TEMET
end-to-end IT security

Keeping Pace

How to Integrate Cybersecurity & Compliance Requirements into Fast-Moving IT

Moritz Zollinger

28.10.2025, Kursaal Bern, Switzerland

About

Moritz Zollinger

MSc Business Information Systems
BSc Information Technology

Security Consultant
TEMET AG

Areas of Expertise
Security and Compliance Management
Secure Development
Identity and Access Management (IAM)

Contact
Phone: +41 78 897 02 47
Mail: moritz.zollinger@temet.ch
LinkedIn: linkedin.com/in/moritz-zollinger

Keeping Pace
How to integrate Security Requirements into fast moving IT

Abstract

Business is driving rapidly changing IT, constantly demanding new services and technology. Setting up AI and SaaS in corporations has never been easier. Therefore, lots of apps and services pop up left and right, and it’s getting tougher to keep our heads above water when it comes to cybersecurity and compliance.

But how can we keep pace and build in resilience in these fast-moving times? One solution is to get smart about how we design our project security requirements and to get them fulfilled in a decentralized manner.

Together, we will explore a powerful management approach leveraging predefined cybersecurity and compliance requirements to boost resilience. Whether you're all-in on agile or not, this approach will help you to increase security and compliance in services where it truly matters.

Situation, Problem and a Solution

Situation

Business is driving rapidly changing IT and is
constantly demanding new services and technology.
Classic approaches like a “Security Concept per Service” have limitations

Problem

Keeping pace with fast moving IT as Security Responsible is hard.
It’s challenging to keep the new things under control.

A Solution

Management Approach leveraging predefined
Cybersecurity & Compliance Requirements (CCR) with
CyCoRE: Cybersecurity & Compliance Requirements Engineering and Mgmt.

What is a CCR?
Cybersecurity & Compliance Requirement

Two types of Requirements in RE

- Functional Requirement
  "system shall **do** <requirement>"

- Non-Functional Requirement (NFR)
  "system shall **be** <requirement>

  In our case:
  shall **be** secure & compliant

NFR/CCR Examples (simplified)

- APIs requests shall **be** authenticated
- Data shall **be** encrypted
- Offline backup shall **be** established
- The system shall **be** connected to the IdP and using SSO
- Roles and permissions shall **be** defined
- Personal data shall **be** deleted when no longer needed
- Data Protection Impact Assessment (DPIA) shall **be** conducted

What is a CCR?
Cybersecurity & Compliance Requirement

NFR vs. CCR

- NFR is a well known industry term
- CCR was invented at Temet
- CCR is (most often) an NFR focusing on Security or Compliance

CCRs can be derived from

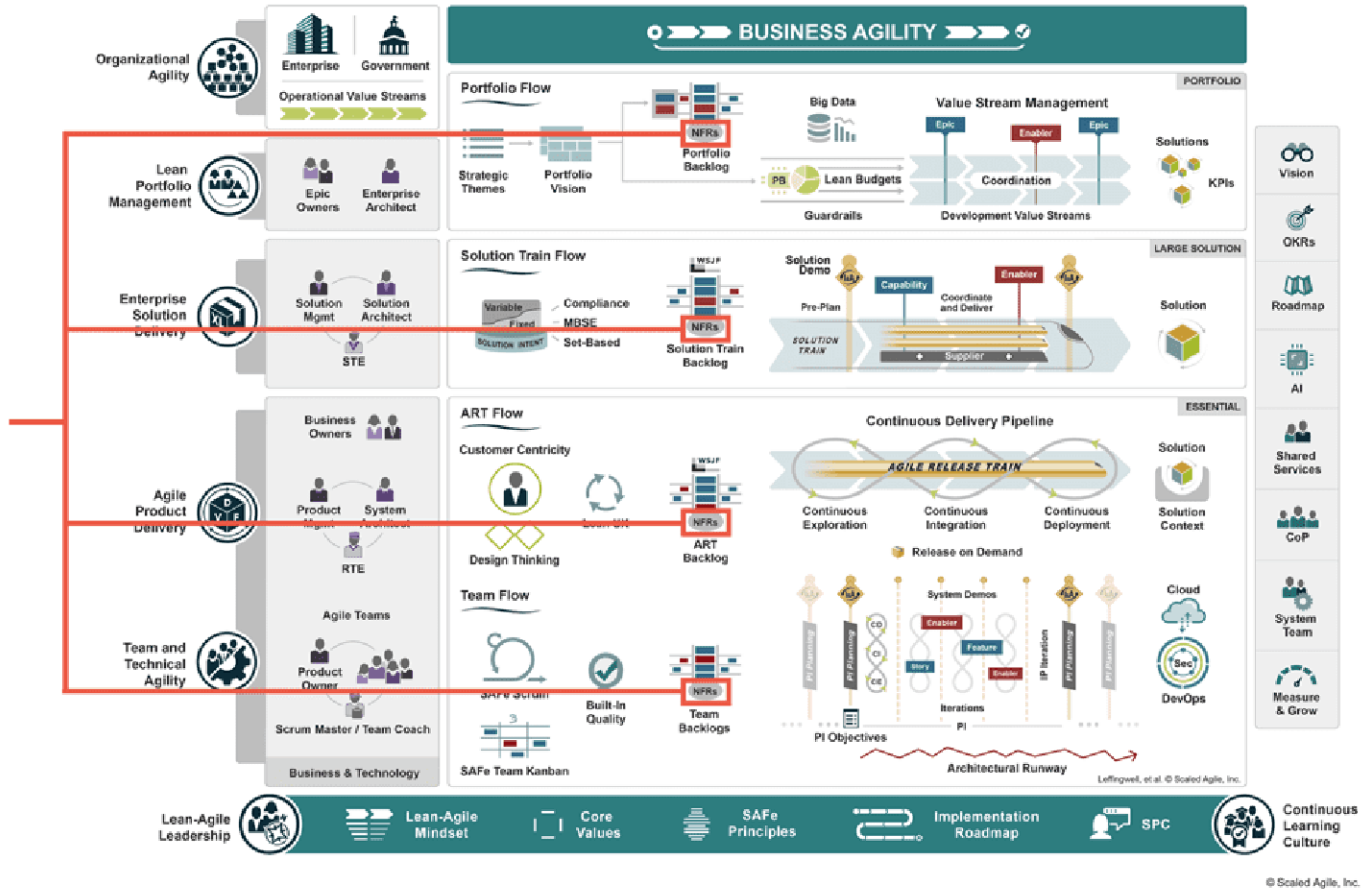
- Acts & Ordinances (DSG/FADP)
- Regulations (FINMA)
- External Standards (ISO 27001/2)
- Internal Standards
- Experience

A **CCR** can (most often) be treated like an **NFR** focusing on Security

What is a CCR?
Cybersecurity & Compliance Requirement

Link to the Agile Method: SAFe

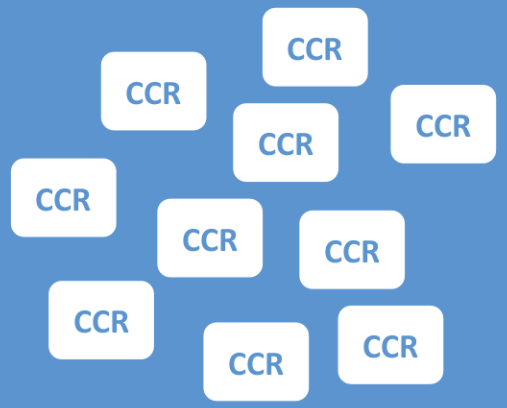
Non-Functional Requirements thus CCRs are built into Agile Methods such as SAFe, but can also be used without Agile Methods

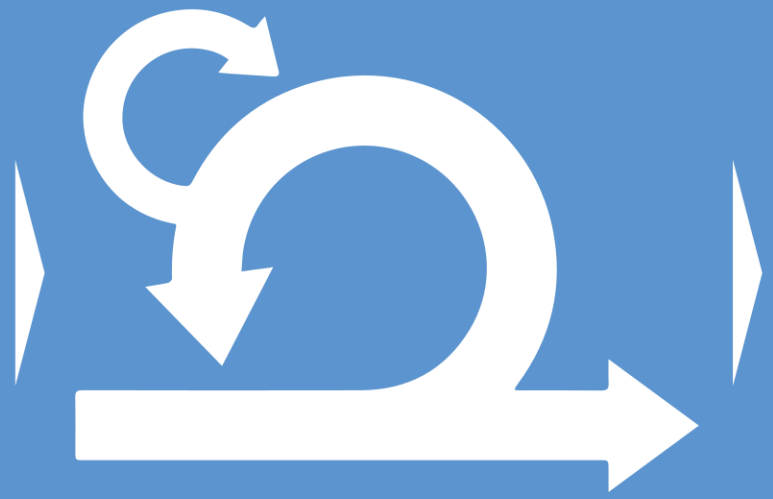


Bring Security to the Backlog!

Figure NFRs occur with all backlogs in SAFe from https://scaledagileframework.com/nonfunctional-requirements/

Security Requirements Engineering & Mgmt.
Very Basic Concept



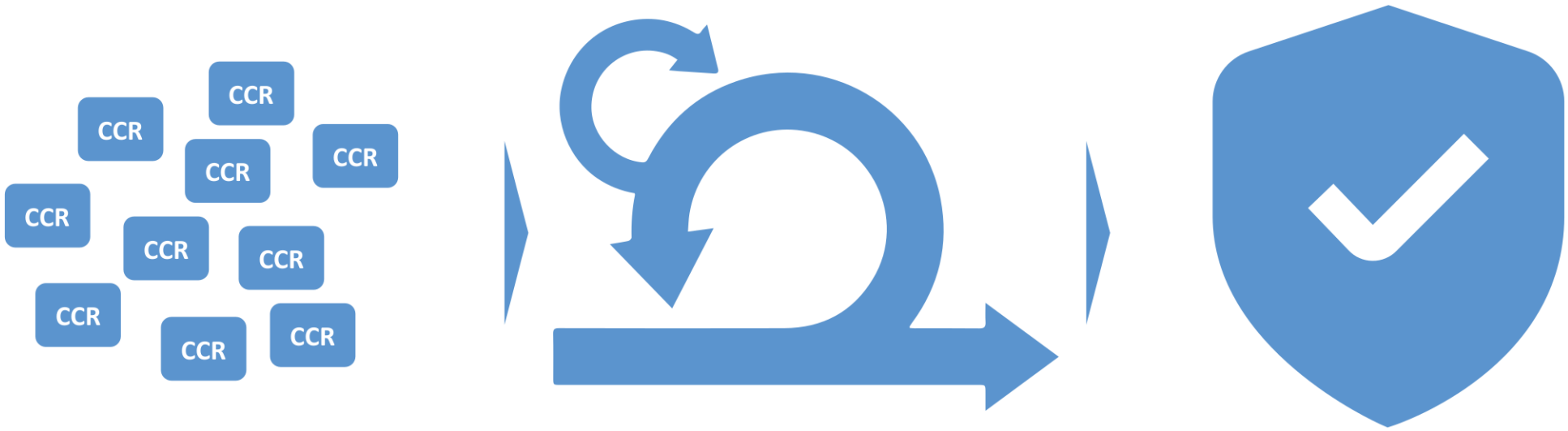


Input: CCR

Project / Epic

Output: Secure Deliverable

Security Requirements Engineering & Mgmt.
Very Basic Concept

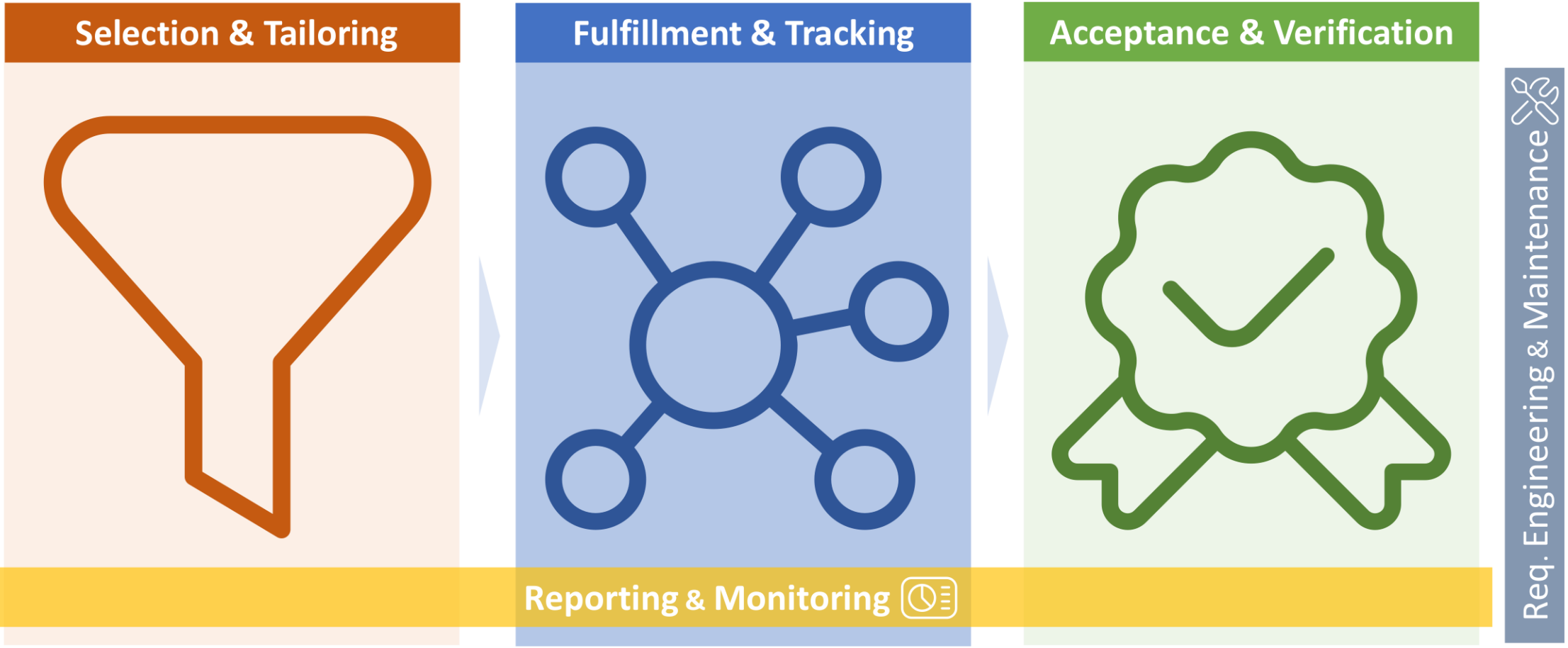


Input: CCR

Project / Epic

Output: Secure Deliverable

Security Requirements Engineering & Mgmt.
CyCoRE 3 Phase Process



TEMET
end-to-end IT security

Security Requirements Engineering & Mgmt.
CyCoRE 3 Phase Process

Selection & Tailoring

- Tailor the CCR Catalog using
- a Security Questionnaire (Shortcut Risk Analysis) to
- a comprehensible CCR List

CCRs to the Backlog

Fulfillment & Tracking

- Fulfill CCRs distributed
- Track CCRs centralized
- Gather Evidence

- Enable the organization to
  - independently fulfill CCRs

Fulfilled – Agreed – Accepted

Acceptance & Verification

- Stakeholders accept and verify CCRs

Always Trust – Sometimes Verify

Reporting & Monitoring

Req. Engineering & Maintenance

Initialization | Analysis | Design

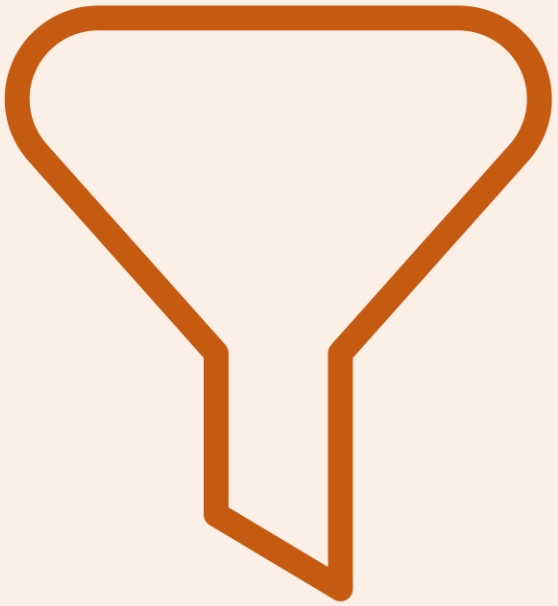
Implementation | Realization

Review | Release | Increment

TEMET
end-to-end IT security

Cybersecurity & Compliance Requirements Engineering & Management: CyCoRE

Selection & Tailoring

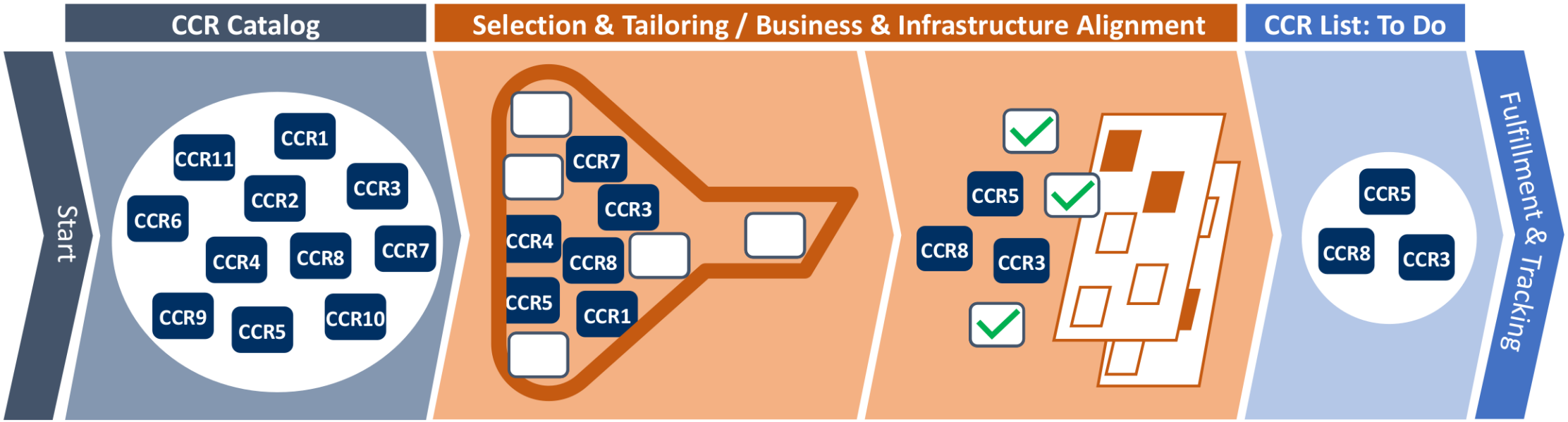


Fulfillment & Tracking

Acceptance & Verification

CCR Selection & Tailoring
Business & Infrastructure Alignment

ST FT AV



Security Organization | Epic / Project Specific

Cybersecurity & Compliance Req.
Predefined CCRs derived from laws, external and internal standards as well as experience

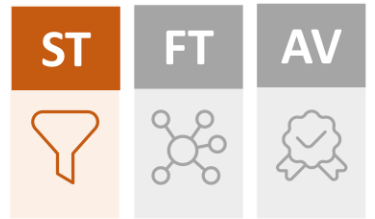
Business Alignment
Security & Compliance Questionnaire
(Shortcut Risk Analysis)
> Project relevant CCRs remain

Infrastructure Alignment
Building upon existing Platforms
Remove CCRs already fulfilled by using existing Platforms.

CCR List for implementation
Project specific CCR List for the Backlog
(DoR: Definition of Ready)

TEMET end-to-end IT security

CCR Selection & Tailoring
Security Questionnaire (Example)

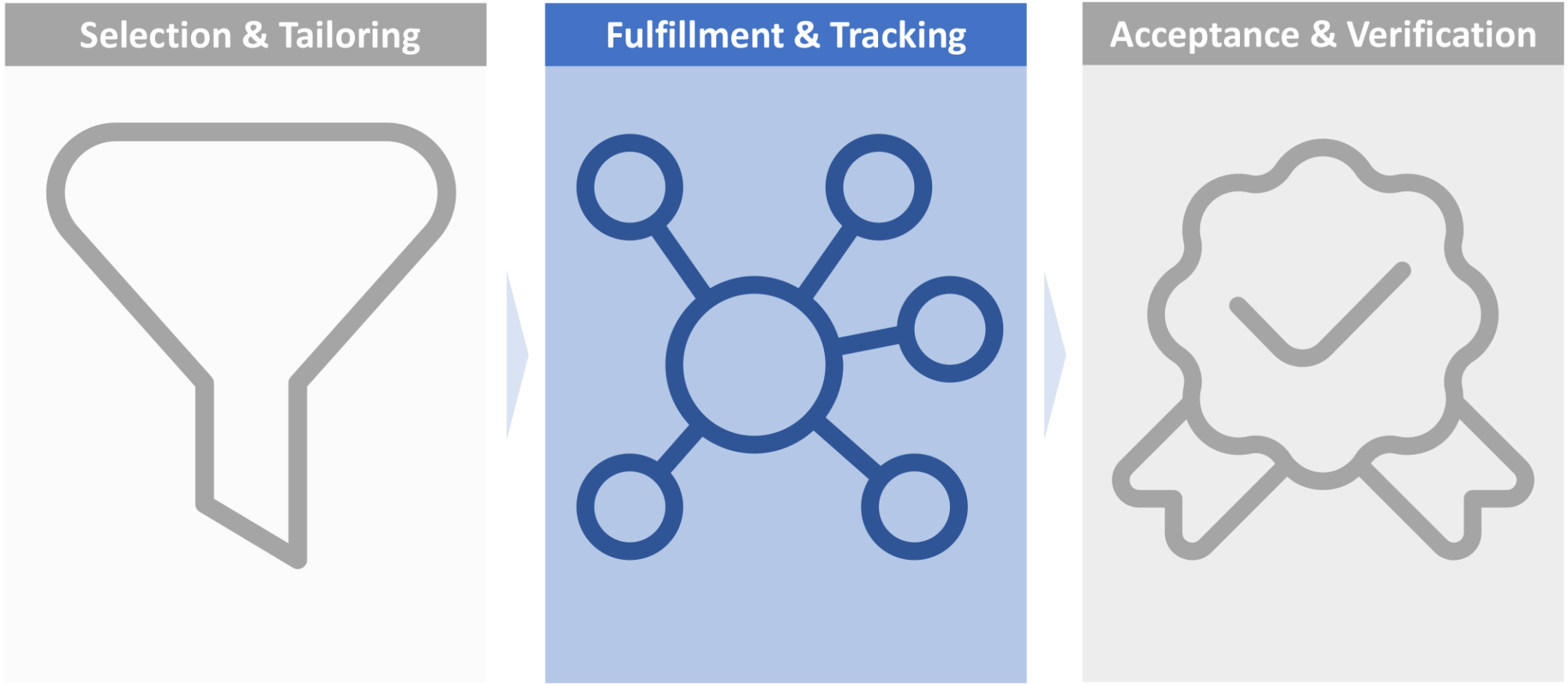


Questions

- What is your venture about:
  > *Important service for customers*
- How is the data you are processing classified? > *confidential*
- How critical would it be, if the data is unrecoverable? > *disastrous*
- Are there roles & permissions req. for your service? > *yes*
- Is sensitive personal data with a high risk being processed? > yes
- Which platform are you running the service on? > *Our Stack CH*

- **CCRs**
- CCR1 API Security: APIs requests shall be authenticated
- ~~CCR4 Encryption: Data shall be encrypted~~
- ~~CCR7 Backup: Offline backup shall be established~~
- CCR3 IdP: the system shall be connected to the IdP and using SSO
- CCR5 IAM: Roles and permissions shall be defined
- CCR8 Data Protection: A Data Protection Impact Assessment (DPIA) shall be conducted

Cybersecurity & Compliance Requirements Engineering & Management: CyCoRE



CCR in depth
CASE Structure: CCR, AC, Support, Evidence

Cybersecurity & Compliance Requirement

- The (Non-Functional) Requirement

Acceptance Criteria (AC)

One CCR has one or many ACs

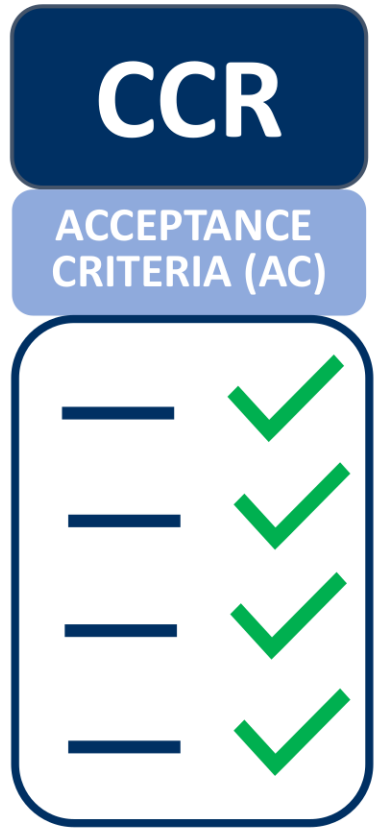
- AC = "conditions that must be satisfied in order to be accepted"
- ACs are a list to check / verify if a CCR is fulfilled resp. the requirement is met

Support

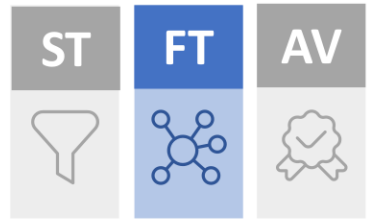
- Guidance for the Project Lead / Engineer on how to fulfill the CCR

Evidence

- Evidence which shall be provided to document the fulfillment



CCR Fulfillment & Tracking
CCRs based on Tailoring (Examples)



CCR3 IdP

- The system shall be connected to the IdP and using Single Sign-On

AC

✓The Service is Single Sign-On (SSO) enabled

✓The SAML or OIDC protocol is used

Evidence

- Architecture Overview: <insert link>

Support

- See: Connect to IdP via OIDC
- Contact: iam@company.ch

CCR5 IAM

- Roles and permissions shall be defined

AC

✓Role Concept is defined

✓Roles are impl. within the IAM

✓Roles are assigned

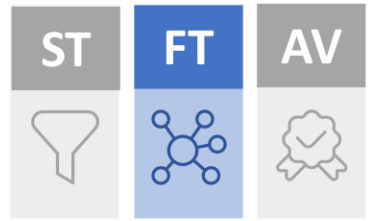
Evidence

- Role Concept within IAM System: <insert link>

Support

- See: Guidance on Role Concepts

CCR Fulfillment & Tracking
CCRs based on Tailoring (Examples)



CCR8 DPIA

- A Data Protection Impact Assess. (DPIA) shall be conducted

AC

✓The DPIA is completed

✓and approved by the Data Protection Office

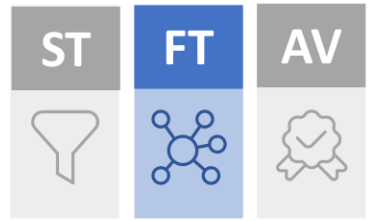
Evidence

- DPIA: <insert link here>

Support

- Use this Template: DPIA
- Ask dataprotection@company.ch

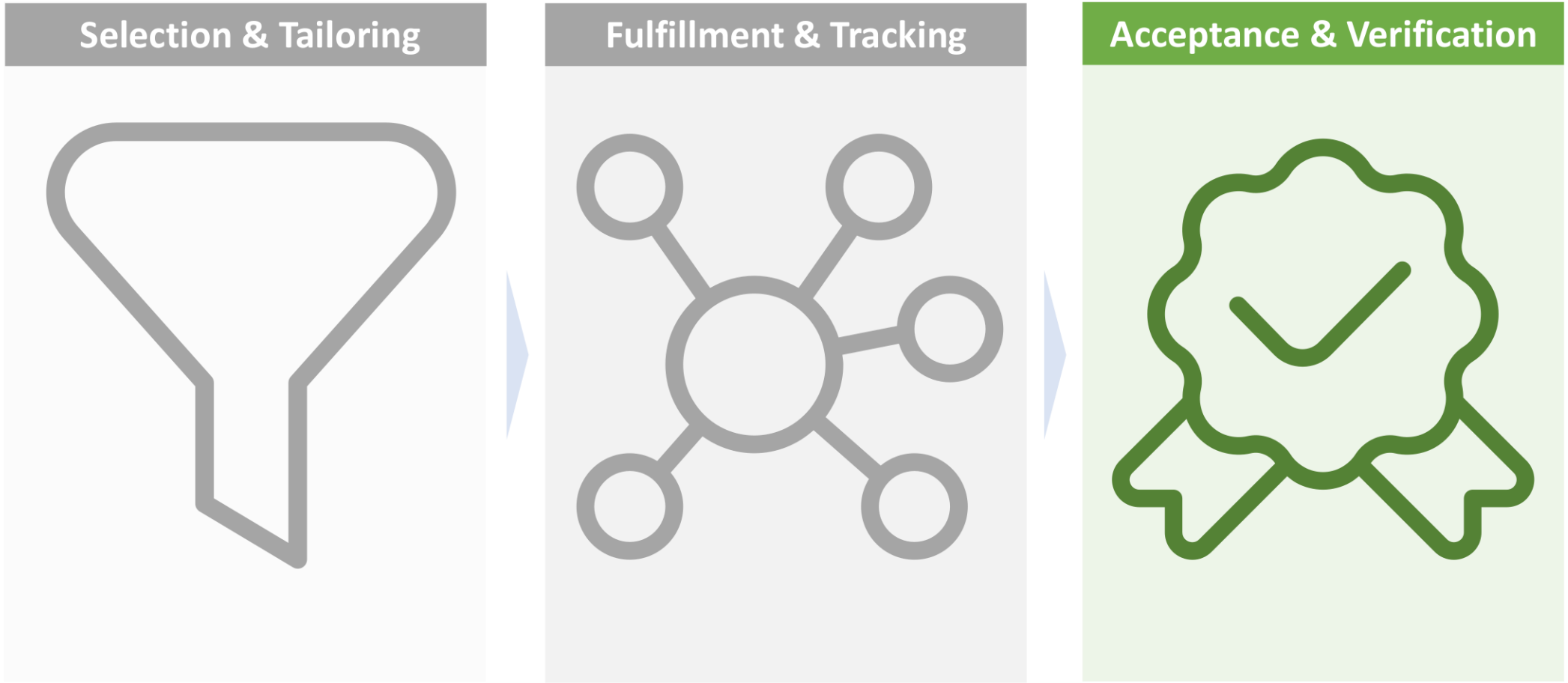
CCR Fulfillment & Tracking
CCR List



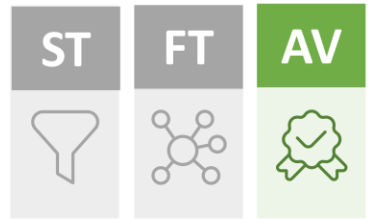
CCR	Acceptance Criteria (AC)	Fulfilled & Agreed	Evidence
CCR3 **IdP**	□ The Service is SSO-enabled □ SAML or OIDC protocol is used	□ Engineer □ Team Lead	Architectural overview: <Link> Ticket: <Link to Jira>
CCR5 **IAM**	✓ Role Concept is defined ✓ Roles are impl. within the IAM ✓ Roles are assigned	✓ Engineer ✓ Team Lead	Role Concept within IAM: MyApp
CCR8 **DPIA**	✓ The DPIA is completed □ The DPIA is approved by the Data Protection Office	✓ Project Lead	DPIA: MyDPIA

- CCR List implementation: in Confluence or in Jira/Kanban or in a dedicated Tool
- A lean Exception Management Process is required

Cybersecurity & Compliance Requirements Engineering & Management: CyCoRE



CCR Acceptance & Verification
CCR List

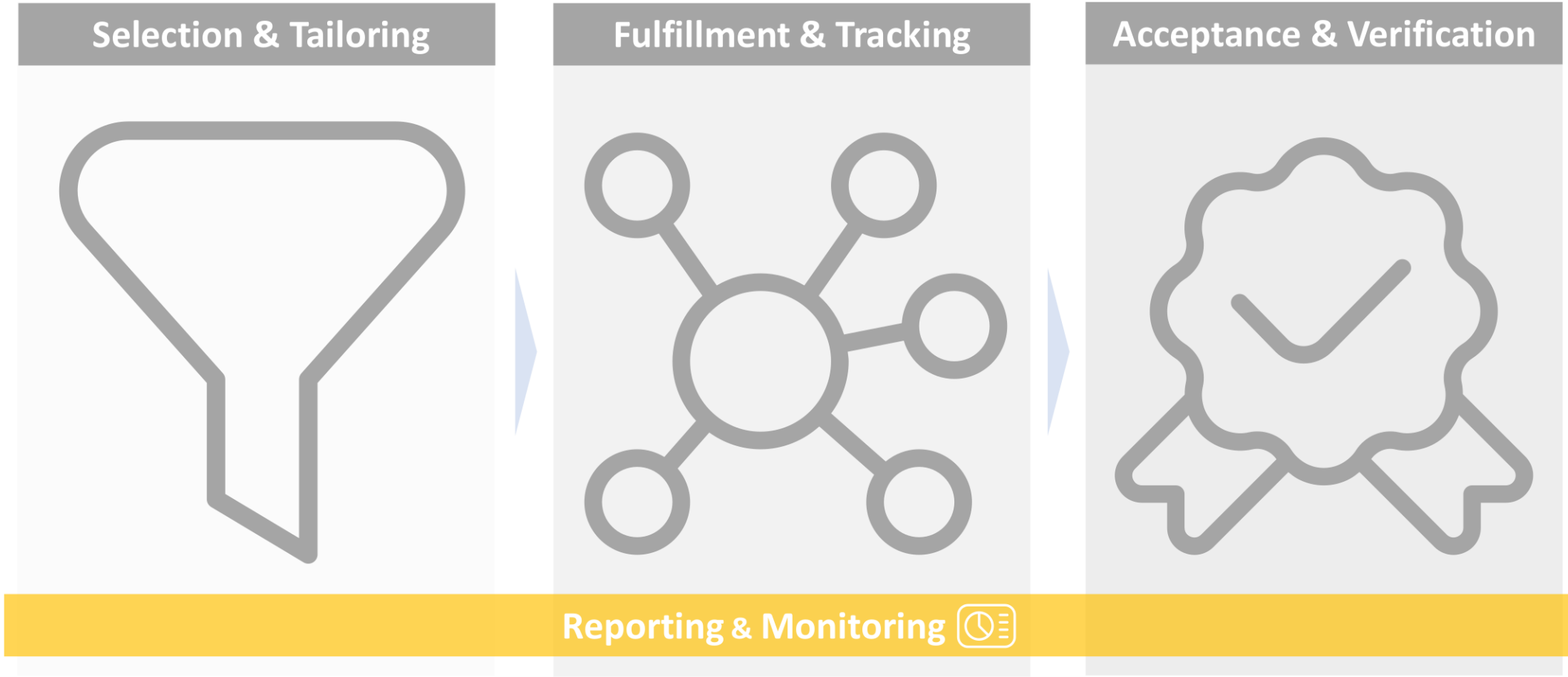


- Stakeholders review the CCR List, may check Evidence and accept CCR

Stake holder	CCR	Acceptance Criteria (AC)	Fulfilled & Agreed	Evidence	Accepted
Security Team	CCR3 **IdP**	✓ The Service SSO-enabled ✓ The SAML or OIDC protocol is used	✓ Engineer ✓ Team Lead	Architectural overview Ticket: JIRA-123	✓ Security
IAM Team	CCR5 **IAM**	✓ Role Concept is defined ✓ Roles are impl. within the IAM ✓ Roles are assigned	✓ Engineer ✓ Team Lead	Role Concept: MyApp	✓ IAM Team
Data Protection Office	CCR8 **DPIA**	✓ The DPIA is completed ✓ The DPIA is approved by the Data Protection Office	✓ Project Lead	DPIA: MyDPIA	✓ Data Protection

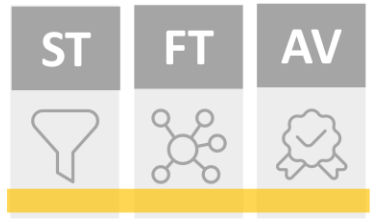
We now, hopefully, have a Secure and Compliant product

Cybersecurity & Compliance Requirements Engineering & Management: CyCoRE

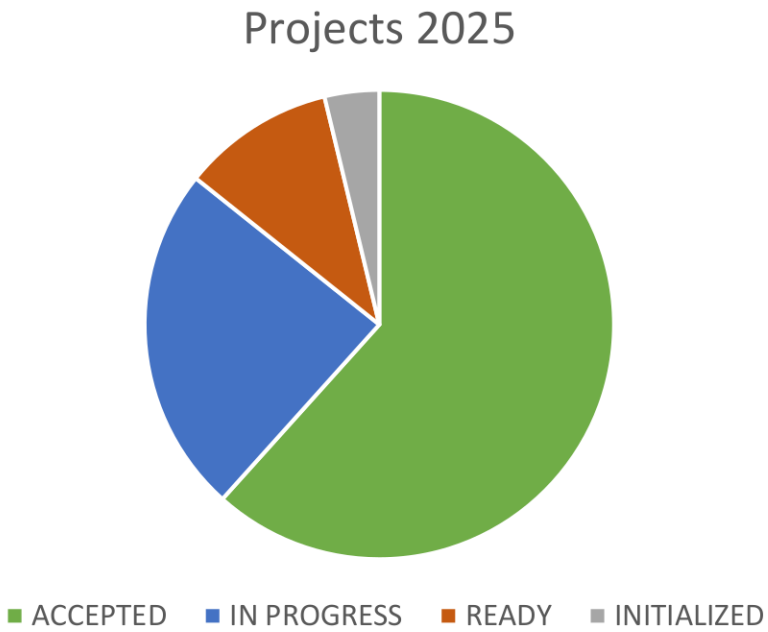


TEMET
end-to-end IT security

CCR Reporting & Monitoring
Dashboard



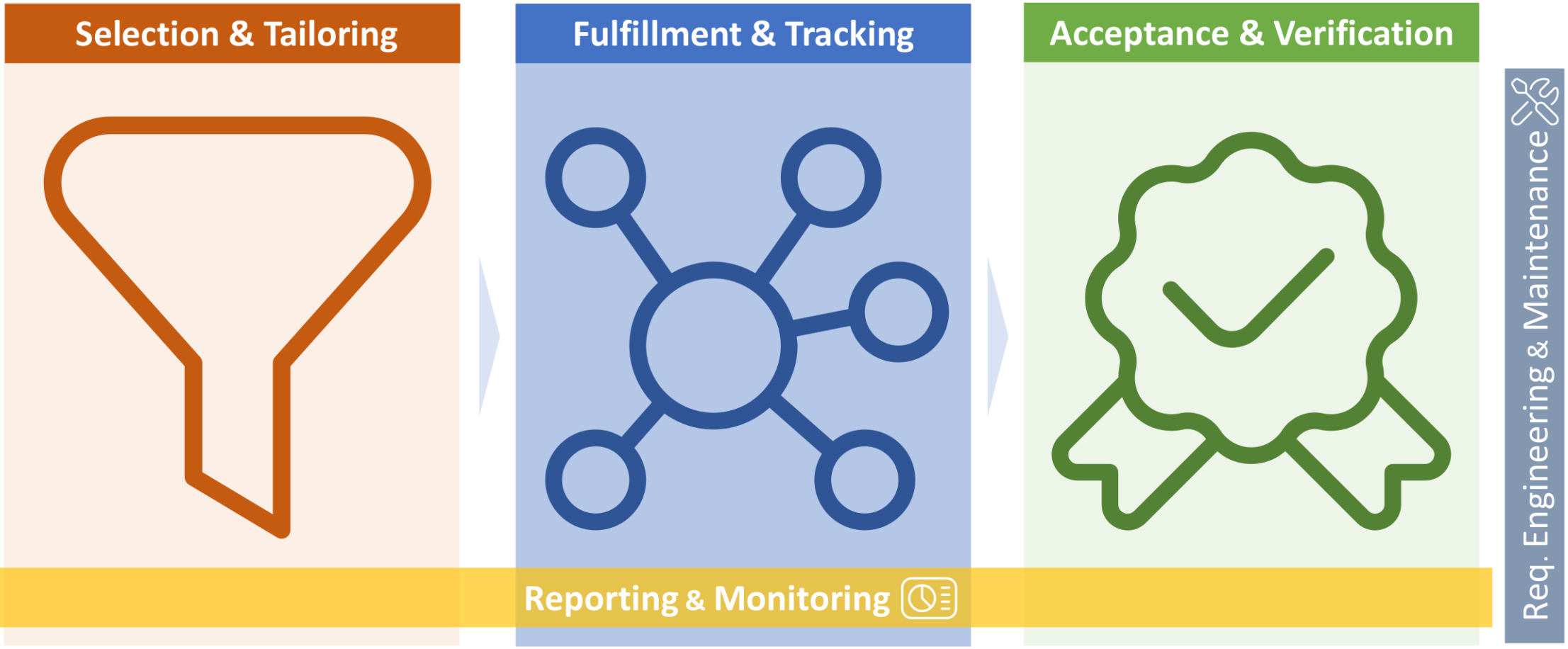
Project	Project Status	Status CCR List	CCR completed	Criticality	Pers. Data	Exceptions
Venture 42	Design	READY	00 / 31	High	Sensitive	3
Epic 27	Implementation	IN PROGRESS	05 / 25	Low	None	1
Project 1	Done	ACCEPTED	11 / 11	Medium	Yes	0



TEMET
end-to-end IT security

Security Requirements Engineering & Mgmt.

CyCoRE 3 Phase Process | ReCap



Implementing CyCoRE
Preconditions

CyCoRE

- **Cy**bersecurity & **Co**mpliance **R**equirement **E**ngineering and Management

Precondition

- An Epic Flow / Project Management Process …to hook into
  - Design > Implementation > Release

- A Security Team & Management with power & will …to drive the process

Implementing CyCoRE
Artifacts & Enablers

Security Artifacts

- CCR Catalog with defined CCRs incl. AC, Support and Evidence (CASE)
- Security Questionnaire to select CCRs & tailor them to projects
- CCR List to Track & Accept CCR fulfillment
- Dashboard over all Projects / Epics for reporting & monitoring
- Process: Defined and established Cybersecurity & Compliance Requirement Engineering and Mgmt. Processes linked to the Epic Flow / PM

Enable the Organization

- Education and Training
- Security Champions Program
- Stakeholder Management

Implementing CyCoRE
Benefits & Advantages

- Clearly defined Requirements (CCR)
- Step-by-step processes reduce implementation effort and therefore costs
  - CyCoRE nudges teams to define processes
- Distribution reduces load on the Security Organization
  - CyCoRE scales even in larger enterprises
- Evidence of fulfilled requirements is gathered along the way
  - CyCoRE supports revisions with transparency dashboard
- Overall Cybersecurity and Compliance increases

- CCRs could be included in contracts as part of 3rd Party Risk Mgmt. (TPRM)

Thanks

- Temet

https://www.temet.ch

- La Mobilière

https://www.mobiliar.ch

- Co-Workers

Daniel F. Maurer

Bruno Blumenthal

- Government Organizations

Icons: Uicons by Flaticon.com