Engenharia de Segurança

13 de Abril de 2021

Grupo 7	
a83899	André Morais
a84485	Tiago Magalhães

Prática 1 - Aula 05

Mestrado Integrado em Engenharia Informática
Universidade do Minho

Conteúdo

1 Secure Software Development Lifecycle (S-SDLC) 2

1.1 Pergunta 1.1 2

1.2 Pergunta 1.3 2

2 SAMM (Software Assurance Maturity Model) 3

2.1 Pergunta 2.1 3

2.2 Pergunta 2.2 5

2.3 Pergunta 2.3 6

1 Secure Software Development Lifecycle (S-SDLC)

1.1 Pergunta 1.1

No modelo *Microsoft Security Development Lifecycle* é na **Fase de Requisitos** que se deve ter por base a legislação em vigor como é o caso do regulamento europeu RGPD, devendo ser traduzidos em requisitos específicos para o *software* a desenvolver.

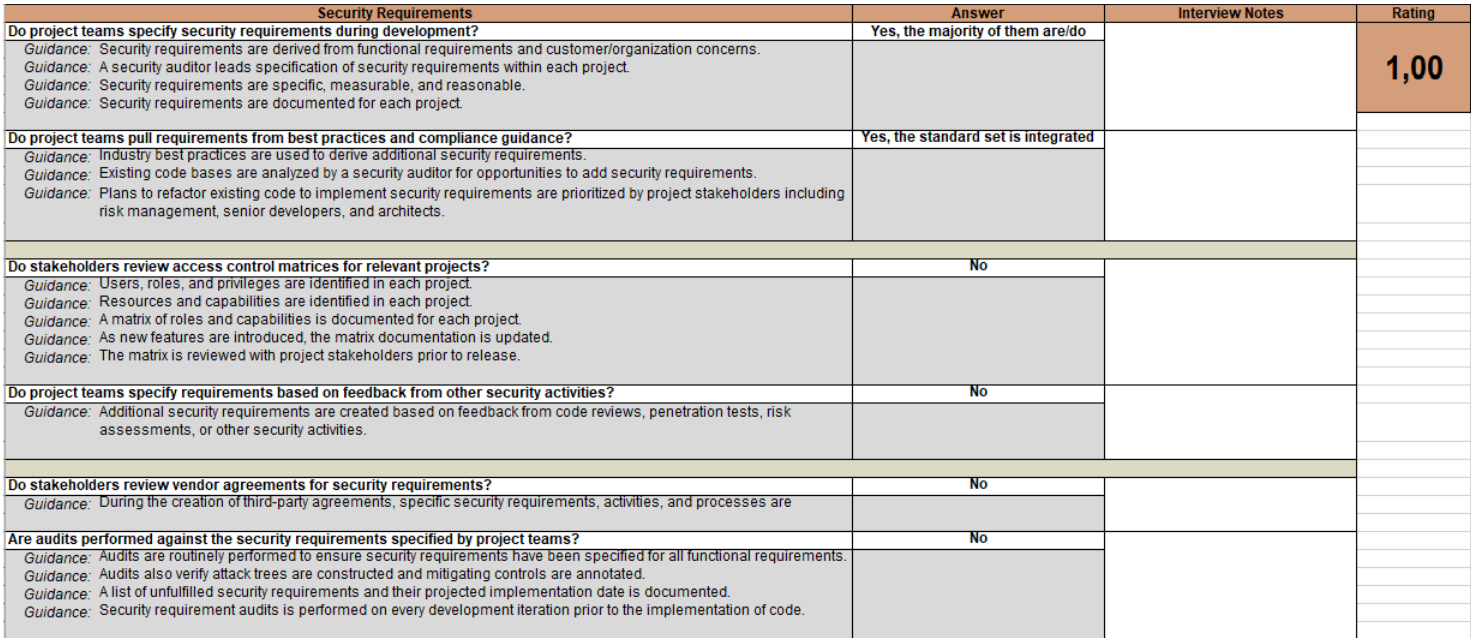
1.2 Pergunta 1.3

Visto que o nosso grupo é composto apenas por 2 elementos, não é possível englobar todos as funções e responsabilidades de segurança como no SDLC. Mesmo assim, as funções que vamos realizar são as mais vocacionadas com a programação e a arquitetura do projeto, como por exemplo:

- **Software Developer**
- **System Architect**
- **Program Manager / Official (Information Owner)**

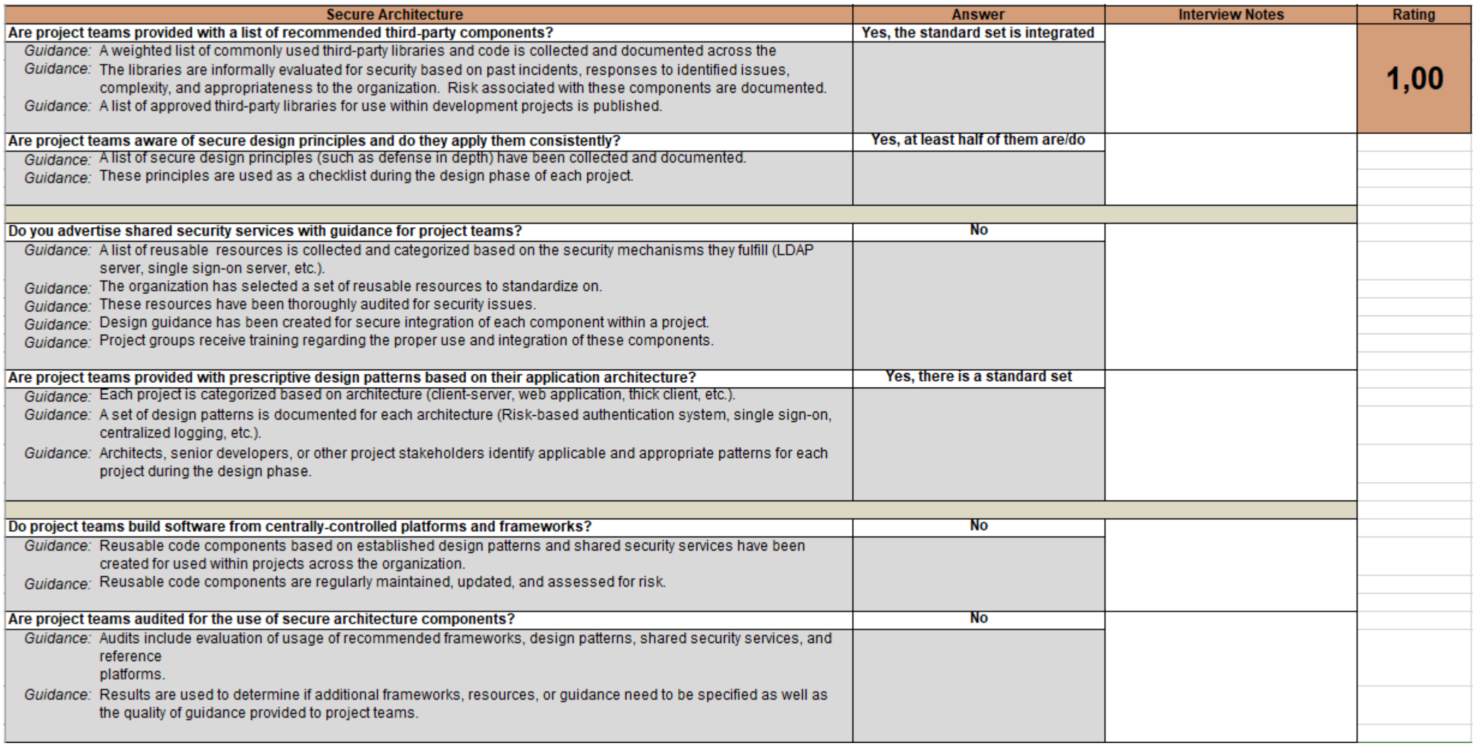
2 SAMM (Software Assurance Maturity Model)

2.1 Pergunta 2.1



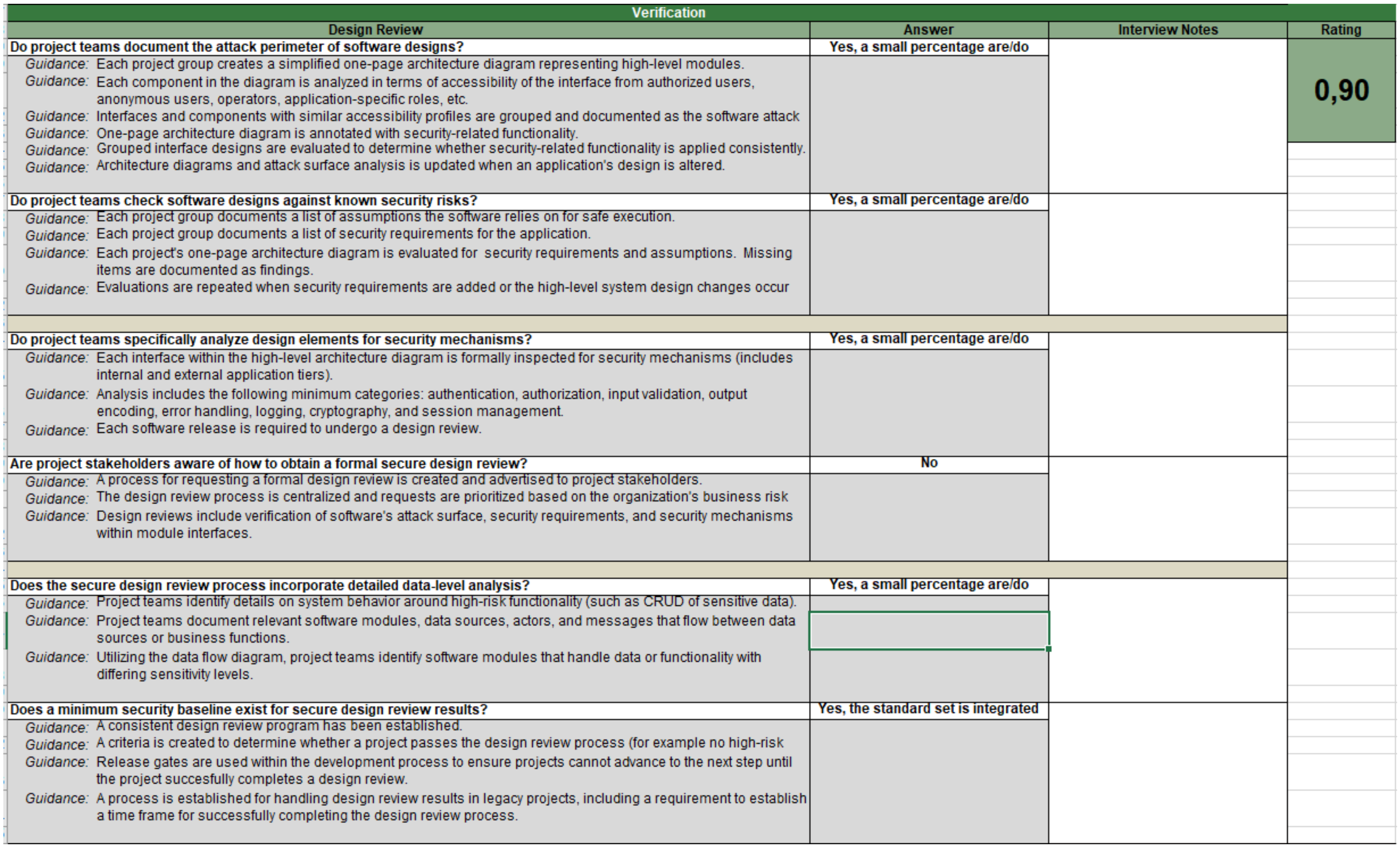
Security Requirements	Answer	Interview Notes	Rating
Do project teams specify security requirements during development?	**Yes, the majority of them are/do**		**1,00**
Guidance: Security requirements are derived from functional requirements and customer/organization concerns. *Guidance:* A security auditor leads specification of security requirements within each project. *Guidance:* Security requirements are specific, measurable, and reasonable. *Guidance:* Security requirements are documented for each project.			
Do project teams pull requirements from best practices and compliance guidance?	**Yes, the standard set is integrated**		
Guidance: Industry best practices are used to derive additional security requirements. *Guidance:* Existing code bases are analyzed by a security auditor for opportunities to add security requirements. *Guidance:* Plans to refactor existing code to implement security requirements are prioritized by project stakeholders including risk management, senior developers, and architects.			
Do stakeholders review access control matrices for relevant projects?	**No**		
Guidance: Users, roles, and privileges are identified in each project. *Guidance:* Resources and capabilities are identified in each project. *Guidance:* A matrix of roles and capabilities is documented for each project. *Guidance:* As new features are introduced, the matrix documentation is updated. *Guidance:* The matrix is reviewed with project stakeholders prior to release.			
Do project teams specify requirements based on feedback from other security activities?	**No**		
Guidance: Additional security requirements are created based on feedback from code reviews, penetration tests, risk assessments, or other security activities.			
Do stakeholders review vendor agreements for security requirements?	**No**		
Guidance: During the creation of third-party agreements, specific security requirements, activities, and processes are			
Are audits performed against the security requirements specified by project teams?	**No**		
Guidance: Audits are routinely performed to ensure security requirements have been specified for all functional requirements. *Guidance:* Audits also verify attack trees are constructed and mitigating controls are annotated. *Guidance:* A list of unfulfilled security requirements and their projected implementation date is documented. *Guidance:* Security requirement audits is performed on every development iteration prior to the implementation of code.			

Figura 1: Security Requirements



Secure Architecture	Answer	Interview Notes	Rating
Are project teams provided with a list of recommended third-party components?	**Yes, the standard set is integrated**		**1,00**
Guidance: A weighted list of commonly used third-party libraries and code is collected and documented across the *Guidance:* The libraries are informally evaluated for security based on past incidents, responses to identified issues, complexity, and appropriateness to the organization. Risk associated with these components are documented. *Guidance:* A list of approved third-party libraries for use within development projects is published.			
Are project teams aware of secure design principles and do they apply them consistently?	**Yes, at least half of them are/do**		
Guidance: A list of secure design principles (such as defense in depth) have been collected and documented. *Guidance:* These principles are used as a checklist during the design phase of each project.			
Do you advertise shared security services with guidance for project teams?	**No**		
Guidance: A list of reusable resources is collected and categorized based on the security mechanisms they fulfill (LDAP server, single sign-on server, etc.). *Guidance:* The organization has selected a set of reusable resources to standardize on. *Guidance:* These resources have been thoroughly audited for security issues. *Guidance:* Design guidance has been created for secure integration of each component within a project. *Guidance:* Project groups receive training regarding the proper use and integration of these components.			
Are project teams provided with prescriptive design patterns based on their application architecture?	**Yes, there is a standard set**		
Guidance: Each project is categorized based on architecture (client-server, web application, thick client, etc.). *Guidance:* A set of design patterns is documented for each architecture (Risk-based authentication system, single sign-on, centralized logging, etc.). *Guidance:* Architects, senior developers, or other project stakeholders identify applicable and appropriate patterns for each project during the design phase.			
Do project teams build software from centrally-controlled platforms and frameworks?	**No**		
Guidance: Reusable code components based on established design patterns and shared security services have been created for used within projects across the organization. *Guidance:* Reusable code components are regularly maintained, updated, and assessed for risk.			
Are project teams audited for the use of secure architecture components?	**No**		
Guidance: Audits include evaluation of usage of recommended frameworks, design patterns, shared security services, and reference platforms. *Guidance:* Results are used to determine if additional frameworks, resources, or guidance need to be specified as well as the quality of guidance provided to project teams.			

Figura 2: Secure Architecture



Verification			
Design Review	**Answer**	**Interview Notes**	**Rating**
Do project teams document the attack perimeter of software designs?	**Yes, a small percentage are/do**		**0,90**
Guidance: Each project group creates a simplified one-page architecture diagram representing high-level modules. *Guidance:* Each component in the diagram is analyzed in terms of accessibility of the interface from authorized users, anonymous users, operators, application-specific roles, etc. *Guidance:* Interfaces and components with similar accessibility profiles are grouped and documented as the software attack *Guidance:* One-page architecture diagram is annotated with security-related functionality. *Guidance:* Grouped interface designs are evaluated to determine whether security-related functionality is applied consistently. *Guidance:* Architecture diagrams and attack surface analysis is updated when an application's design is altered.			
Do project teams check software designs against known security risks?	**Yes, a small percentage are/do**		
Guidance: Each project group documents a list of assumptions the software relies on for safe execution. *Guidance:* Each project group documents a list of security requirements for the application. *Guidance:* Each project's one-page architecture diagram is evaluated for security requirements and assumptions. Missing items are documented as findings. *Guidance:* Evaluations are repeated when security requirements are added or the high-level system design changes occur			
Do project teams specifically analyze design elements for security mechanisms?	**Yes, a small percentage are/do**		
Guidance: Each interface within the high-level architecture diagram is formally inspected for security mechanisms (includes internal and external application tiers). *Guidance:* Analysis includes the following minimum categories: authentication, authorization, input validation, output encoding, error handling, logging, cryptography, and session management. *Guidance:* Each software release is required to undergo a design review.			
Are project stakeholders aware of how to obtain a formal secure design review?	**No**		
Guidance: A process for requesting a formal design review is created and advertised to project stakeholders. *Guidance:* The design review process is centralized and requests are prioritized based on the organization's business risk *Guidance:* Design reviews include verification of software's attack surface, security requirements, and security mechanisms within module interfaces.			
Does the secure design review process incorporate detailed data-level analysis?	**Yes, a small percentage are/do**		
Guidance: Project teams identify details on system behavior around high-risk functionality (such as CRUD of sensitive data). *Guidance:* Project teams document relevant software modules, data sources, actors, and messages that flow between data sources or business functions. *Guidance:* Utilizing the data flow diagram, project teams identify software modules that handle data or functionality with differing sensitivity levels.			
Does a minimum security baseline exist for secure design review results?	**Yes, the standard set is integrated**		
Guidance: A consistent design review program has been established. *Guidance:* A criteria is created to determine whether a project passes the design review process (for example no high-risk *Guidance:* Release gates are used within the development process to ensure projects cannot advance to the next step until the project succesfully completes a design review. *Guidance:* A process is established for handling design review results in legacy projects, including a requirement to establish a time frame for successfully completing the design review process.			

Figura 3: Design Review

2.2 Pergunta 2.2

- **Security Requirements**: Esperamos uma pequena melhoria no que diz respeito as matrizes de controlo de acesso. Quanto aos outros fatores, não se aplicam no nosso caso. *Rating* esperado é de **1,50**.
- **Secure Architecture**: Pretendemos melhorar pelo menos para um *Rating* de **1,50**.
- **Design Review**: Planeamos um *Rating* de **1,50** nesta prática de segurança.

2.3 Pergunta 2.3

Encontra-se no Excel presente no github