Overview of Information Security in projects in Allianz SE

Thomas Stocker
Information Security Officer
Allianz SE

TROOPERS12
Make the world a safer place.

Allianz

Common situation for Information Security Officers

Overall IT-project status

1.in budget ☑

2.in time ☑

3.in senior-management expectations ☑

4.in required security level ?

➢Request for “Security approval” just before already communicated rollout

Different options to “lose”:

a)Ask for security investigation and try to postpone rollout

b)Escalate and blame project manager for ignoring security

c)Approve rollout and pray

Situations like that have to be prevented proactively!

Security Objectives within projects

General objective: Setup of IT Systems

1. in budget
2. in time
3. in required security level

Key security requirements to achieve objectives

a)Early allocation of security resources – budget and time (Objective 1 + 2)

b)Alignment business to security requirements (1+2+3)

c)Review/Definition of security concept (3)

d)Fixation of security level/measures in detail (1+2+3)

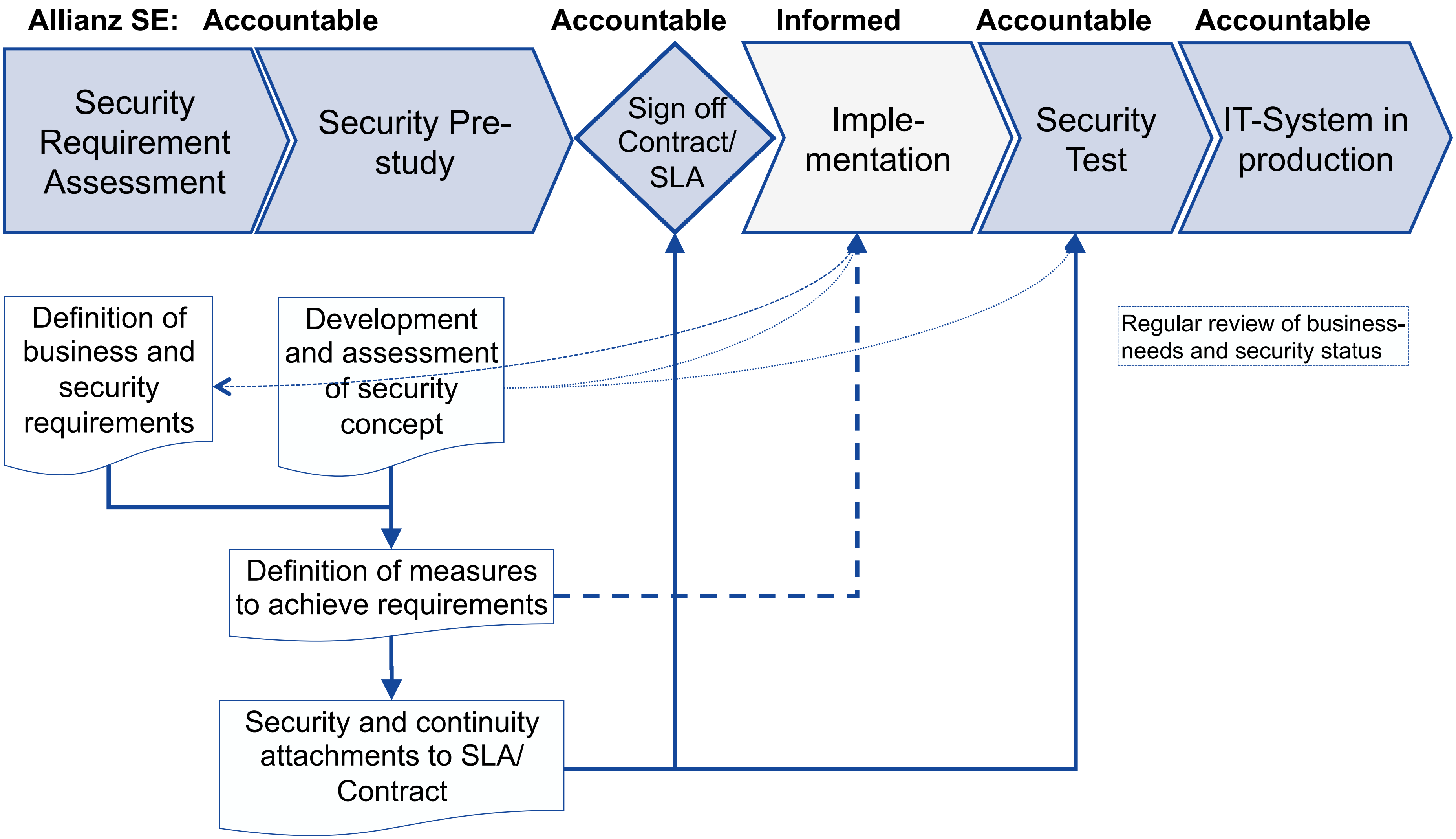
e)Performance of security test (3)

f)Identification of security vulnerabilities (3)

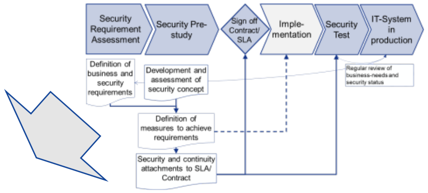
g)Management of risks (1+2+3)

h)Costs for vendor-caused security vulnerabilities to be taken over by vendors (1)

Process to achieve IT-System security at a glance


Allianz SE: Accountable
Accountable
Informed
Accountable
Accountable
Security Requirement Assessment
Security Pre-study
Sign off Contract/ SLA
Imple-mentation
Security Test
IT-System in production
Definition of business and security requirements
Development and assessment of security concept
Definition of measures to achieve requirements
Security and continuity attachments to SLA/ Contract
Regular review of business-needs and security status

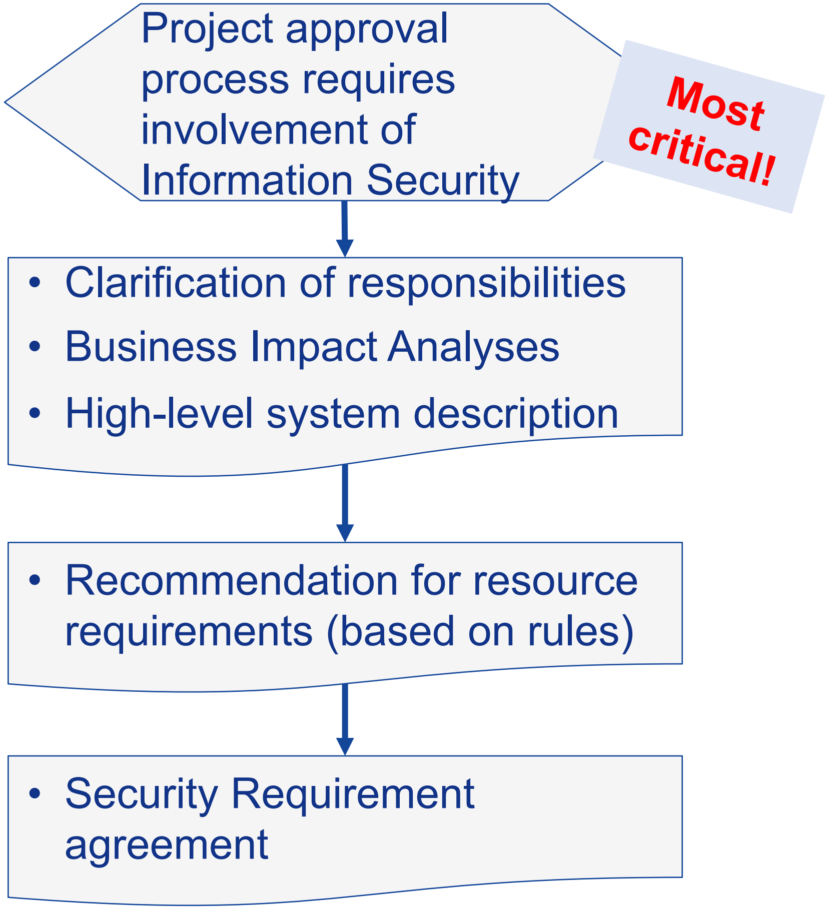
Overview Allianz SE / ISO-D tools within process


Security Requirement Assessment
Security Pre-study
Sign off Contract/ SLA
Imple-mentation
Security Test
IT-System in production
Definition of business and security requirements
Development and assessment of security concept
Regular review of business-needs and security status
Definition of measures to achieve requirements
Security and continuity attachments to SLA/ Contract

Project approval tool

Project approval tool

Description



Project approval process requires involvement of Information Security

Most critical!

- Clarification of responsibilities
- Business Impact Analyses
- High-level system description

- Recommendation for resource requirements (based on rules)

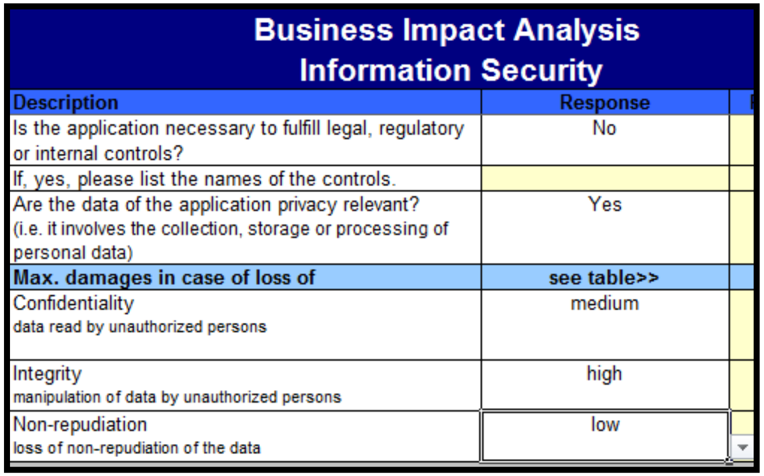
- Security Requirement agreement

Most common alternative

Information Security will be involved “later”

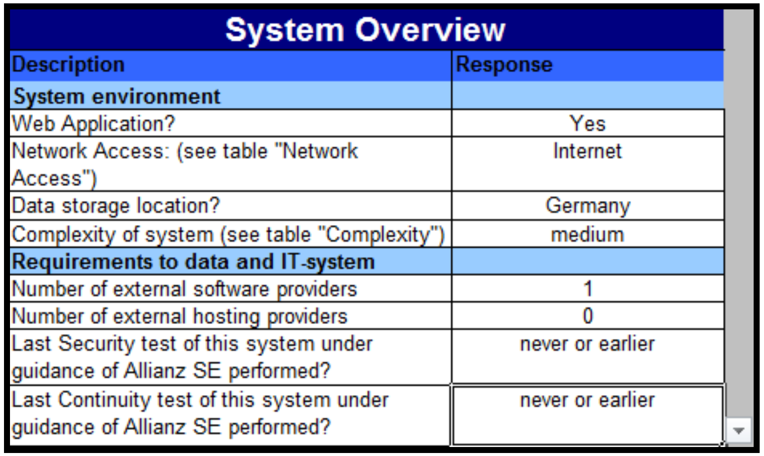
Project approval tool - samples

Input (samples)



Business Impact Analysis Information Security

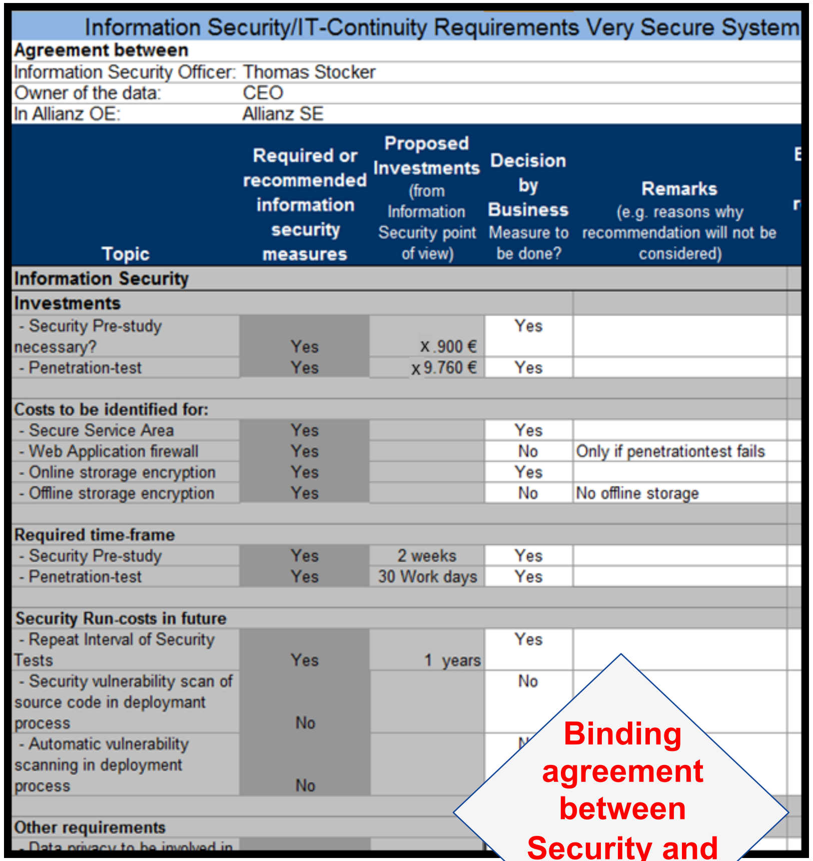
Description	Response
Is the application necessary to fulfill legal, regulatory or internal controls?	No
If, yes, please list the names of the controls.	
Are the data of the application privacy relevant? (i.e. it involves the collection, storage or processing of personal data)	Yes
Max. damages in case of loss of	**see table>>**
Confidentiality data read by unauthorized persons	medium
Integrity manipulation of data by unauthorized persons	high
Non-repudiation loss of non-repudiation of the data	low



System Overview

Description	Response
System environment	
Web Application?	Yes
Network Access: (see table "Network Access")	Internet
Data storage location?	Germany
Complexity of system (see table "Complexity")	medium
Requirements to data and IT-system	
Number of external software providers	1
Number of external hosting providers	0
Last Security test of this system under guidance of Allianz SE performed?	never or earlier
Last Continuity test of this system under guidance of Allianz SE performed?	never or earlier

Output (extract)



Information Security/IT-Continuity Requirements Very Secure System

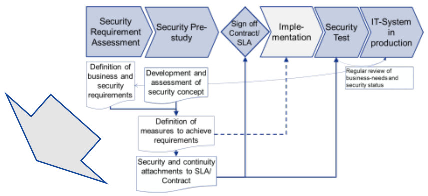
Agreement between

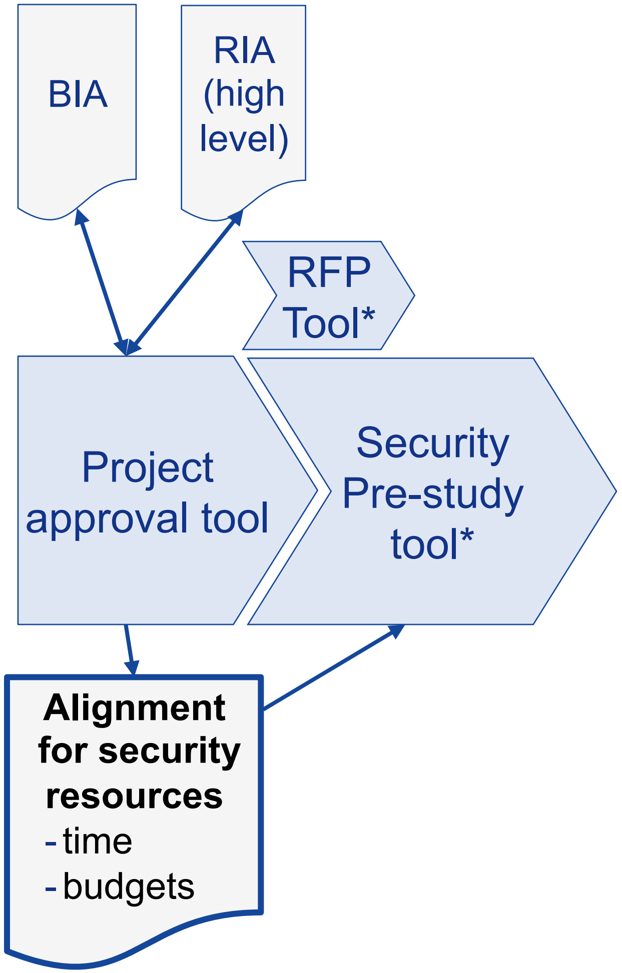
Information Security Officer:	Thomas Stocker
Owner of the data:	CEO
In Allianz OE:	Allianz SE

Topic	Required or recommended information security measures	Proposed Investments (from Information Security point of view)	Decision by Business Measure to be done?	Remarks (e.g. reasons why recommendation will not be considered)
Information Security				
Investments				
- Security Pre-study necessary?	Yes	x .900 €	Yes	
- Penetration-test	Yes	x 9.760 €	Yes	
Costs to be identified for:				
- Secure Service Area	Yes		Yes	
- Web Application firewall	Yes		No	Only if penetrationtest fails
- Online strorage encryption	Yes		Yes	
- Offline strorage encryption	Yes		No	No offline storage
Required time-frame				
- Security Pre-study	Yes	2 weeks	Yes	
- Penetration-test	Yes	30 Work days	Yes	
Security Run-costs in future				
- Repeat Interval of Security Tests	Yes	1 years	Yes	
- Security vulnerability scan of source code in deploymant process	No		No	
- Automatic vulnerability scanning in deployment process	No		N	
Other requirements				
- Data privacy to be involved in				

Binding agreement between Security and business

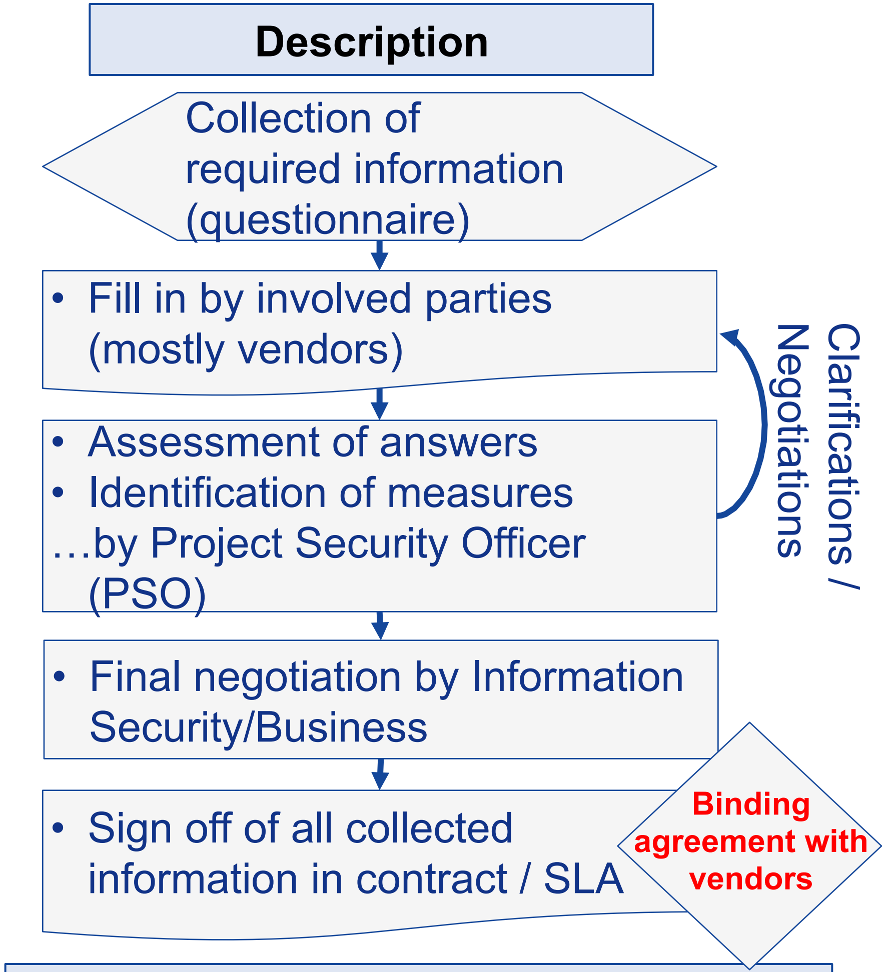
Overview Allianz SE / ISO-D tools within process


Security Requirement Assessment
Security Pre-study
Sign off Contract/ SLA
Imple-mentation
Security Test
IT-System in production
Definition of business and security requirements
Development and assessment of security concept
Regular review of business-needs and security status
Definition of measures to achieve requirements
Security and continuity attachments to SLA/ Contract



* In small projects RFP Tool can be used instead of Security Pre-study tool

Security Pre-study tool



Description

Collection of required information (questionnaire)

- Fill in by involved parties (mostly vendors)

- Assessment of answers
- Identification of measures

…by Project Security Officer (PSO)

- Final negotiation by Information Security/Business

- Sign off of all collected information in contract / SLA

Clarifications / Negotiations

Binding agreement with vendors

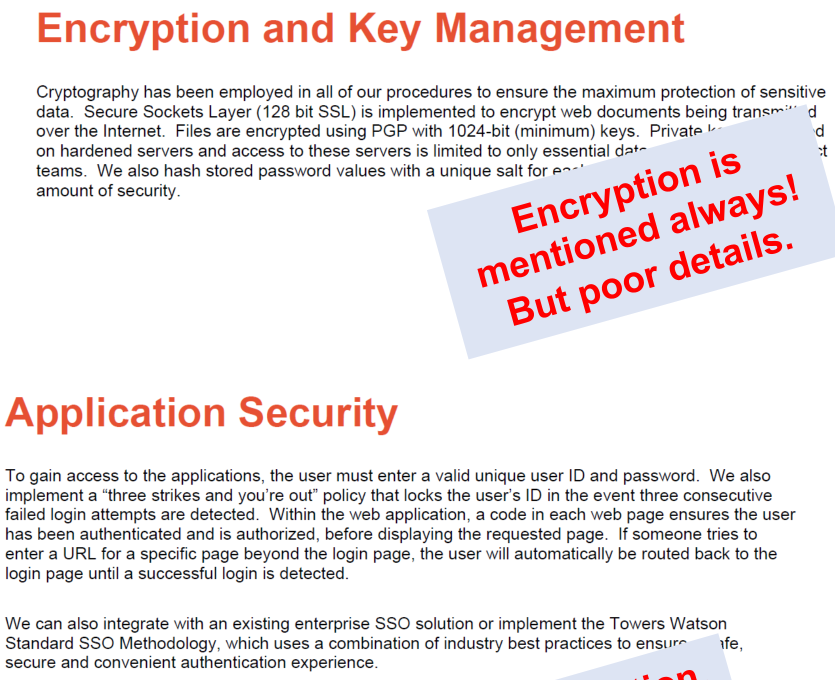
Most critical success factor: Qualification of PSO

Most common alternatives

- Request of security information by vendor
  - ⇒ Information are in 95% very poor
- Check for compliance (e.g. ISO 27001, TÜV-Certificate)
  - ⇒ No certificate guarantees a secure product (experiences from many penetration tests)
- No contract with detailed security specification of all components
  - ⇒ Risks that vulnerabilities will be classified as Change-Requests

Samples for vendor security descriptions

Two of the best security descriptions



Encryption and Key Management

Cryptography has been employed in all of our procedures to ensure the maximum protection of sensitive data. Secure Sockets Layer (128 bit SSL) is implemented to encrypt web documents being transm d over the Internet. Files are encrypted using PGP with 1024-bit (minimum) keys. Private k d on hardened servers and access to these servers is limited to only essential dat t teams. We also hash stored password values with a unique salt for ea amount of security.

Encryption is mentioned always! But poor details.

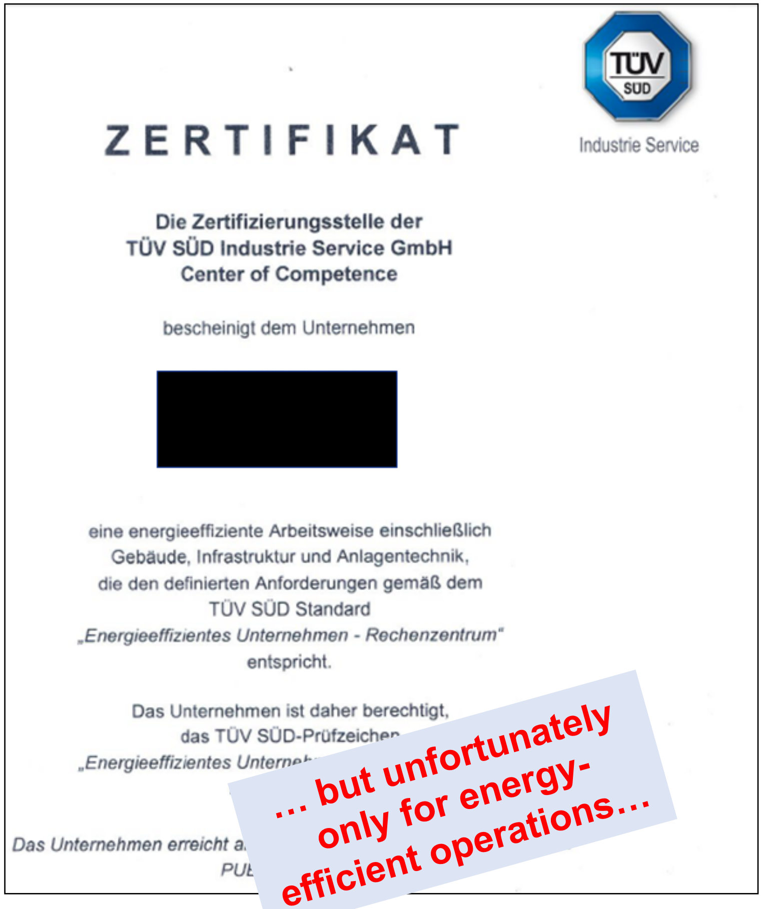
Application Security

To gain access to the applications, the user must enter a valid unique user ID and password. We also implement a "three strikes and you're out" policy that locks the user's ID in the event three consecutive failed login attempts are detected. Within the web application, a code in each web page ensures the user has been authenticated and is authorized, before displaying the requested page. If someone tries to enter a URL for a specific page beyond the login page, the user will automatically be routed back to the login page until a successful login is detected.

We can also integrate with an existing enterprise SSO solution or implement the Towers Watson Standard SSO Methodology, which uses a combination of industry best practices to ensur afe, secure and convenient authentication experience.

That's all about the application, But at least there is anything. But by far not enough

A TÜV-certificate in the folder "security"



TÜV SÜD

Industrie Service

ZERTIFIKAT

Die Zertifizierungsstelle der
TÜV SÜD Industrie Service GmbH
Center of Competence

bescheinigt dem Unternehmen

[redacted]

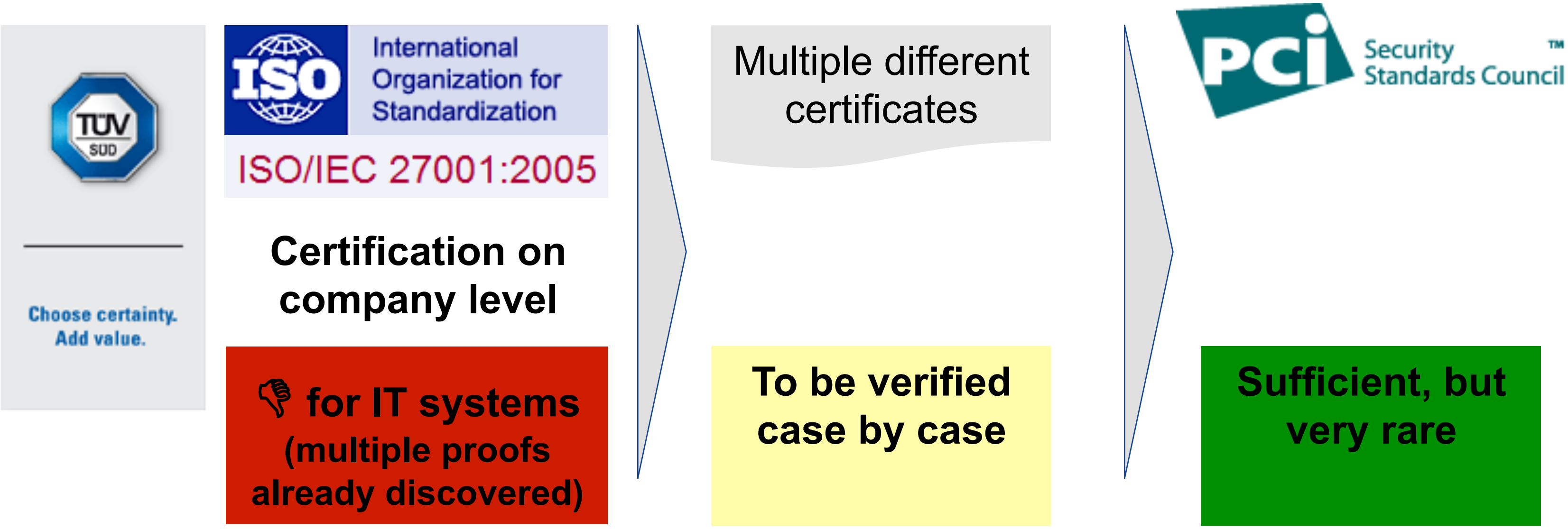
eine energieeffiziente Arbeitsweise einschließlich
Gebäude, Infrastruktur und Anlagentechnik,
die den definierten Anforderungen gemäß dem
TÜV SÜD Standard
„Energieeffizientes Unternehmen - Rechenzentrum"
entspricht.

Das Unternehmen ist daher berechtigt,
das TÜV SÜD-Prüfzeichen
„Energieeffizientes Unterne

Das Unternehmen erreicht a
PUE

… but unfortunately only for energy-efficient operations…

Certification as sufficient security description for IT systems?


TÜV SÜD
Choose certainty. Add value.
ISO International Organization for Standardization
PCI Security Standards Council™

ISO/IEC 27001:2005

Certification on company level

👎 for IT systems (multiple proofs already discovered)

Multiple different certificates

To be verified case by case

Sufficient, but very rare

Pros

- Saving potential for security concept and penetration test

Cons

- No detailed contractual agreement with provider (Risks of costly CRs for security updates)
- Most certifications do not guarantee a secure product

Well known and highly trusted organizations a reference customer

“The system is also used in [Brands, organizations with very trustworthy name]. Do we really need to care about Information Security in this case?”

Experiences

-Rule of thumb: The more this argument is used the less secure is the product

Reasons

-???

Assumptions

-No other arguments

-Systems are used in other environments (separated LAN, other data, ..)

-Also Information Security departments in organizations with a very trustworthy name sometimes have no full control about all IT-systems

TROOPERS12 Make the world a safer place.

Allianz

Security Pre-study tool- samples

Input (samples)

Application			
Description	**Security Investigation**		**Assess ment**
To be filled by Softw. vendor	**Response Provider**	**Comment PSO/ISO**	**PSO**
Input / Output validation			
Which protective measures are taken to prevent cross-site scripting?	We only allow trustworthy users access to the application	180.000 users will get access to the application. We need a countermeasure	not O.K
Do these measures ensure that cross-site scripting isn't possible?	No, but this is not necessary	It is necessary	not O.K
Which protective measures are taken to prevent SQL-injections?	We recommend to secure the database against injection attacks with a firewall in front of the database-server	Please look up in Wikipedia about "SQL-Injection"	not O.K
Do these measures ensure that SQL-injection isn't possible?	Yes, if a firewall will be installed	as above	not O.K
How the system reacts if input is getting rejected during validation?	The user is getting logged out and the session will be destroyed	We need an error message	not O.K

Output (extract)

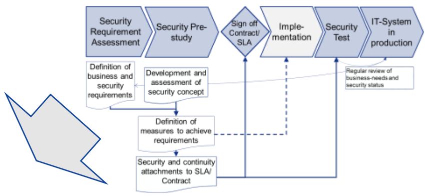
Contract Annex IT Security

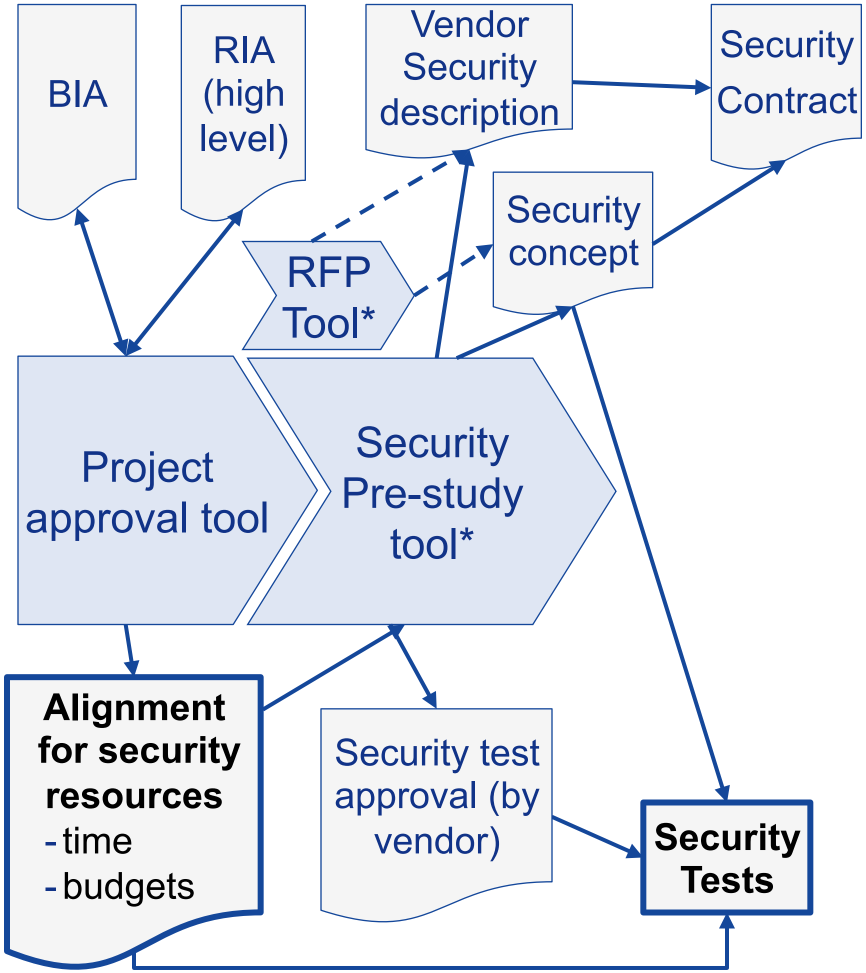
Description	**Response / Warranted description**
Which protective measures are taken to prevent cross-site scripting?	We escape all XSS-related characters by converting all applicable characters to HTML entities (e.g. “>” => &gt;)
Do these measures ensure that cross-site scripting isn't possible?	Yes
Which protective measures are taken to prevent SQL-injections?	All database queries are done via “prepared statements”
Do these measures ensure that SQL-injection isn't possible?	Yes
How the system reacts if input is getting rejected during validation?	We provide an custom error message which e.g. explains that no special character are allowed

Binding agreement with vendors

No costs for security patches

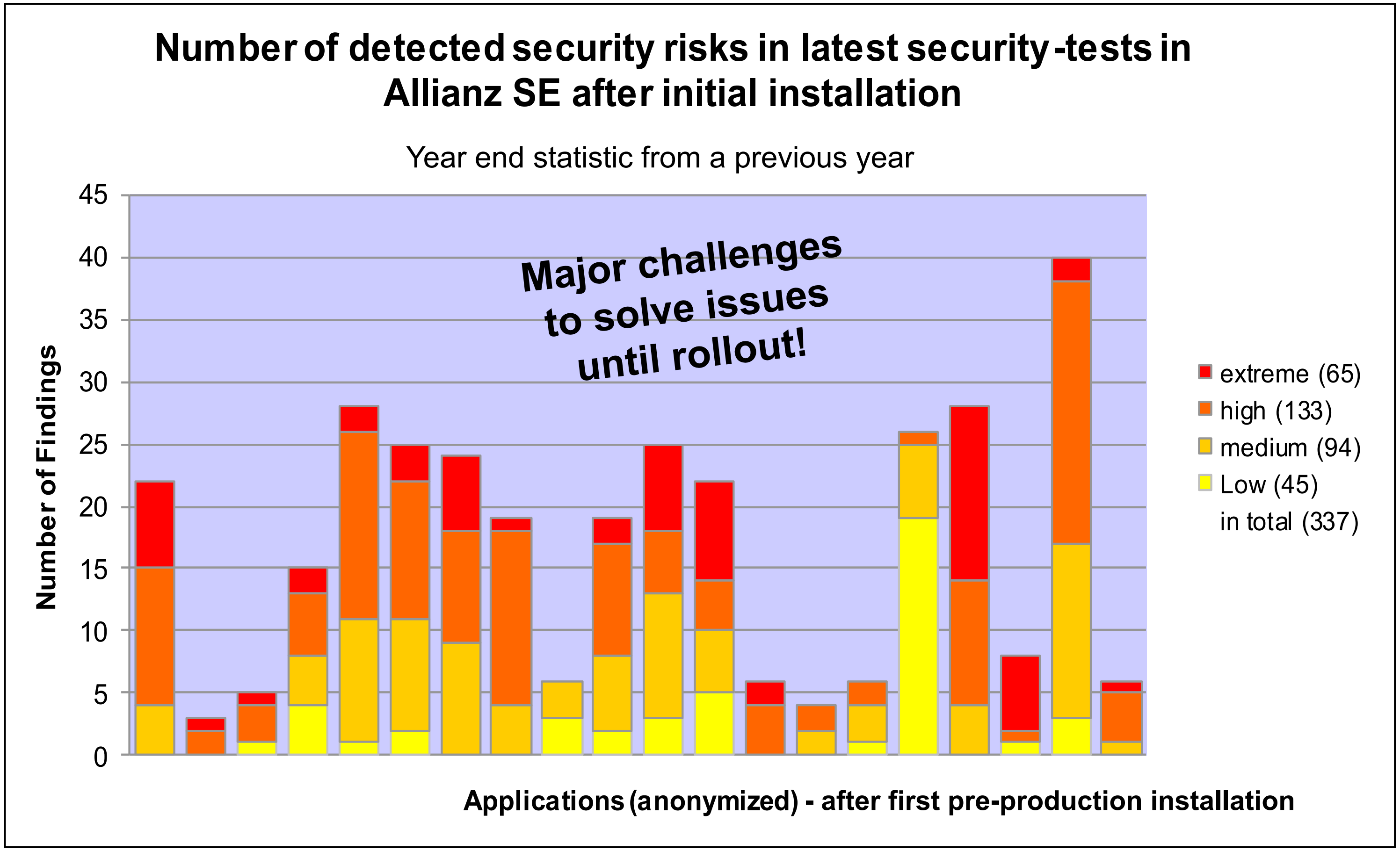
Overview Allianz SE / ISO-D tools within process


Security Requirement Assessment
Security Pre-study
Sign off Contract/ SLA
Imple-mentation
Security Test
IT-System in production
Definition of business and security requirements
Development and assessment of security concept
Regular review of business-needs and security status
Definition of measures to achieve requirements
Security and continuity attachments to SLA/ Contract



* In small projects RFP Tool can be used instead of Security Pre-study tool

Vulnerabilities in IT-systems after initial installation



Number of detected security risks in latest security-tests in Allianz SE after initial installation

Year end statistic from a previous year

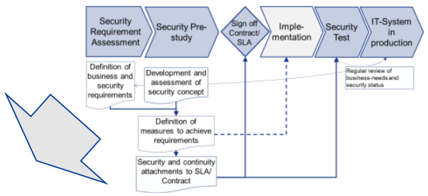
Major challenges to solve issues until rollout!

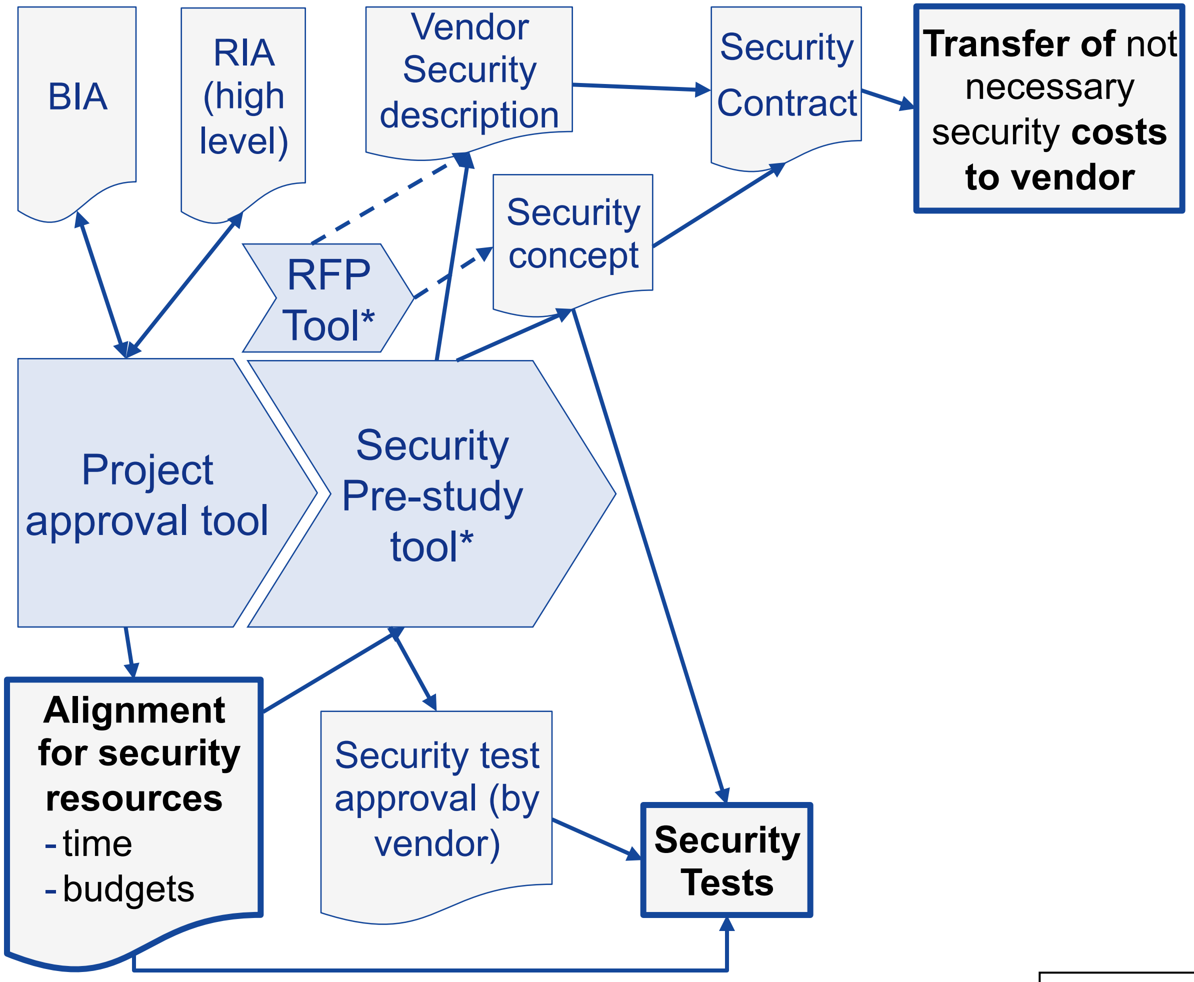
- 80% of Products in use at other globally acting enterprises
- 60% of all software were already "security tested" by the vendor

You never can expect a secure IT-system without quality assurance by a security test

TROOPERS12
Make the world a safer place.

Overview Allianz SE / ISO-D tools within process


Security Requirement Assessment
Security Pre-study
Sign off Contract/ SLA
Imple-mentation
Security Test
IT-System in production
Definition of business and security requirements
Development and assessment of security concept
Regular review of business-needs and security status
Definition of measures to achieve requirements
Security and continuity attachments to SLA/ Contract

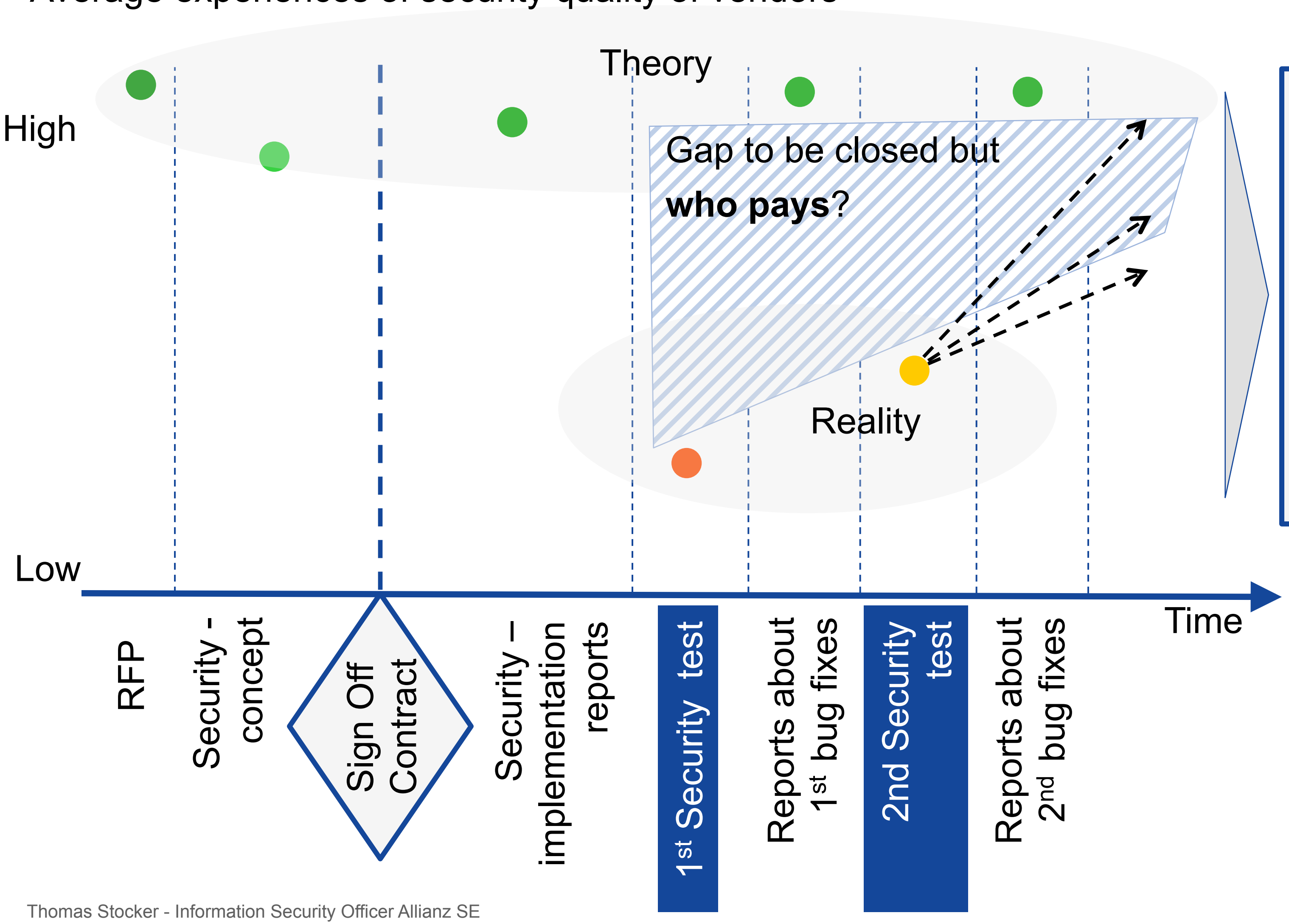

BIA
RIA (high level)
Vendor Security description
Security Contract
Transfer of not necessary security **costs to vendor**
RFP Tool*
Security concept
Project approval tool
Security Pre-study tool*
Alignment for security resources
- time
- budgets

Security test approval (by vendor)
Security Tests

* In small projects RFP Tool can be used instead of Security Pre-study tool

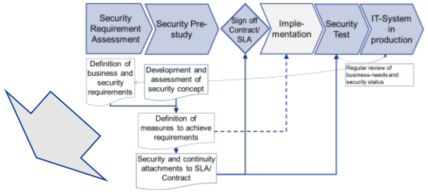
Necessity for detailed Security Contract

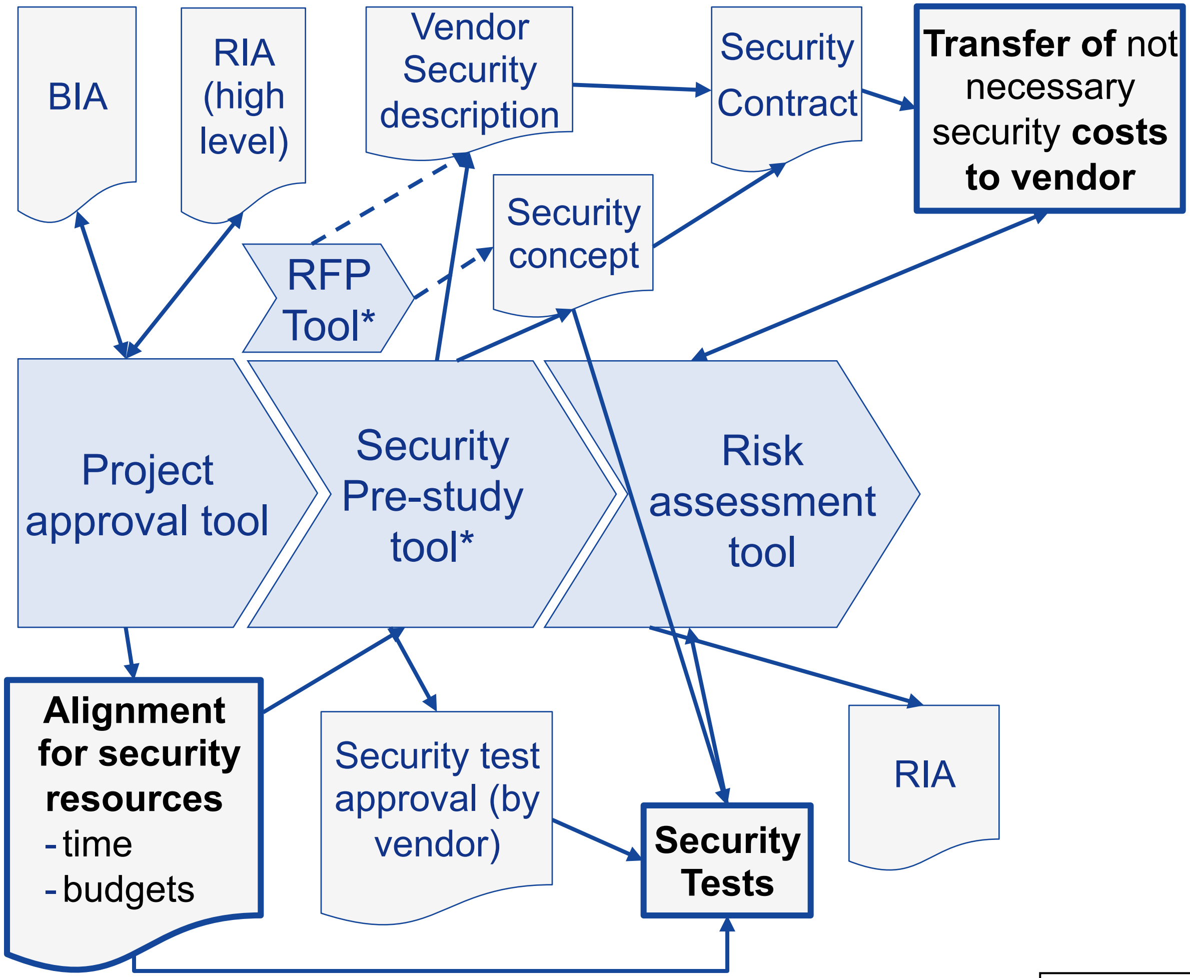
Average experiences of security quality of vendors



"Transfer of not necessary security costs to vendor" only ensured if all security relevant details are included in contract

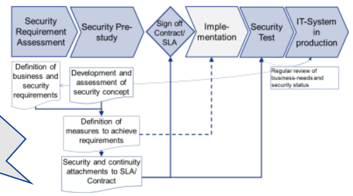
Overview Allianz SE / ISO-D tools within process


Security Requirement Assessment
Security Pre-study
Sign off Contract/ SLA
Imple-mentation
Security Test
IT-System in production
Definition of business and security requirements
Development and assessment of security concept
Regular review of business-needs and security status
Definition of measures to achieve requirements
Security and continuity attachments to SLA/ Contract



* In small projects RFP Tool can be used instead of Security Pre-study tool

Overview Allianz SE / ISO-D tools within process



Security Requirement Assessment

Security Pre-study

Sign off Contract/ SLA

Imple-mentation

Security Test

IT-System in production

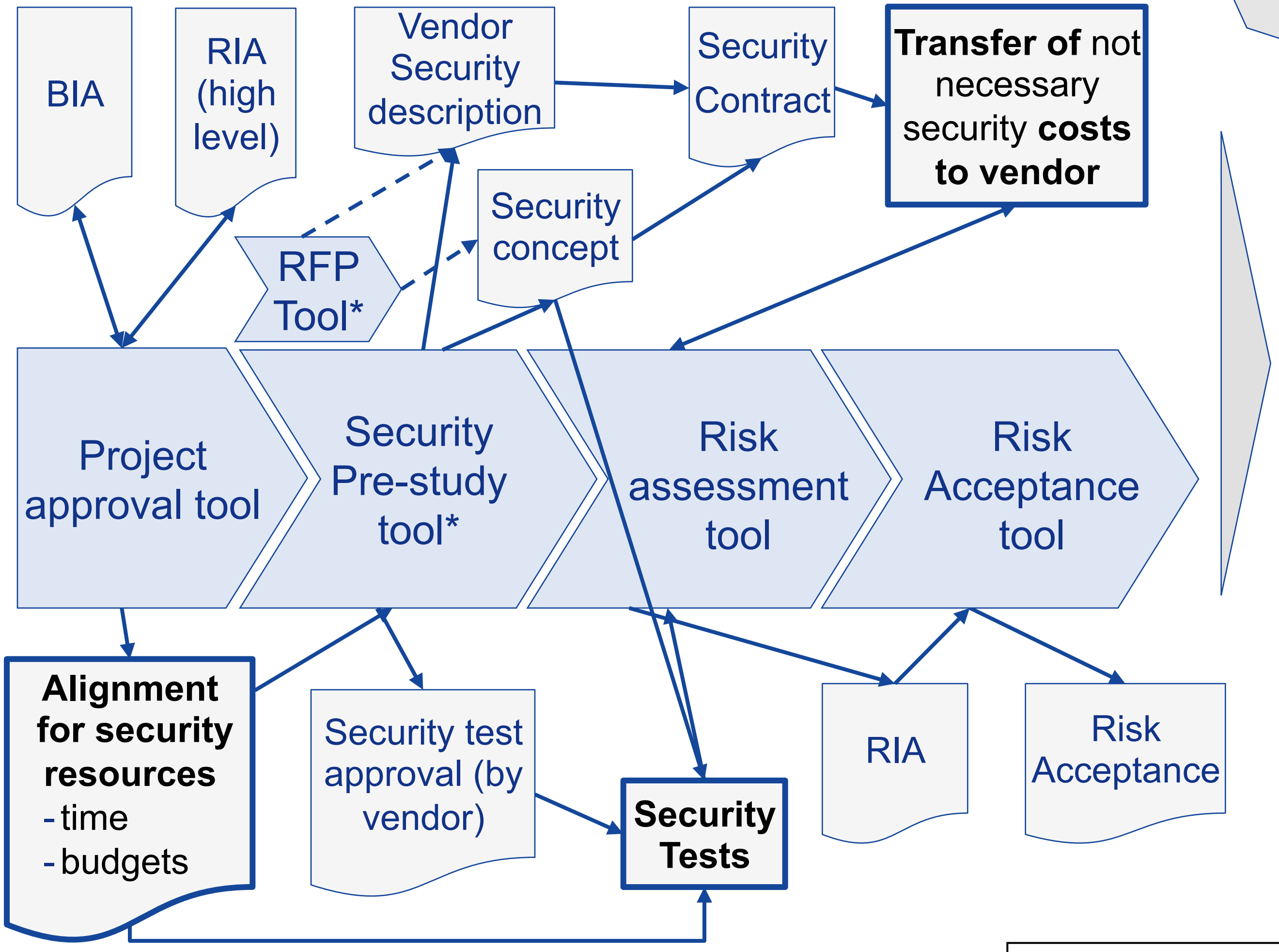
Definition of business and security requirements

Development and assessment of security concept

Regular review of business-needs and security status

Definition of measures to achieve requirements

Security and continuity attachments to SLA/ Contract



BIA

RIA (high level)

Vendor Security description

Security Contract

Transfer of not necessary security **costs to vendor**

RFP Tool*

Security concept

Project approval tool

Security Pre-study tool*

Risk assessment tool

Risk Acceptance tool

Alignment for security resources
- time
- budgets

Security test approval (by vendor)

Security Tests

RIA

Risk Acceptance

General Output

Projects
- in budget
- in time

IT-Systems
- in required security level

* In small projects RFP Tool can be used instead of Security Pre-study tool

Mapping Key security requirements - Tools process steps

a) Early allocation of security resources – budget and time

b) Alignment business to security requirements Review/ Definition of security concept

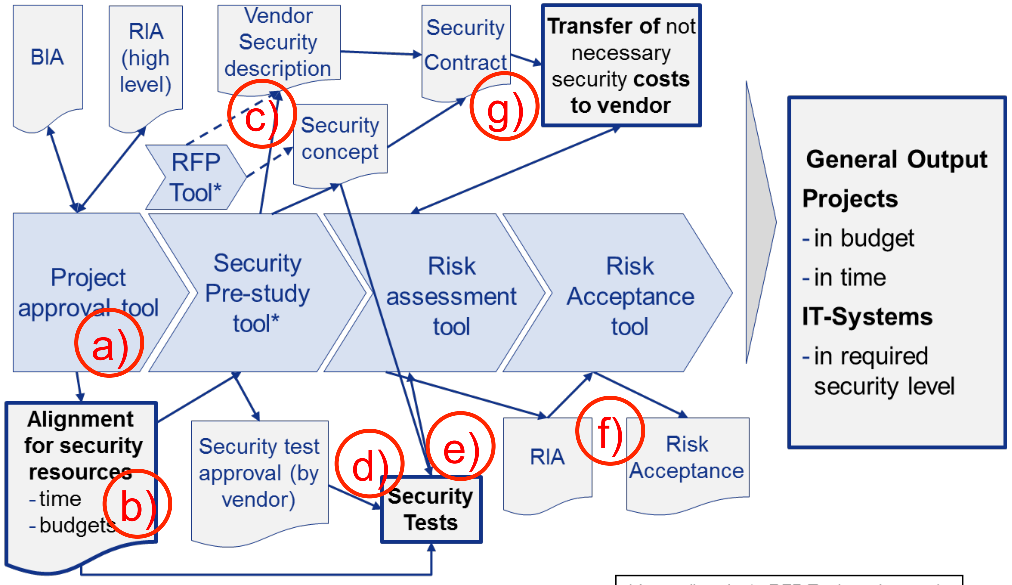
c) Fixation of security level/ measures in detail

d) Performance of security test

e) Identification of security vulnerabilities

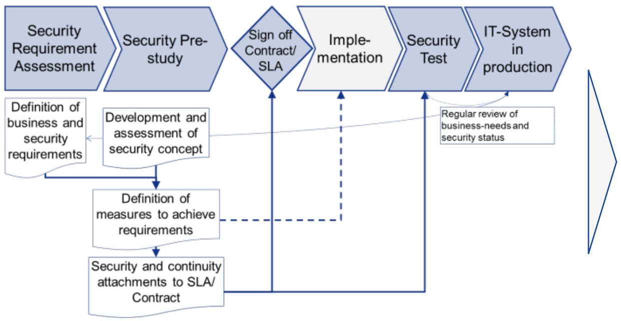
f) Management of risks

g) Costs for vendor-caused security vulnerabilities to be taken over by vendors



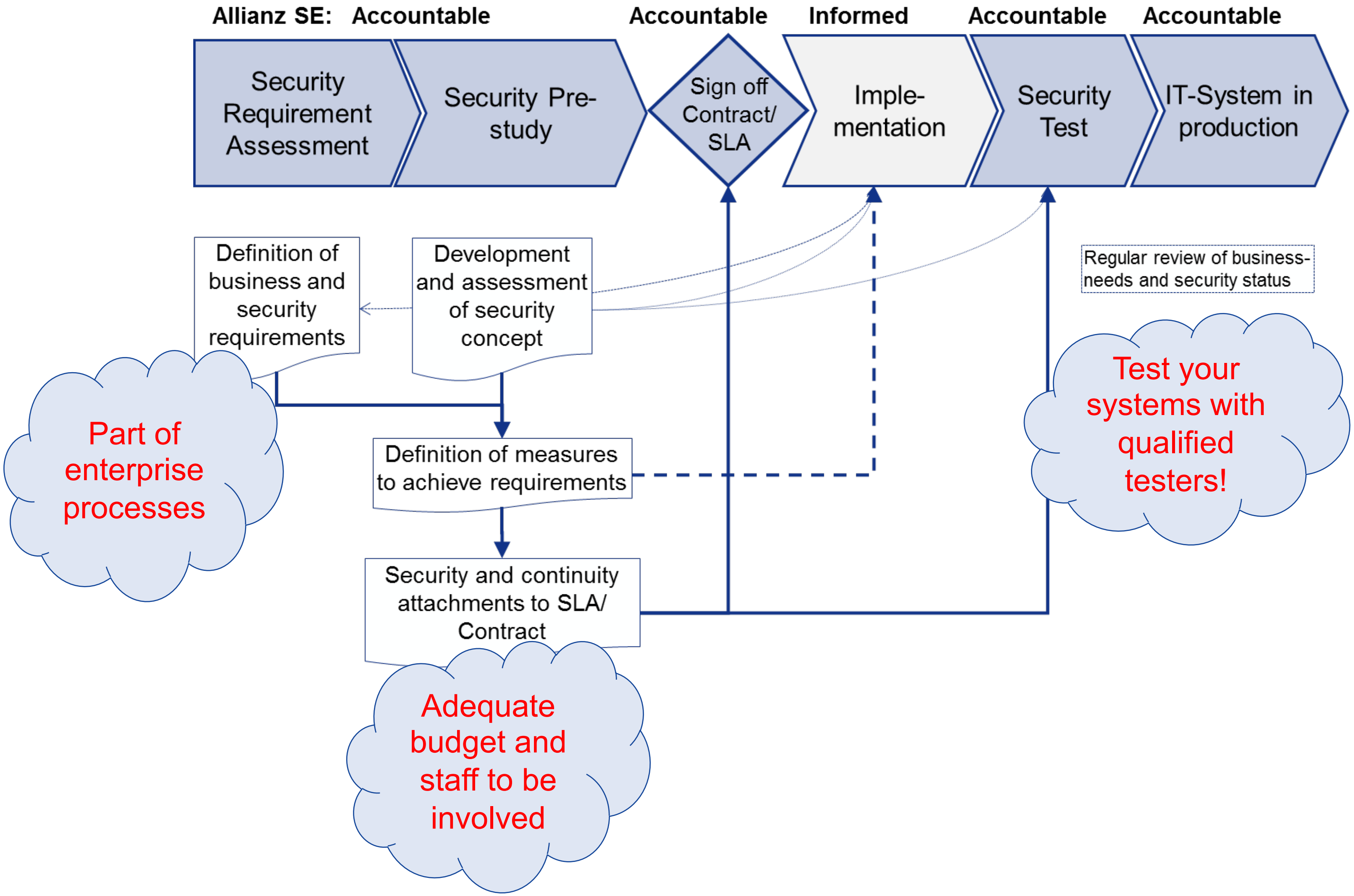
* In small projects RFP Tool can be used instead of Security Pre-study tool

Added-value to Allianz at a glance

Process	Added value		Required
	!	Security Awareness for Service Provider	• Pre-study • Testing
	🤝	IT-system on required security level	• All process steps
	🤝	IT-system on required continuity level	• All process steps
	🤝	Alignment with Business	• All process steps
	€	Heavily reduced risk of unplanned security costs	• Contract/SLA
	⚠	Heavily reduced risk of internal escalations	• Contract/SLA • Testing
	⚠	Heavily reduced risk of external escalations (e.g. Top-management with media)	• Testing

Security Requirement Assessment
Security Pre-study
Sign off Contract/ SLA
Imple-mentation
Security Test
IT-System in production
Definition of business and security requirements
Development and assessment of security concept
Regular review of business-needs and security status
Definition of measures to achieve requirements
Security and continuity attachments to SLA/ Contract

Summary with the 3 most critical process-steps



Allianz SE:
Accountable
Accountable
Informed
Accountable
Accountable
Security Requirement Assessment
Security Pre-study
Sign off Contract/ SLA
Imple-mentation
Security Test
IT-System in production
Definition of business and security requirements
Development and assessment of security concept
Definition of measures to achieve requirements
Security and continuity attachments to SLA/ Contract
Regular review of business-needs and security status

Part of enterprise processes

Test your systems with qualified testers!

Adequate budget and staff to be involved

Thank you very much for your attention!

Any questions?

Hope to see you tonight for a beer!