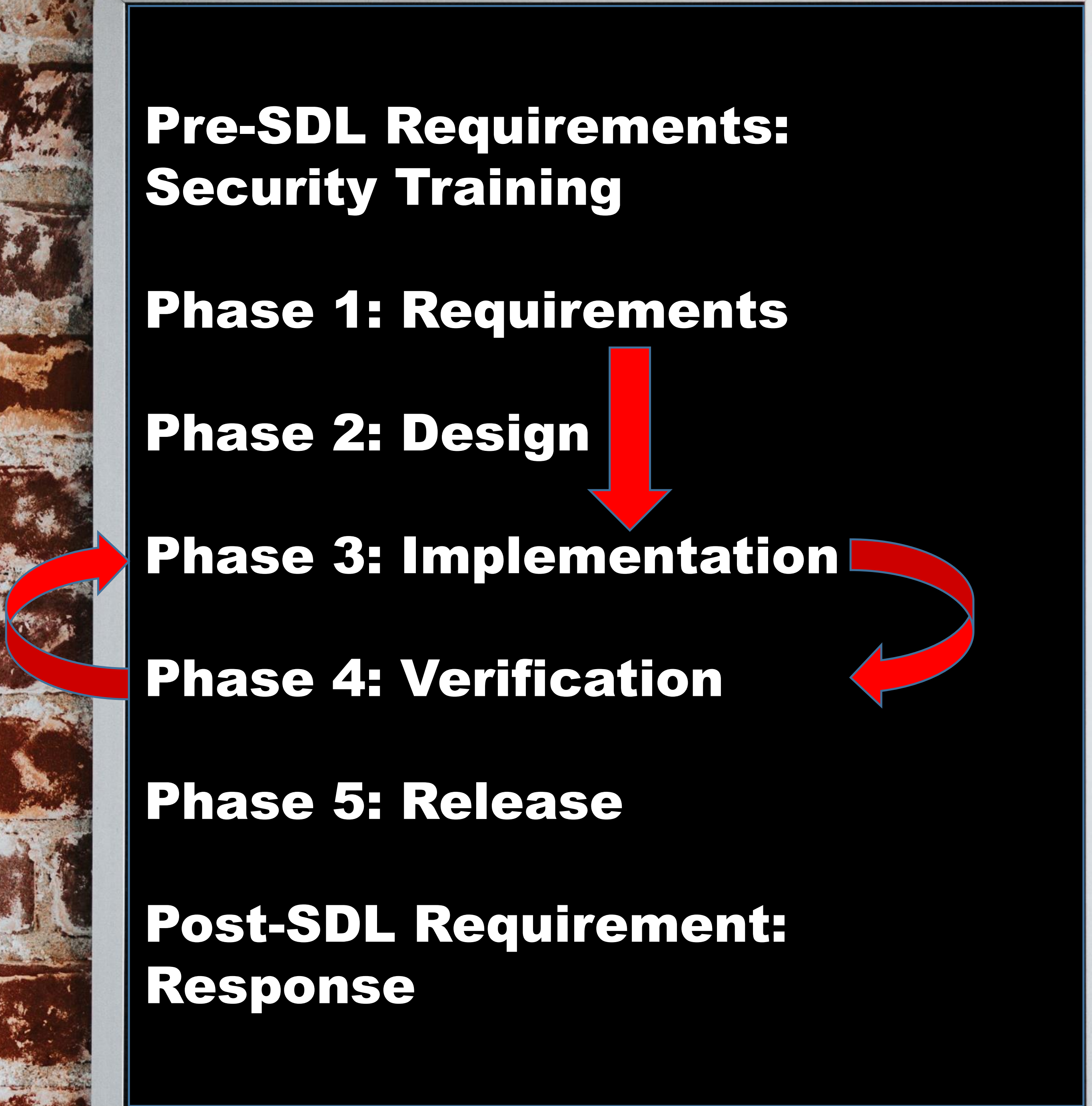
…

Requirements in Case of Increased Protection Needs

APP.7.A9 Trusted Storage (H)

APP.7.A10 Commissioning Certified Software Development Companies (H)

Implementation Guidance →
APP.7.**M**10



Pre-SDL Requirements:
Security Training

Phase 1: Requirements

Phase 2: Design

Phase 3: Implementation

Phase 4: Verification

Phase 5: Release

Post-SDL Requirement:
Response

INFO

Proof
ALL HANDS
4/24/2019
WIN
ANNAPOLIS, MD
#CUSTOMER OBSESSED
HUNGRY
YOU
SMART
HUMBLE
BRAZOS
80

YOUR STORY

H1-H6 Design
Video Module
Homepage
H1
H2
Email
Download
H1-Headline
Menu

REQUIREMENTS

Done
Doing
To Do

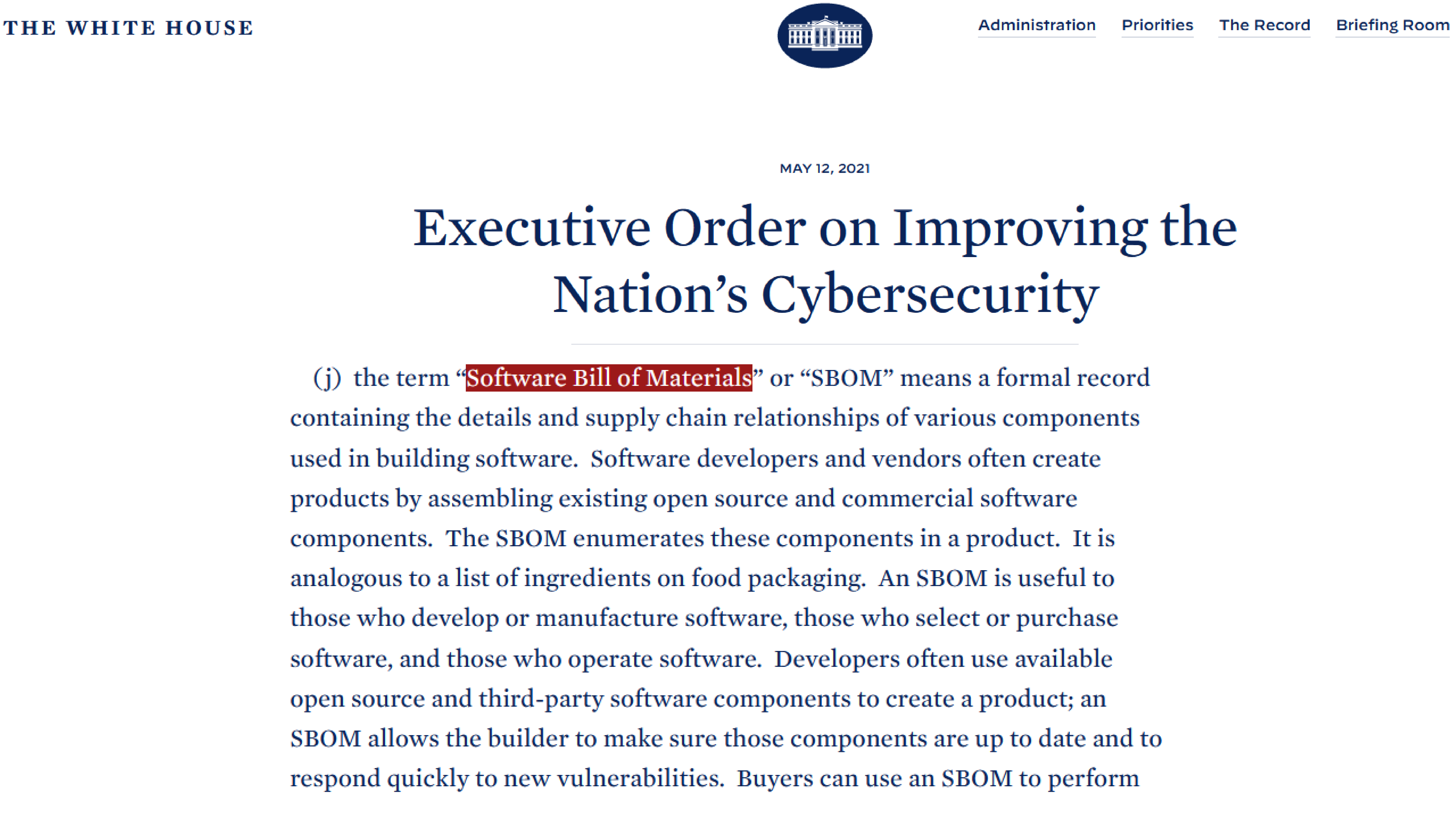
get_users_payload.js
get_tweets_payload.py
get-user.js
get-tweet.js
LABS-SAMPLE-CODE
.github
Tweets_and_Users
get_tweets_payload.js
get_tweets_payload.py
get_tweets_payload.rb
get_tweets_sample.js
get_tweets_sample.py
get_users_payload.js
get_users_payload.py
get_users_payload.rb
get_users_sample.js
get_users_sample.py
README.md
NORMAL

Welcome to website
Home

P 3
R 1 I 1
O 1 R 1 I 1
T 1 I 1 S 1 E 1

TESTING

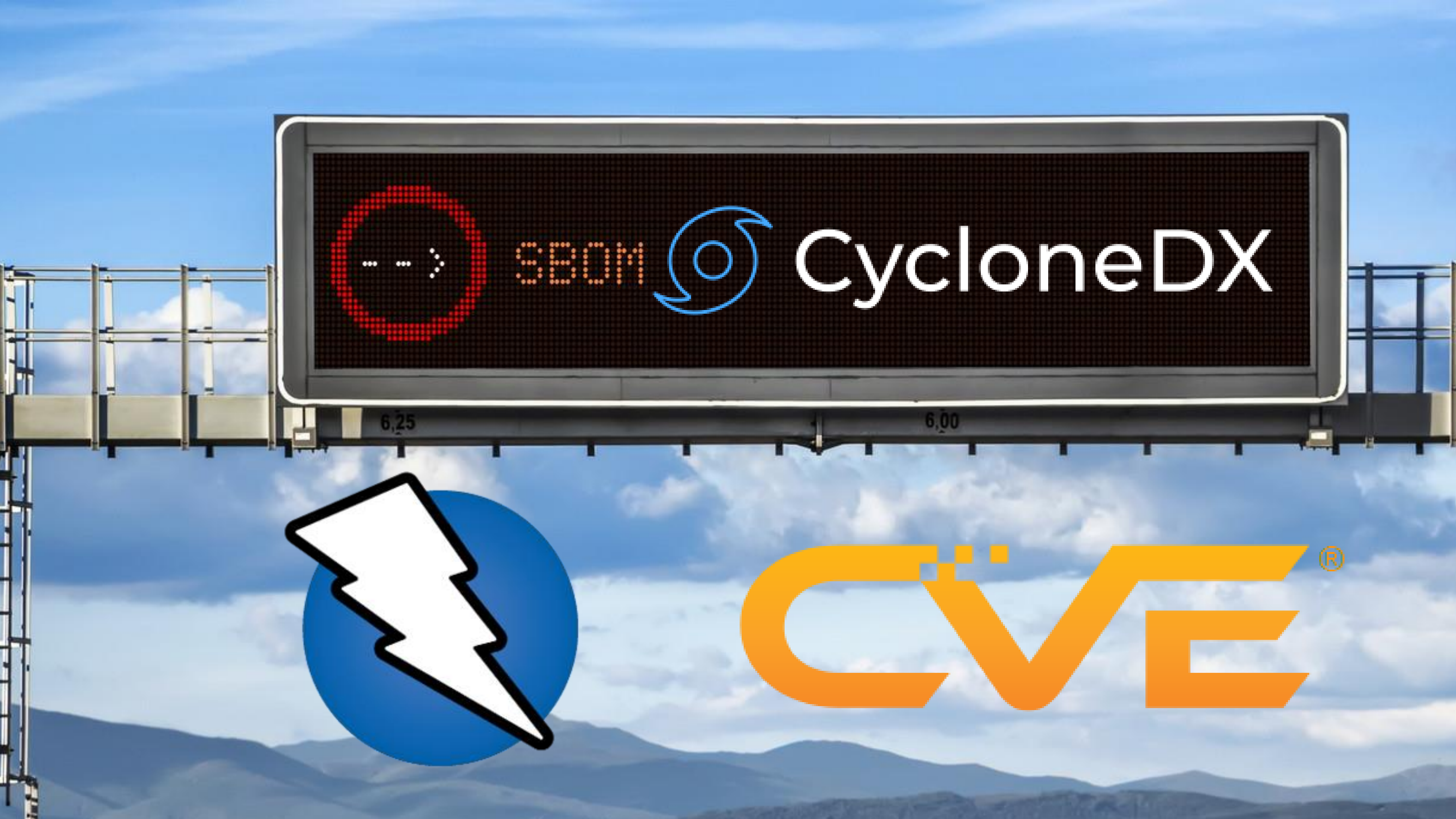
IMPLEMENTATION

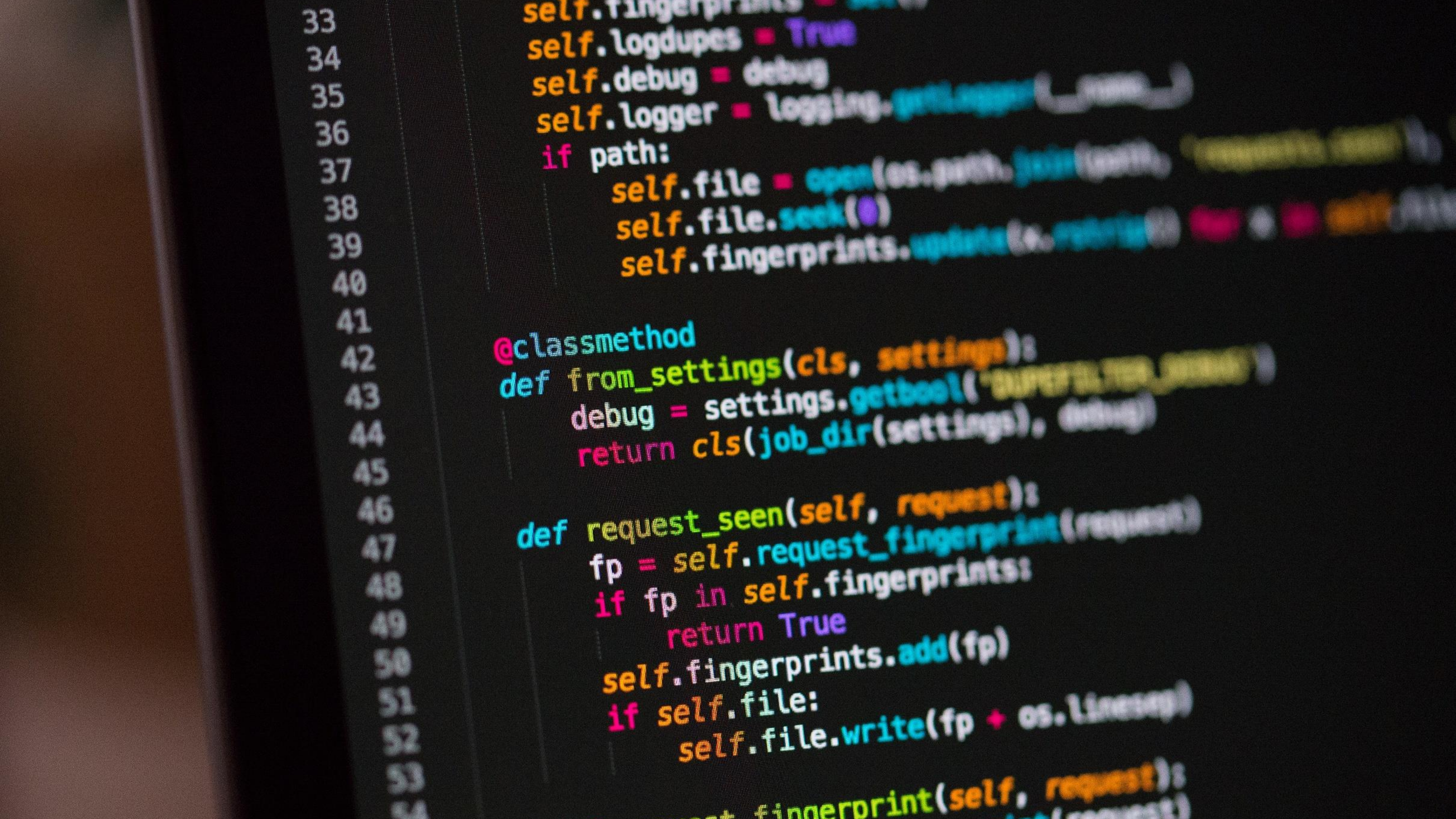


MAY 12, 2021

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


SBOM
CycloneDX
6,25
6,00
CVE



```
        self.fingerprints = set()
        self.logdupes = True
        self.debug = debug
        self.logger = logging.getLogger(__name__)
        if path:
            self.file = open(os.path.join(path, 'requests.seen'), 'a+')
            self.file.seek(0)
            self.fingerprints.update(x.rstrip() for x in self.file)

    @classmethod
    def from_settings(cls, settings):
        debug = settings.getbool('DUPEFILTER_DEBUG')
        return cls(job_dir(settings), debug)

    def request_seen(self, request):
        fp = self.request_fingerprint(request)
        if fp in self.fingerprints:
            return True
        self.fingerprints.add(fp)
        if self.file:
            self.file.write(fp + os.linesep)

    def request_fingerprint(self, request):
```

msc
tex
msc
msc
msc
msc
CAPITAL
TAL

Crisis

To do

Testing

Done

FINISH

2

url
Bios
EVENT
content
Demo
Input Box

1056
F1479
F1378

geprüft:
sachlich:
rechnerisch:
Abschnitt 1
§ 27
§ 28
§ 29
§ 30
§ 31
§ 32

USA
NASA
Challenger

OWN
YOUR
ERROR

Change

ONE WAY

CVE®

Shit
-HAPPENS-

HAPPY NEW YEAR

NEW YEAR
Resolutions

Project Title
Project Owners
Elizabeth Smith
Assigned Project Manager
James Regan
Assigned Talent
Latest Activity
Creative Director
Graphic Designer
Digital Marketer
SEO Specialist
SAMSUNG

TO DO LIST

END
PLEASE HELP PREVENT EROSION

Thank
you!