CYBERDISE

Cyber Awareness Playbook (CAP)

Version 3.0.3

Sep-14th-2026

1 Management Summary 2

2 Introduction 2

3 Scope, Plan, Run, Evolve - Overview of the CAP phases 4

3.1 Scoping the Awareness Program 5

3.2 Plan the Program and its Campaigns 7

3.3 Run Campaigns 9

3.4 Evolve the IT-Security Awareness Program 11

4 One level deeper - frameworks for Testing & Training Content 12

4.1 Testing Content Roadmap 12

4.2 Training Content Roadmap 13

4.2.1 Mandatory Security Education 13

4.2.2 Generic Security Trainings 13

5 Additions 15

5.1 Infrastructure for Testing and Attack Simulations 15

5.2 Training Infrastructure (LMS) 16

5.3 Gamification 16

6 Small or large project? 17

7 Relation to Cybersecurity Frameworks 17

7.1 NIST CSF 2.0 Coverage 18

7.2 Complementarity with NIST SP 800-50 Rev.1 (CPLP) 19

7.3 ISO/IEC 27001 20

7.4 Related Framework Summary 21

8 Change Control 21

1 Management Summary

Cyber Awareness Playbook CAP - This playbook provides a structured, experience-based framework for building and operating an effective cybersecurity awareness program focused on risk behavior reduction. Using the iterative phases Scope, Plan, Run, and Evolve, it enables organizations to design, execute, and continuously improve awareness initiatives in a measurable and sustainable way.

Purpose:

- Using CAP as a guide, IT security awareness is introduced in an organization.
- The organization benefits from the experience of other customers.
- The procedure is generally applicable and is not bound to any software or platform
- **CAP fills the operational awareness execution gap in the NIST documents**, especially in NIST CPLP[1]

Benefits:

- Structured, comprehensive approach.
- Decomposition of the overall task into manageable parts (Scope, Plan, Run, Evolve)
- Estimability of the project in the context of the organisation is made possible.
- A clean foundation for the success of security awareness is created

Related Foundation:

- The Cyber Awareness Playbook is an integral component of the overarching "Human Risk Engineering Framework".

This document and its content has been entirely human crafted.

2 Introduction

Using this best practice guide you will establish a successful awareness program. The CAP guide will help you with the implementation of the pre-project in your organization.

Corporate security cannot be guaranteed without IT security systems and hardware. Protective systems are getting better and better, so it is not surprising that today 47% of all cyber-attacks focus on the human factor and not the

[1] CPLP= NIST SP 800-50 Rev.1 (“Building a Cybersecurity and Privacy Learning Program”)

machine [1]. AI now outperforms humans when it comes to creating phishing emails [2], so criminal activity will continue to focus on employees.

For this reason, awareness measures for employees and programs to promote IT security awareness have become increasingly important.

Cybersecurity Awareness Programs are a proven methodology for improving risk behavior. Scientific studies have proven that properly implemented awareness improves user risk behavior by up to 60% [3].

[1] IBM Cost of Data Breach Report 2024, Fig. 7
[2] Heiding, F., Lermen, S., Kao, A., Schneier, B., & Vishwanath, A. (2024). Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects. arXiv:2412.00586 [cs.CR].
[3] Pugnetti, C., & Stacho, P. (2025). *Improving cyber risk behavior through AI-enabled spearphishing – A comparative analysis*. Lucerne School of Business (HSLU), Institute of Financial Services Zug (IFZ); Cyberdise AG.

Setting up Security Awareness Programs requires thinking like a hacker sometimes. With the Cybersecurity Awareness Playbook (CAP) we offer a modular guideline for building comprehensive cybercrime sensitization initiatives. The CAP guide allows an efficient implementation of a pre-project for the setup of an awareness program.

Its implementation stages such as 'Scope', 'Plan', 'Run' and 'Evolve' allows to cover all levels of the organization: normative, strategic and operational. This ensures the effectiveness of preventive measures in the cyber risk area effectively and sustainably.

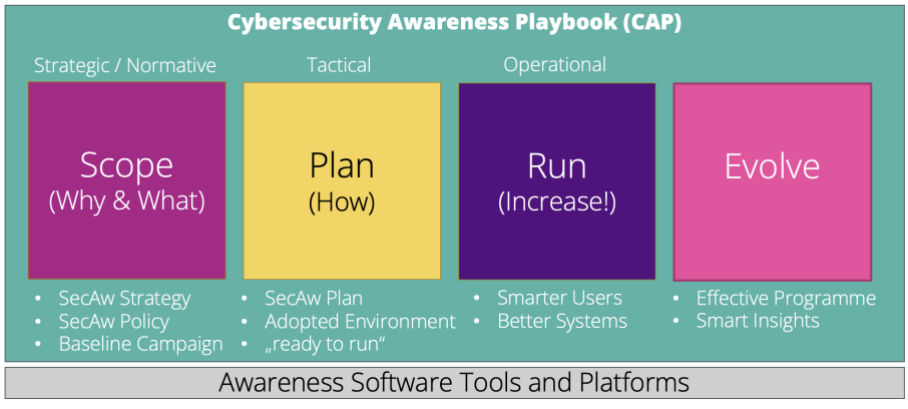


Figure 1: CAP Implementation Model

Scoping is about understanding the business context and making strategic decisions, defining the global anchor points and conducting an initial baseline for phishing and training campaign to determine where the company stands. The

results are a security awareness policy, a security awareness strategy (-year plan) and the results of the basic campaign.

Planning is all about creating a master plan for security awareness. What should be tested, trained and in what order. Which phishing simulations will be used? Which training contents must be imperatively taught and which general IT security topics do you want to train? The results are a conducted mail and web filter analysis (what goes through?), roadmaps for the testing content and the training content, a campaign plan and an established awareness training infrastructure.

The **RUN** phase basically refers to the individual campaign. What needs to be considered when preparing a single awareness campaign with your attack scenarios and training? The **EVOLVE** phase ultimately serves to ensure that the employee awareness program retains its effect on the staff, improves and that further insights are gained.

The documentation of the framework includes a description of the individual processes necessary to build a cyber sensitization / awareness program. The documentation is provided free of charge by securityawarenesss.guru. Please contact us using the following form if you wish to get a detailed handbook.

3 Scope, Plan, Run, Evolve - Overview of the CAP phases

Please note: The phases are overlapping. This is not a waterfall model.

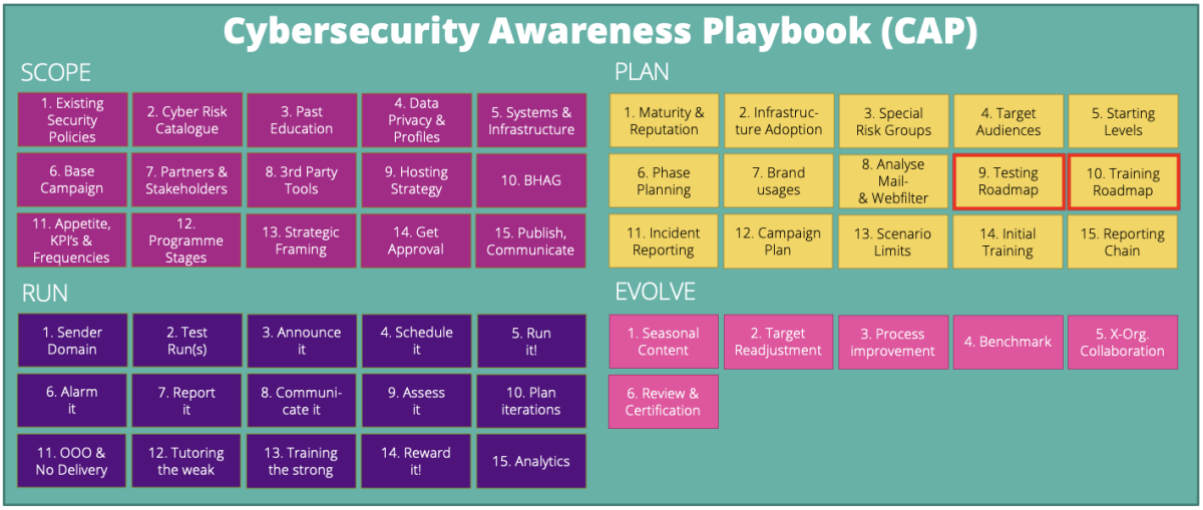


Figure 2: CAP Implementation Breakdown

3.1 Scoping the Awareness Program

Level: Strategic - Normative
Goal: Why and What
Outcome: Sec-Awareness-Strategy, Sec-Awareness-Policy, Baseline Campaign

Figure 3: CAP Phase 'Scope' and its activities

1. Understand your existing security policy framework (and risk appetite, if available) in the company. This drives what you need to test, to assess and to train. It also gives you an early answer what to measure.
2. Understand your courrent cyber risk catalogue. You need to train your staff along the attack vectors.
3. Understand past security education. You need to know where you want to start with the standardized education.
4. Understand your data privacy implications. Be mindful that you are gathering personal data. This is especially true if you want to create educational vulnerability profiles for your employees using OSINT.
5. Understand your technical infrastructure and systems. Knowledge on the technical components is important. You can never plan a successful phishing program until you know and understand all the technical information involved. Example: It does not make sense to run a drop-box phishing simulation when drop box access is denied by your systems.
6. Perform immediate actions: Run Baseline Training and Test (in order to identify special flaws in and identify state of knowledge). Yes, run your first phishing and training campaign already in the scoping phase. And don't forget to plan pilot runs, many organizations face challenges with whitelisting the environment for their awareness campaigns.

7. Discover your stakeholders, supporters and influencing units (System Engineering, Management, HR, SOC, CSIRT, Work Council, Helpdesk, etc.)
8. Investigate dependencies and interfaces to 3rd party tools.
9. Define hosting strategy for the security awareness systems. Do you want to a software on your own premises, on your own cloud servers, do you want to use 3rd party providers or a hosting provided by a awareness platform provider?
10. Define global goals for the program (BHAG), desired click rates, training completion rates, incident rates.
11. Define your risk appetite depending on your certifications, regulatory needs, legal obligations, financial stability, operations, andor reputation. Define KPI's that matter and desired training frequencies, training lengths, etc. (also relate to your risk appetite)
12. Define global stages of the program. Don't try to address everything in one giant leap.
13. Strategic Framing. This might be multiple documents or a single policy. Write down a
    i. Overall strategy (two-to-three-year plan, don't go into details. If 2 years are too long, choose 18 months) and awareness program policy (The findings, definitions and decisions you made in this phase, also reflecting your risk appetite).
    ii. Also explain any disciplinary measures for repeat offenders and who is responsible for dealing with these users and their treatment/special education
    iii. Think about a supporting communication strategy (how to support the behavioral change, informing about campaign results, fun facts, storytelling etc. Also define if and how often the stakeholder groups must be informed, updated.

    These documents need not be large! Often one page or two is enough and the content can be integrated into existing policy documents.
14. Get approval from the management, human resources, workers councils and other governance units if needed.
15. Publish and communicate your awareness program policy document and the strategy document.

3.2 Plan the Program and its Campaigns

Level: Tactical
Goal: How, in which order and when
Outcome: Sec-Awareness-Program-Plan, adopted environment, it's "ready to run"

Figure 4: CAP Phase 'Plan' and its activities

1. Define Maturity Levels and Reputation Levels to be used in the tools.
2. Plan and implement infrastructural adoptions (Spam Filter, Whitelists, WAF, Firewalls).
3. Identify special risk groups. They will get dedicated campaigns and content.
4. Define target audiences (recipient groups).
5. Define starting levels of the tests and trainings. Do you want to start easy or already sophisticated?
6. Define phases of the program (phase planning). You can't train everything at once. It makes sense to set priorities and bundle certain topics.
7. Decide on brand usage. Attackers use well-known brands, companies, websites, etc. because they know that users are highly likely to click on them. Should your campaigns take this into account? You should also plan campaigns with your own faked or spoofed company name.
8. Whitelisting: Perform mail- and web filter analysis. Discover what is blocked. Run pilot campaigns to be sure that the campaigns will go through.
9. Create the exercise/testing content roadmap for your organization ('Attack content framework', see below). Have there been successful

social engineering attacks (phishing, smishing, business email compromise, etc.) in the company that should be prevented through better employee behavior? Are there attack scenarios that must be avoided at all costs and should therefore be practiced? Please note that real risk exposure in the form of attack simulations improves risk behavior most!

10. Create your training content roadmap ('Awareness content framework', see below). Be aware that trainings drive users risk attitude more than their behavior.
11. Plan empowerment of users in identifying and reporting threads. Define the reporting process together with support desk and SOC. Roll-out the Phishing Incident plugin and configure the 'incident console' within the given awareness plattform if needed.
12. Create a campaign plan (Campaign & Audience Planning) for the next 12-18 months.
13. Weigh the limits of any attack scenarios. Sometimes it may happen that you should run an attack simulation but the scenario you should use for it is a no-go. Are there any limitations in terms of scenarios/themes that cannot be used in attack simulations in your organization?
14. Carry out the initial training campaign in the sense of basic training. Before you initialize the awareness program and its first simulated phishing campaign in your organization, your current employees need to go through an introductory training scheme.
15. Setup the reporting and communication chain in the company. When running campaigns, who needs to be informed? Who gets the campaign results? What information is distributed?

And: Don't die in beauty!

3.3 Run Campaigns

Level: Operational, mostly single campaign
Goal: Increase awareness, knowledge and infrastructural quality
Outcome: Smarter employees and better systems

Figure 5: CAP Phase 'Run' and its activities

1. Sender Domain: An important part of your phishing attempt is choosing the right mail sender domain from which the phishing simulation emails will be sent out. Choose domain names that will normally pass through spam filters. If this is not the case you need to 'white label' them. Be aware that there isn't much sense in using domains that would normally get filtered out via SPF protection because these will never make it to your employees' inbox. Invitations to awareness trainings can easily be sent from the company's own domain.
2. Test run: Do a test run before firing the campaigns.
3. Announce it: Do you have to notify phishing campaigns to (official) bodies?
4. Schedule it. How many mails should be sent in which period of time? When should the training be sent? Immediately or after a time interval? Should phishing be sent randomly?
5. Run it: Make sure you can and do monitor it in real time in case something goes awry. Don't just do awareness training and phishing simulations. Also run 'Bad USB' or smishing campaigns.
6. Alarm it: The employees should use the Phishing Incident Button!
7. Report it: After the campaign create the report.
8. Communicate it. Publish the results. People are curious.
9. Assess it: Don't only test and train people. Run assessment campaigns using malware simulation toolkits available on the market. Perform

extended mail- and web filter tests. Assess the network using the ransomware simulator. So you can find out until what extend a malware would be successful in your network.

10. Campaign Iteration planning & execution: Often the results of the campaign indicate the need for follow-up training or the need for a follow-up campaign.
11. OOO / no delivery campaigns: Create more sophisticated campaigns by enabling response detection provided by the Awareness platform vendors. Create campaigns that automatically respond to auto-reply and out of office messages (ooo).
12. Tutoring the weak: Create special training for the weakest employees. Pay attention to small and short training modules. Respect all employees.
13. Special education for the strong: Do not allow your best and most attentive employees to slip away; they are your most important asset and your strongest defense.
14. Reward it! Create incentives through rewards, awards and competitions at employee and team level!
15. Analytics it! Compare campaign results, identify trends, and carry out benchmarks. Your organization is unique; comparisons with other organizations mostly make little sense.

3.4 Evolve the IT-Security Awareness Program

Level: Operational, tactical, strategic & normative
Goal: Improve staff, organization, partners and infrastructure
Outcome: More effective awareness program

Figure 6: CAP Phase 'Evolve' and its activities

1. Provide seasonal / actual content: Is there a current threat in the market or has a new security policy been published that requires training?
2. Target readjustment: Are the objectives still okay?
3. Process improvement. After a certain time you certainly can improve campaign preparation, reporting or alarming processes.
4. Benchmarking. Once you have a basic data set and results for your organization and its units set up a benchmarking framework and use the power of comparison and gamification.
5. Cross organizational collaboration. Start to share trainings and templates with other organizations. Perform cross company 'competitions'. It's here where you can start benchmarking. But beware! As already mentioned earlier, most external benchmarks make no sense, really. Your organization is unique and it's hard to compare it with others, especially for click rates and similar. BUILD YOUR OWN BENCHMARK HISTORY INSTEAD!
6. External Review & Certification. A review by an external body can certainly make sense.

4 One level deeper - frameworks for Testing & Training Content

The testing roadmap and training roadmap show what you want to test, train and practice. They serve as the basis for the campaign plan, in which the concrete awareness campaigns, goals and recipient groups are planned. These artefacts show the management and other interested recipient groups what learning content is to be conveyed in principle, without a time reference or detailed assignment to risk and recipient groups.

4.1 Testing Content Roadmap

Performing a phishing simulation in your own organization is nothing more than a realistic exercise to prepare for an emergency. Many companies conduct regular evacuation exercises of their office buildings. Educational social engineering measures such as fake phishing mails are virtually the same.

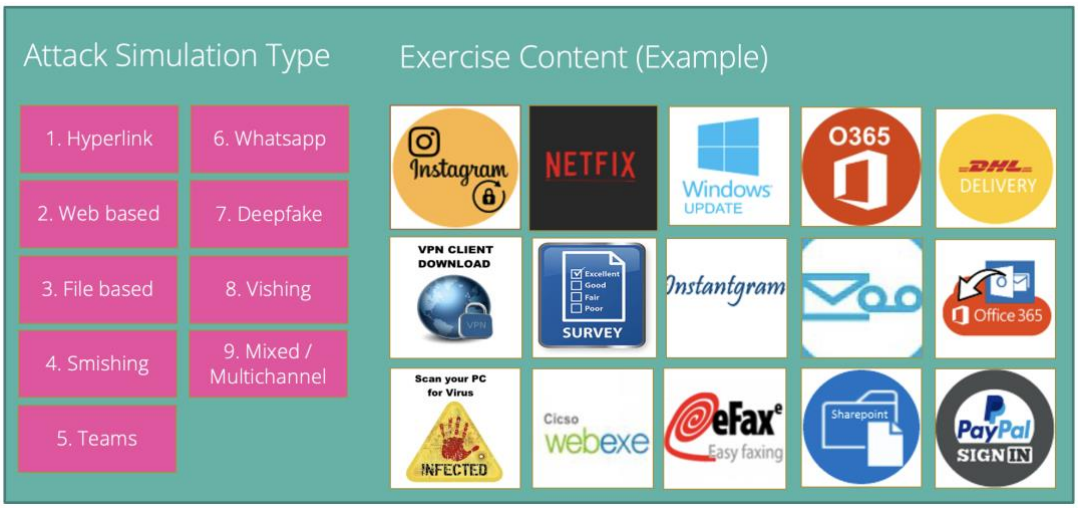


Figure 7: Testing Roadmap - Types, Elements and Scenario Examples

The Testing Roadmap helps to plan these IT security 'fire drills'. Many anti phishing / awareness products available on the market support not only fake phishing, but also educational smishing, vishing, USB hacks and others. Often a selection can be made from hundreds of different templates. But most are useless given the fact that there are 20-30 attack scenarios that still work. Advanced 2nd generation platforms and products also allow the efficient creation of individual attacks or adaptation of the templates. And as of today (2026), there are a handful of 3rd generation, AI-native solutions that allow you to run multi-channel simulations and to prompt exercise scenarios. With the latter products in particular, you can create custom phishing emails and landing pages to improve your employees' risk behavior and create lasting awareness.

4.2 Training Content Roadmap

This roadmap helps you to plan which IT security content will be made available when, how and for which recipient groups. When teaching IT security training courses, a distinction must be made between what content **must** be taught and what **should** be trained. Please note that there are always different literacy levels in your organization that should be trained to their level of knowledge. Build the training into the daily work of your employees, award diplomas/certificates and keep the lessons short.

Figure 8: Training Roadmap - Channels and Content

4.2.1 Mandatory Security Education

This is often referred to as compulsory training or policy driven training. The organization is obliged to enforce existing safety guidelines and safety instructions among its employees. This category includes in particular training for GDPR, PCI-DSS, ISO27001, HIPAA, etc.

4.2.2 Generic Security Trainings

Industry-specific training content on IT security and security in general fall into this category. This includes all topics in the field of social engineering with which the employee could be confronted:

T00. Awareness for Security Awareness
T01. Security Mindset and Behaviour
T02. How Hackers Work and Think
T03. Basic Cyber Security Proficiency
T04. Identity, Passwords & Authentication

T05. Safe Email & Messaging Behavior
T06. Safe Surfing & Cloud Usage
T07. Social Engineering & Phishing
T08. AI-Enabled Attacks
T09. Risks and Responsible Usage of AI
T10. Deep Fakes & Synthetic Media
T11. Attack Vectors & Common Cyber Threats
T12. Foundational Cybersecurity Concepts
T13. Data Protection & Privacy
T14. Clean Desk
T15. Social Media, Digital Footprint & Oversharing
T16. Mobile Devices
T17. BYOD
T18. Workplace & Physical Security
T19. Remote Work & Travel
T20. Verification & Safe Decision-Making
T21. Incident Recognition & Response
T22. Cyber Risk Management
T23. Malware & Protection
T24. IT Systems and Security
T25. Compliance and Cybersec Laws
T26. Cyber Security Culture

Depending on the industry, there are additional special modules such as

- Classification of information
- Industrial Security
- Credit card data handling
- Handling of personal data
- Handling of patient data / health data
- Physical data carriers / disposal companies

5 Additions

5.1 Infrastructure for Testing and Attack Simulations

The infrastructure for attack exercises must enable organizations to run realistic cybersecurity simulations with minimal effort and maximum impact. It shall emphasize **simplicity and automation**, allow deep **customization**, preserve **freedom and independence** from vendors, and support **universal applicability** across attack types, channels, and audiences.

Simplicity and Automation

- Provide industry-specific templates and built-in best practices
- Integrate seamlessly into existing business and security processes
- Enable unlimited, AI-driven attack and training scenarios
- Support automated provisioning of customer tenants
- Offer personalized cybersecurity chatbots for end users
- Support large-scale white-labelling of training and simulation content
- Reduce dependency on scarce cybersecurity personnel through automation

Customization

- Allow easy customization of scenarios, content, and workflows
- Offer a lightweight customization service for advanced needs
- Support use of proprietary (customer-owned) content
- Enable integration of third-party content and tools
- Support template or scenario import/export

Freedom and Independence

- Provide full control over the end-to-end simulation process
- Deliver a complete product, not just a platform framework
- Offer long-term (long-tail) product support
- Include comprehensive product documentation
- Allow customers to purchase only the core product and optionally add services

Universality

- Support multiple exercise formats, including eLearning modules
- Support phishing, smishing, and vishing simulations
- Support collaboration and messaging platforms such as Microsoft Teams, WhatsApp, etc.
- Support advanced threat scenarios, including deepfake-based attacks

5.2 Training Infrastructure (LMS)

Traditional LMS environments are often very powerful, complex, and sometimes expensive. However, much leaner LMS implementations can be used. The solution should include the following functionality:

- Support SCORM 1.2 and SCORM 2004, as well as HTML, video, and PDF content
- Provide full tracking and reporting capabilities, including completion status, pass/fail results, and time spent
- Offer comprehensive reporting with export functionality and API access
- Enable automated course assignments with dynamic user groups and
- Reminder notifications
- Support multi-level, multi-tenant environments
- Provide strong authentication options, including MFA and SSO
- Support directory integration via LDAP and Azure AD synchronization

5.3 Gamification

Gamification in Cybersecurity Awareness uses selected game elements to increase engagement with awareness content. In cyber security, its role is supportive: it can lower participation barriers, but it is not a primary driver of secure behaviour.

Typical gamification artefacts

- Progress indicators (module or topic completion)
- Short quizzes with immediate feedback
- Badges linked to demonstrated competence (not mere participation)
- Time-bound challenges (e.g. weekly phishing scenario)
- Light narrative or campaign framing (themes, seasons)
- Leaderboards (inside the tools or outside as communication element of the program)

Gamification is often overrated in Cybersecurity Awareness. It improves engagement metrics but does not reliably translate into sustained risk reduction on its own. Used correctly, it is a UX and activation tool; used incorrectly, it becomes cosmetic. Rewards and competitions should support engagement but are not a substitute for simulations and training. Effective awareness programs treat gamification as an optional enabler, not as a security control.

6 Small or large project?

The answer to this question depends mainly on the size of the company. Of course, the IT security awareness level of the organization also plays a role, as does the number of organizational units, risk groups, stakeholders etc. affected.

Smaller companies with a proactive decision-making culture can implement the basics for an awareness program including the first Baseline Phish and Train campaign in two to three days. Larger institutions, on the other hand, can take weeks or months to implement such a project. It's not so much the amount of effort involved that matters, but rather the lead time. Welcoming all affected or involved stakeholders, as well as decision-making in a heterogeneous environment, simply take time.

7 Relation to Cybersecurity Frameworks

Where does the Cyber Awareness Playbook stand in relation to existing cybersecurity frameworks?

The Cyber Awareness Playbook (CAP) is designed as an operational awareness framework that integrates cleanly into established cybersecurity and compliance frameworks like NIST and ISO/IEC 27001.

It does not replace normative standards; instead, it translates their abstract requirements into executable practice.

It is fully compatible with NIST standards, see next page.

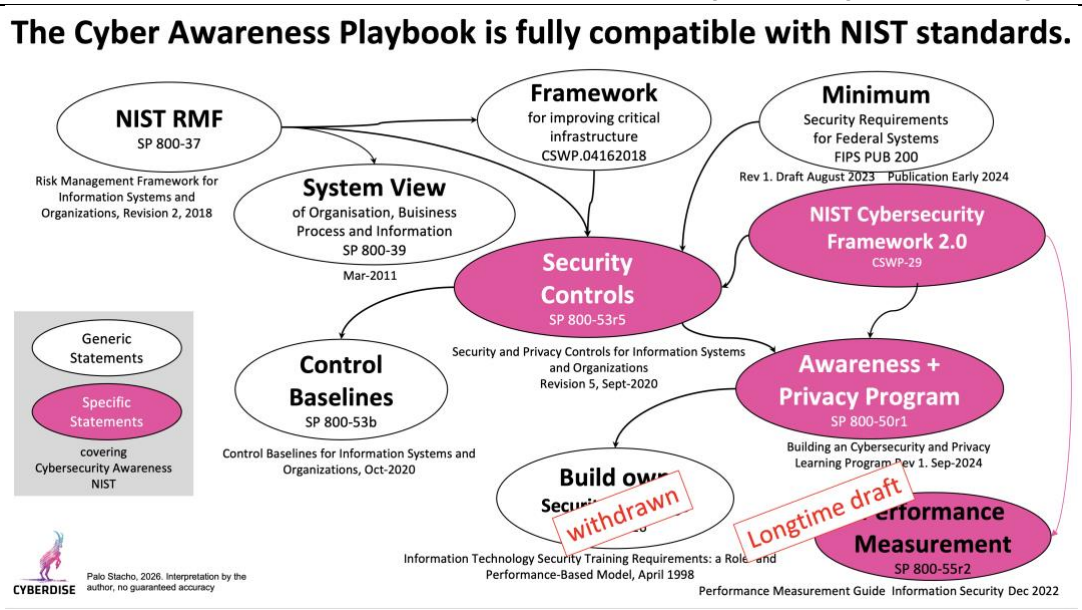
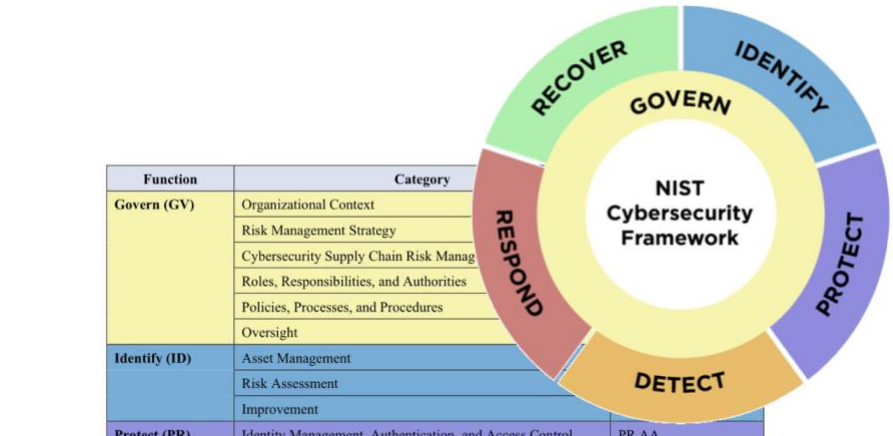


Figure 9: CAP is fully compatible with NIST

7.1 NIST CSF 2.0 Coverage

The NIST Cybersecurity Framework (CSF 2.0) defines **PR.AT – Awareness and Training** as the category ensuring that personnel are trained and aware of cybersecurity-related risks and their responsibilities. CAP fully covers this category by design.



Function	Category	
Govern (GV)	Organizational Context	
	Risk Management Strategy	
	Cybersecurity Supply Chain Risk Manag	
	Roles, Responsibilities, and Authorities	
	Policies, Processes, and Procedures	
	Oversight	
Identify (ID)	Asset Management	
	Risk Assessment	
	Improvement	
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
PR.AT	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
RS.AN RS.CO	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Figure 10: CAP assures full PR.AT Coverage NIST CSF 2.0

Through its structured phases (Scope, Plan, Run, Evolve), an implementation of the Cyber Aware Playbook ensures that:

- Cybersecurity awareness is established as a structured program rather than ad-hoc training,
- Employees understand common attack vectors and their role in prevention and detection,
- Awareness activities are continuous, measurable, and improved over time,
- Training and exercises are aligned with real-world threats and organizational risk.

The **NIST category family PR.AT** is directly implemented operationally through the Awareness Program with recurring campaigns, simulations, training modules, and evaluation mechanisms. When implementing a Phishing Incident Button functionality and the analysis of reported messages then there is also a coverage in the NIST categories **RS.AN and RS.CO**.

7.2 Complementarity with NIST SP 800-50 Rev.1 (CPLP)

The NIST Publication SP 800-50 Rev.1 (“Building a Cybersecurity and Privacy Learning Program”) defines how organizations should design and govern an awareness and training program from a policy and management perspective. CAP is fully complementary to NIST SP 800-50 Rev.1:

- NIST SP 800-50 provides the normative foundation: definitions, governance expectations, roles, and lifecycle principles.
- CAP provides the execution playbook: how awareness and training are scoped, planned, delivered, measured, and continuously improved.

CAP can therefore be understood as the **practical implementation layer** of the CPLP concepts defined in SP 800-50r1. Organizations may reference SP 800-50 to justify structure and governance, while using CAP as the primary method for running the program in practice.

We confirm that there are no overlapping conflicts, NIST defines *what is needed and* CAP shows *how it is done*.

7.3 ISO/IEC 27001

A coverage of ISO/IEC 27001 Clause 7.3 (Awareness) requires organizations to ensure that persons doing work under the organization's control are aware of:

- the information security policy,
- their contribution to the effectiveness of the ISMS,
- the benefits of improved information security performance,
- the implications and consequences of nonconformity with ISMS requirements.

CAP fully covers Clause 7.3 through its Scope and Run phases:

- Information security policies and awareness objectives are defined, communicated, and reinforced as part of the program setup.
- Employees are explicitly trained on how their behavior affects security outcomes and incident prevention.
- Training and simulations demonstrate the practical benefits of secure behavior, such as reduced incidents and faster detection.
- Consequences of non-compliance are addressed through realistic attack simulations, reporting processes, and feedback mechanisms.

Awareness is therefore not limited to policy communication but embedded into daily behavior and decision-making.

Coverage of ISO27001 Annex A Control 6.3

Annex A Control 6.3 requires that awareness, education, and training activities are established, appropriate, maintained, and effective.

The implementation of CAP within an organization fully satisfies these requirements:

- Awareness, education, and training are systematically planned through the defined CAP roadmaps and multi-phase programs.
- Content is role-based, risk-oriented, and relevant**,** addressing general staff, high-risk groups, and advanced users.
- The Awareness Program is regularly updated through the Evolve phase to reflect new threats, incidents, policies, and organizational changes.

- Effectiveness is measured and evaluated using campaign metrics, behavioral indicators, and trend analysis, enabling continuous improvement.

As a result, Annex A Control 6.3 is not only formally fulfilled, but operationalized in a sustainable and auditable manner.

7.4 Related Framework Summary

CAP acts as an execution framework that translates NIST and ISO requirements into day-to-day awareness operations. When CAP is implemented, the relevant awareness and training obligations of NIST CSF, NIST SP 800-50 Rev.1, and ISO/IEC 27001 are inherently met without introducing parallel or redundant structures.

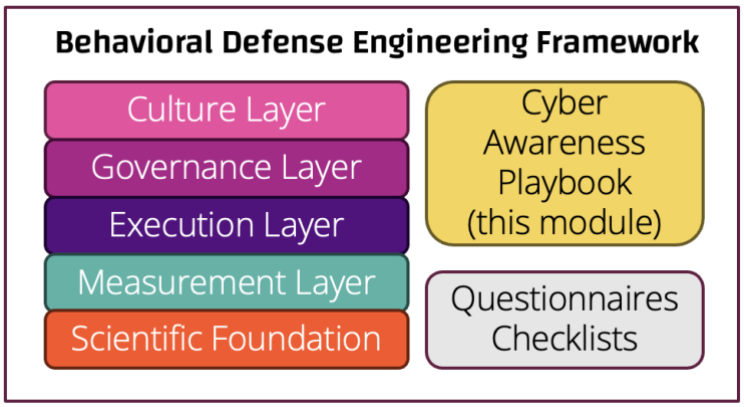
8 Change Control

Version	Date	Who	What
1.0	02.05.2020	P. Stacho	Initial Version (SAPF)
1.1	16.10.2020	P. Stacho	New Content Types
2.0	15.10.2022	P. Stacho	CAPIG Fork, Process Updates, Infrastructure description
2.1	21.10.2023	P. Stacho	Review and Adoption to NIST CSF2.0; SP-800-50r1 and SP800-53r5
3.0	15.01.2026	P. Stacho	Generic Make-Up and Updates
3.0.1	23.02.2026	P. Stacho	Adding Risk-Appetite, Attack Channels, Usage of personal data (vulnerability profiles)
3.0.2	08.03.2026	P. Stacho	Inconsistencies removed
3.0.3	12.09.2026	P. Stacho	Context to Behavioral Defense Engineering Framework added

Cyber Awareness Playbook as part of the Human Engineering Framework

The framework provides a tiered structure to systematically plan, implement, and continuously improve the security-relevant risk behavior of employees within an organization.

Measures and artifacts are described and structured along defined layers: Culture, Governance, Execution, Measurement, and Scientific Foundation. The framework is complemented by this Playbook as well as additional checklists and questionnaires.



About the Author

Palo Stacho has worked as a cybersecurity architect and consultant and entrepreneur, in the IT industry for over 30 years. He holds a federal diploma in computer science and a postgraduate degree in corporate governance from the University of St. Gallen. As early as 2010, he focused on digitalization and cybersecurity.

In 2015, Palo co-founded LUCY Security and built it into one of the world's leading providers of cybersecurity awareness software before the company was sold to a TechEd company in 2022. As a Principal Consultant, he gained experience across hundreds of cybersecurity awareness projects, including engagements with Lufthansa, Bosch, Mobiliar Insurance, OMV, Helvetia Insurance, Teleperformance, Swisscom, and others. Since 2023, he leads CYBERDISE Awareness, an AI-native provider of cybersecurity awareness software. His second passion is his role as a startup coach and scale-up tutor.

He lives with his family near Bern, Switzerland.