TOOL

DIALOGUE TOOL

PREPARATION

A detailed guide to support the dialogue with your client around security

INDUSTRIENS FOND

ALEXANDRA INSTITUTTET

AUTHORS

Michael Rømer Bennike, Alexandra Institute

Zaruhi Aslanyan, Alexandra Institute

The Dialogue Tool has been developed by the Sb3D project in collaboration with the following companies:

Mjølner INFORMATICS · Openminds · Prevas Hello Possibility. · TRIFORK. Trifork Digital Health · VERTICA

Partners in the Sb3D project.
The project is funded by the Danish Industry Foundation:

ALEXANDRA INSTITUTE · Erhvervshus MIDTJYLLAND · DANSK ERHVERV · DTU · Dansk Industri · AALBORG UNIVERSITET · Sb3D SECURITY BY DESIGN · INDUSTRIENS FOND

Table of Contents

Purpose of the *Preparation* document

This document is part of the *Dialogue Tool*, together with *Presentation* and *Checklist*.

It comprises a set of questions that are meant to facilitate the conversation on developing secure software between various stakeholders. Each question is coupled with additional guidance that provides context to the question. The scope spans a range of security topics in relation to software development, both as part of the development process itself and in scoping the security capabilities that the software should include.

The *Preparation* document can be used by a software development team to engage with the customer who commissioned the software and address security requirements with them.

Introduction

The below dialogue questions are derived from the OWASP SAMM model. Since the model is intended for maturity assessment and for internal use (rather than customer-developer use) and is not dialogue-oriented, we have selected the relevant questions and refurbished them to support the dialogue more directly. The relevant questions are those that impact the cost of software development and that are up for discussion between the customer and the developer. We suggest a dedicated security scoping meeting between the developer and customer in which the following questions are covered.

Each question abides by the following structure:

a. **Question**
b. **Motivation**
   Why is this question important to address?
c. **Challenges**
   Why can this question difficult to address and what should you be aware of?
d. **Guidance**
   How to approach, interpret and discuss the question?
e. **How to address non-binary answers** (if applicable)
   When the answer is not a hard “yes-or-no”-answer, this section will help reaching consensus. This section may not be equally relevant for all questions.

Dialogue Questions

1. THIRD-PARTY REQUIREMENTS

Source: https://owaspsamm.org/model/governance/policy-and-compliance/

a. Question

What are the external regulatory requirements for the application? (E.g., what are the requirements for data processing, data storing, etc.?).

b. Motivation

Identifying the external compliance requirements that need to be fulfilled ensures that your business follows all the applicable laws and regulations. Moreover, security policies should be built around these requirements.

It is important to know the applicable external requirements as well as to follow them. Not complying with laws and regulations can lead to fines, reputation damage, data breaches, etc.

c. Challenges

While legal requirements should be non-negotiable, the specific approach to reach compliance with legal requirements are still very much up for interpretation, and it is therefore critical that the two parties align on legal requirements and reach a common understanding.

Compliance should be expected to have a high impact on pricing. This is predominantly due to the combination of high level of security requirements set forth by legislation combined with a high burden of proof of conformity. This may include 3rd party audit and certification.

d. Guidance

Start by identifying all the laws and regulations that are applicable for the application. You may need to seek legal counsel or obtain input from internal compliance officers.

You can consider factors such as types of data that is used or stored, geographic location of the company to identify any country specific laws, etc. This step can be prepared beforehand.

e. Addressing non-binary answers

Compliance with many laws and regulations are still up for interpretation. When in doubt, always seek legal counsel. If you struggle to reach consensus, always strive for industry best practices or industry standards that are known to be harmonized with regulatory requirements.

2. ORGANISATIONAL SECURITY REQUIREMENTS

Source: https://owaspsamm.org/model/governance/policy-and-compliance/

a. Question

What are the internal security requirements for software in the organisation?
Are the security requirements aligned with compliance requirements as per the previous question?

b. Motivation

Company security requirements (or a security policy for software) sets a standard for minimum requirements that all applications in the organisation must adhere to. In this way, compliance reporting and security management across the application ecosystem become more uniform.

c. Challenges

A company policy is usually aligned with (or an interpretation of) external requirements. However, the requirements in an internal policy can be deviated from, especially depending on budget constraints. Furthermore, it requires a certain degree of maturity and oversight to implement and enforce a security policy. For this reason, it is not always the case that companies have formal internal guidelines and policies in place that can readily be mapped against a new software design.
As with all policies, there is often room for interpretation on how to achieve conformity, and it is also common to have exceptions where it is not feasible to abide strictly by a policy. While regulatory requirements can be difficult to deviate from, internal policies tend to allow for more leniency, assuming that deviations can be approved by upper management.

d. Guidance

The preparation for this step can be done beforehand: The customer should check with their organisation's security responsible whether they have a security policy that applies to software development and the applications being put into production. Either beforehand or during the session, this policy should be scrutinized and mapped against the software in question. This should result in a relatively strict list of 'non-negotiable' security requirements that are aligned with both the organisation's internal policy and any external/regulatory requirements.
If no policy/requirements exist, the future owner of the software should align expectations with the organisation's security responsible.
It is recommended to include in this step to commit to Security by Design principles when developing the software.

e. Addressing non-binary answers

Similar to 1.e: If you struggle to reach consensus, always strive for industry best practices or industry standards that are known to be harmonized with regulatory requirements. Security policy owner should be able to clarify whether an interpretation is adequate.

3. RISK PROFILE

Source: https://owaspsamm.org/model/design/threat-assessment/stream-a/

a. Question

Do both parties have a common understanding of the risk profile of the application?
I.e., an agreement on the degree of importance of protecting the application from compromise in the context of the sensitive nature of the application and the application's exposure.

b. Motivation

It can be hard to determine what an adequate level of security of an application should be. Reaching a common understanding of the high-level risk profile of an application, i.e., the business-level risks of the application in case the application is compromised, is critical to align expectations between developer and customer. A risk assessment with the business impact in mind helps the customer and the developer to take a step back from the application itself and consider the wider significance of the application. In this way, the risk assessment helps understand and prioritise business-level security requirements which in turn should be reflected in the security budget and risk appetite.

c. Challenges

Performing risk assessments can become very cumbersome, and a detailed assessment may not be fit for purpose for all types of projects, especially not during an early stage. However, it is important to establish a common understanding of the application's overall risk-level and business impact.

d. Guidance

The risk assessment should not necessarily be a full-fledged assessment at this point. Aim to perform the assessment at a very high level and focus on business risks. Specific vulnerabilities and threats to the application should be addressed in the next question.
If the customer has an existing risk framework or standard, you should follow that framework. This ensures that the results are comparable to the rest of the customer's IT ecosystem, which in turn helps prioritise resources for addressing security risks.
If no framework exists in the customer's organisation, the developer may present their framework.
If neither party has an existing framework, you can use the guidance below:
If you can rank each question on a scale of 1-5 where 5 is high risk and 1 is low risk, an average of the combined score is often sufficient for the purpose of this exercise to get a ballpark estimate of the business impact. Sample questions for evaluating the overall risk level of an application:

a. Confidentiality: What is the sensitivity of the data that the application will have access to? For example, will it hold highly sensitive data, intellectual property, trade secrets, personally identifiable data, etc.
b. What are the availability requirements?
c. Exposure: Will the application be internet-facing or internal only?
d. Exposure: Will the application be stand-alone, or will it be integrated with a larger eco system? I.e., can a compromise of the application lead to a compromise of other parts of the infrastructure?
e. Host: Who will host the application and, if it is a third-party, has the security posture of the host been assessed and are adequate SLAs in place?
f. Compromise: Can a compromise of the application lead to regulatory violations and hence to fines?
g. Compromise: What is the reputation impact to your organisation if the application or application data are compromised?
h. Compromise: What is the impact on the users of the application if it is compromised?

e. Addressing non-binary answers

Risk assessments are notoriously difficult to perform with high precision as some variance, bias and assumptions will always impact the assessment. You should accept that a finite answer of the risk can be very difficult to reach and strive to score risks in ranges, e.g., express monetary loss as a range from X-Y and avoid the pitfall of discussing whether a given risk is ‘X’ or ‘Y’ – everything is estimates. Choose a scale to evaluate risks that is granular enough to rank and compare risks, but not so granular that you get stuck in detail. For example, on a high-resolution scale of 1 to 100, a risk being 56 or 57 often doesn’t matter much, and a narrow scale of “low, medium, high” may be too simple to compare and prioritise risks. Something in between, like a scale of 1-5 or 1-10 may be fit for many scenarios.

4. THREAT ASSESSMENT

Source: https://owaspsamm.org/model/design/threat-assessment/stream-b/

a. Question(s)

Is there a common understanding about the risks and/or threats between both parties?
Is there an existing risk assessment or threat modelling or another approach through which the software in question has been assessed?

b. Motivation

Threat modelling is a process that helps an organisation identify security threats and potential vulnerabilities, prioritise them and discuss the possible mitigations. Moreover, it provides a systematic way of analysing and evaluating the threats and defences and allows to identify security requirements.
The process can be used to get the overall picture of the threat landscape to the application. It is also a way of establishing a common language and understanding about the vulnerabilities.

c. Challenges

Threat modelling can be applied in different depths, from a high-level overview to an overly detailed identification of the threats. In this step the focus should be more on the overview of the threats and not so much on the details.

d. Guidance

If there is an existing threat model, use this to start the discussion. If needed, you can consider co-creating a risk assessment/threat model of the software.
If there is no existing threat model, then perform high-level threat modelling. A good starting point can be any existing diagrams, such as system diagram, data flow diagram, etc. You can simply start by brainstorming using a whiteboard or a piece of paper.

There are many threat modelling techniques that one can use. You are free to choose the technique that works for you as there is no universally accepted industry standard for the threat modelling process. Usually, most threat modelling techniques include the following three steps: system modelling, threat identification, and risk response in some form. Each of the steps can have different approaches as well as different levels of detail.

The following three questions can help to structure threat modelling, and they are linked with the three steps mentioned above:

- What are we working on? (system modelling)
- What can go wrong? (threat identification)
- What are we going to do about it? (risk response)

e. Addressing non-binary answers

While there can easily be non-binary answers in this section, use the above guidance to reduce the uncertainty as much as possible.

5. FUNCTIONAL SECURITY REQUIREMENTS

Source: https://owaspsamm.org/model/design/security-requirements/

a. Question

Is there a security requirements specification in place?

a. Are the security requirements aligned with the requirements identified in the *Organisation Security Requirements* question?
b. Are the security requirements aligned with risk and threat assessment results? I.e., for any identified threat/risk that exceeds acceptable severity are adequate security requirements in place to mitigate the risk?
c. Are the security requirements aligned with a security baseline, framework or standard?

b. **Motivation**

This activity aims to establish an understanding of the key security requirements during development. Furthermore, this activity aims to align security expectations with the results from the *Organisation Security Requirements* questions as well as any risk and threat assessments.

c. **Challenges**

It is difficult to identify and describe all security requirements in detail. However, even high-level security requirements can be a great help to design adequate security measures. Aim to make security requirements as specific as possible and to make them measurable so that you can agree on them.

Strive to make security requirements prioritised and distinguish between need-to-have and nice-to-have, so that you can have a discussion about where to draw the line.

d. Guidance

Derive security requirements from functional requirements and customer concerns. The requirements should be as specific and measurable as possible and be aligned with organisational policies and third-party regulatory requirements.

Review the functional requirements of the application to identify relevant security requirements (i.e., expectations) for each functionality. Base the review on the desired degree of protecting Confidentiality, Integrity, and Availability (CIA) of the given application and data.

Requirements should state the *objective* (e.g., “personal data for the registration process should be transferred and stored securely”), but not the *solution* (e.g., “use TLSv1.2 for secure transfer”).

Beware of adding requirements that are too general-purpose to relate to the application at hand (e.g., “the application should protect against the OWASP Top 10”). While they can be true, they don’t add value to the discussion.

e. Addressing non-binary answers

This question should have relatively few non-binary answers. The outcome of the question should be a list of functional security requirements, which can of course be subjective and non-binary. However, since this question does not identify the solutions to the requirements, agreeing on requirements themselves should be fairly straightforward.

6. SECURITY ARCHITECTURE

Source: https://owaspsamm.org/model/design/security-architecture/

a. Question

Do both parties have a common understanding and agreement about their roles in security architecture development?
Have specific security frameworks or standards been chosen to drive the development of the software?
Sub-questions:

- Is the customer involved in the security architecture development process?
- Is the customer involved in the review and testing process?
- Does or should the security architecture consider the customer's existing security policies and guidelines?

b. Motivation

Security architecture is a collection of tools, methods, and security principles for designing and implementing security measures and policies to protect the product from cyberthreats. It translates the business requirements to executable security requirements.
Having a secure product starts by having a strong security architecture. Considering the appropriate security measures in an early stage allows to reduce vulnerabilities and save the cost of handling them later. Strong security architecture incorporates security into every part of the product's lifecycle and helps to decide which technologies are the best fit and when to implement them. Moreover, it ensures compliance with relevant authorities and regulations.

c. Challenges

It can be challenging to determine the appropriate level of security architecture as the effort is potentially uncapped. To strike the balance between cost and benefit, the level of ambition for security architecture should be aligned with the risk assessment efforts to determine adequate architecture goals and be based on risk appetite. For example, how much training is required, how much time should be spent validating and incorporating security by design features, and what is the complexity of frameworks and standards chosen to design the software architecture.

d. Guidance

The main goal of this activity is to agree on the involvement of each party in the security architecture development process. Make sure that the key stakeholders are part of this activity. Depending on how formally you want to approach this, start by identifying architecture design tasks and then assign roles and responsibilities using a RACI matrix etc.
You might also consider discussing the framework and main points of security architecture. Select a security architecture framework that best suits the product and organisation. Start by establishing a solid understanding of the product. Discuss existing technologies, data, users, etc. of the product and gain knowledge about the processes and policies. Consider the business goals/requirements of the customer and think how to integrate them into the security requirements.

e. Addressing non-binary answers

The goal of this question is to eliminate ambiguous answers when it comes to roles and responsibilities for security architecture related questions. For example, after addressing this question there should be clear cut answers to the degree of involvement between customer and developer.

7. SECURITY TESTING AND SOLUTION DEPLOYMENT

Sources: https://owaspsamm.org/model/verification/requirements-driven-testing/
https://owaspsamm.org/model/verification/security-testing/

a. Question

What type of security tests do you need?
What type of security testing do you perform?

- Do you perform testing for correct functioning of security controls?
- Do you perform security testing (both manual and automated/tool based)?
- Do you use any automated security testing tools?
- Who is responsible for each type of testing?
- Will testing be performed at the end of the SDLC or as an integrated part of a CI/CD pipeline?

b. Motivation

Security testing focuses on validating relevant security controls, i.e., to verify that the standard software security controls operate as expected. Moreover, it helps to identify security vulnerabilities and uncover technical implementation weaknesses.
Security testing ensures that the software is free from vulnerabilities that could compromise its functionality, performance, or data integrity. Addressing the identified weaknesses and confirming that the security controls are correctly implemented will help reduce the attack surface.

c. Challenges

There are many challenges that can make security testing difficult, especially limited time and resources, complex scenarios and changing requirements.
Testing tends to suffer if it is placed as a 'big bang' at the end of the SDLC, as the final stages of the SDLC are the most likely to suffer if there are delays or budget overdraft from previous stages. It is important to consider to what degree the software should be continuously tested to avoid discovering severe vulnerabilities close to the deadline.

d. Guidance

Remember that the earlier in the SDLC you can test and detect issues, the cheaper they usually are to fix. With that in mind, to overcome the challenges, the project should be scoped with continuous testing and/or module testing spread throughout the SDLC. Ensure that customer and developer are aligned about testing, that sufficient time and resources for testing are allocated and communicate value and benefits to the customer.
To have a successful testing program, you must agree upon the testing objectives specified by the security requirements. Seek alignment as to how testing is best performed, how extensively it should be performed, and whether the customer should be involved in defining the test-cases for security testing.
Many security vulnerabilities are hard to detect without carefully inspecting the source code. Consider using automated testing tools including factors such as depth and accuracy of inspection, robustness and accuracy of security test cases, available integrations with other tools, usage, and cost model, etc.

e. Addressing non-binary answers

While there can easily be non-binary answers in this section, use the above guidance to reduce the uncertainty as much as possible.

Wrapping up and next steps

After going through the 7 questions, summarise your answers with the customer and discuss the next steps.

With the summary in mind, you should be able to answer the following:

- Do you have a shared understanding of the security requirements for the application?
- Do you have a shared understanding of the distribution of responsibilities between developer and customer?
- Do you think that there are some security aspects of the solution that you still need to cover?
- Are there any areas where you still need additional alignment in relation to the 7 questions?

If you need further clarification and alignment, agree what additional actions you should take to come to an agreement before you end the meeting. For example, you or the customer may feel that you need further cost-benefit analysis, more detailed risk assessment or to consult with other stakeholders in your respective organisations.

Document any decisions that you make and specify the actions that need to be carried out to reach consensus so that you can follow up on this later.