Design

		Threat Assessment		Answer			Interview Notes	Rating
Application Risk Profile	1	**Do you classify applications according to business risk based on a simple and predefined set of questions?** An agreed-upon risk classification exists The application team understands the risk classification The risk classification covers critical aspects of business risks the organization is facing The organization has an inventory for the applications in scope	B	Yes, most or all of them	1	1.000		3.00
	2	**Do you use centralized and quantified application risk profiles to evaluate business risk?** The application risk profile is in line with the organizational risk standard The application risk profile covers impact to security and privacy You validate the quality of the risk profile manually and/or automatically The application risk profiles are stored in a central inventory	A	Yes, for most or all of the applications	1	1.000		
	3	**Do you regularly review and update the risk profiles for your applications?** The organizational risk standard considers historical feedback to improve the evaluation method Significant changes in the application or business context trigger a review of the relevant risk profiles	R	Yes, at least annually	1	1.000		
Threat Modeling	1	**Do you identify and manage architectural design flaws with threat modeling?** You perform threat modeling for high-risk applications You use simple threat checklists, such as STRIDE You persist the outcome of a threat model for later use	B	Yes, most or all of them	1			
	2	**Do you use a standard methodology, aligned on your application risk levels?** You train your architects, security champions, and other stakeholders on how to do practical threat modeling Your threat modeling methodology includes at least diagramming, threat identification, design flaw mitigations, and how to validate your threat model artifacts Changes in the application or business context trigger a review of the relevant threat models You capture the threat modeling artifacts with tools that are used by your application teams	A	Yes, for most or all of the applications	1			
	3	**Do you regularly review and update the threat modeling methodology for your applications?** The threat model methodology considers historical feedback for improvement You regularly (e.g., yearly) review the existing threat models to verify that no new threats are relevant for your applications You automate parts of your threat modeling process with threat modeling tools	P	Yes, we review it at least annually	1			
		Security Requirements		**Answer**			**Interview Notes**	**Rating**
Software Requirements	1	**Do project teams specify security requirements during development?** Teams derive security requirements from functional requirements and customer or organization concerns Security requirements are specific, measurable, and reasonable Security requirements are in line with the organizational baseline	A	Yes, for most or all of the applications	1	1.000		3.00
	2	**Do you define, structure, and include prioritization in the artifacts of the security requirements gathering process?** Security requirements take into consideration domain specific knowledge when applying policies and guidance to product development Domain experts are involved in the requirements definition process You have an agreed upon structured notation for security requirements Development teams have a security champion dedicated to reviewing security requirements and outcomes	E	Yes, most or all of the time	1	1.000		
	3	**Do you use a standard requirements framework to streamline the elicitation of security requirements?** A security requirements framework is available for project teams The framework is categorized by common requirements and standards-based requirements The framework gives clear guidance on the quality of requirements and how to describe them The framework is adaptable to specific business requirements	A	Yes, for most or all of the applications	1	1.000		
Supplier Security	1	**Do stakeholders review vendor collaborations for security requirements and methodology?** You consider including specific security requirements, activities, and processes when creating third-party agreements A vendor questionnaire is available and used to assess the strengths and weaknesses of your suppliers	E	Yes, most or all of the time	1			
	2	**Do vendors meet the security responsibilities and quality measures of service level agreements defined by the organization?** You discuss security requirements with the vendor when creating vendor agreements Vendor agreements provide specific guidance on security defect remediation within an agreed upon timeframe The organization has a templated agreement of responsibilities and service levels for key vendor security processes You measure key performance indicators	E	Yes, most or all of the time	1			
	3	**Are vendors aligned with standard security controls and software development tools and processes that the organization utilizes?** The vendor has a secure SDLC that includes secure build, secure deployment, defect management, and incident management that align with those used in your organization You verify the solution meets quality and security objectives before every major release When standard verification processes are not available, you use compensating controls such as software composition analysis and independent penetration testing	E	Yes, most or all of the time	1			
		Secure Architecture		**Answer**			**Interview Notes**	**Rating**
Architecture Design	1	**Do teams use security principles during design?** You have an agreed upon checklist of security principles You store your checklist in an accessible location Relevant stakeholders understand security principles	A	Yes, for most or all of the applications	1	1.000		3.00
	2	**Do you use shared security services during design?** You have a documented list of reusable security services, available to relevant stakeholders You have reviewed the baseline security posture for each selected service Your designers are trained to integrate each selected service following available guidance	A	Yes, for most or all of the applications	1	1.000		
	3	**Do you base your design on available reference architectures?** You have one or more approved reference architectures documented and available to stakeholders You improve the reference architectures continuously based on insights and best practices You provide a set of components, libraries, and tools to implement each reference architecture	A	Yes, for most or all of the applications	1	1.000		
Technology Management	1	**Do you evaluate the security quality of important technologies used for development?** You have a list of the most important technologies used in, or in support of, each application You identify and track technological risks You ensure the risks to these technologies are in line with the organizational baseline	A	Yes, for most or all of the applications	1			
	2	**Do you have a list of recommended technologies for the organization?** The list is based on technologies used in the software portfolio Lead architects and developers review and approve the list You share the list across the organization You review and update the list at least yearly	M	Yes, for most or all of the technology domains	1			
	3	**Do you enforce the use of recommended technologies within the organization?** You monitor applications regularly for the correct use of the recommended technologies You solve violations against the list accoranding to organizational policies You take action if the number of violations falls outside the yearly objectives	A	Yes, for most or all of the applications	1			

Implementation

		Secure Build		Answer			Interview Notes	Rating
Build Process	1	**Is your full build process formally described?** You have enough information to recreate the build processes Your build documentation up to date Your build documentation is stored in an accessible location Produced artifact checksums are created during build to support later verification You harden the tools that are used within the build process	A	Yes, for most or all of the applications	1	1.000		3.00
	2	**Is the build process fully automated?** The build process itself doesn't require any human interaction Your build tools are hardened as per best practice and vendor guidance You encrypt the secrets required by the build tools and control access based on the principle of least privilege	A	Yes, for most or all of the applications	1	1.000		
	3	**Do you enforce automated security checks in your build processes?** Builds fail if the application doesn't meet a predefined security baseline You have a maximum accepted severity for vulnerabilities You log warnings and failures in a centralized system You select and configure tools to evaluate each application against its security requirements at least once a year	A	Yes, for most or all of the applications	1	1.000		
Software Dependencies	1	**Do you have solid knowledge about dependencies you're relying on?** You have a current bill of materials (BOM) for every application You can quickly find out which applications are affected by a particular CVE You have analyzed, addressed, and documented findings from dependencies at least once in the last three months	A	Yes, for most or all of the applications	1			
	2	**Do you handle 3rd party dependency risk by a formal process?** You keep a list of approved dependencies that meet predefined criteria You automatically evaluate dependencies for new CVEs and alert responsible staff You automatically detect and alert to license changes with possible impact on legal application usage You track and alert to usage of unmaintained dependencies You reliably detect and remove unnecessary dependencies from the software	A	Yes, for most or all of the applications	1			
	3	**Do you prevent build of software if it's affected by vulnerabilities in dependencies?** Your build system is connected to a system for tracking 3rd party dependency risk, causing build to fail unless the vulnerability is evaluated to be a false positive or the risk is explicitly accepted You scan your dependencies using a static analysis tool You report findings back to dependency authors using an established responsible disclosure process Using a new dependency not evaluated for security risks causes the build to fail	A	Yes, for most or all of the applications	1			
		Secure Deployment		**Answer**			**Interview Notes**	**Rating**
Deployment Process	1	**Do you use repeatable deployment processes?** You have enough information to run the deployment processes Your deployment documentation up to date Your deployment documentation is accessible to relevant stakeholders You ensure that only defined qualified personnel can trigger a deployment You harden the tools that are used within the deployment process	A	Yes, for most or all of the applications	1	1.000		3.00
	2	**Are deployment processes automated and employing security checks?** Deployment processes are automated on all stages Deployment includes automated security testing procedures You alert responsible staff to identified vulnerabilities You have logs available for your past deployments for a defined period of time	A	Yes, for most or all of the applications	1	1.000		
	3	**Do you consistently validate the integrity of deployed artifacts?** You prevent or roll back deployment if you detect an integrity breach The verification is done against signatures created during the build time If checking of signatures is not possible (e.g. externally build software), you introduce compensating measures	A	Yes, for most or all of the applications	1	1.000		
	1	**Do you limit access to application secrets according to the least privilege principle?**	A	Yes, for most or all of the applications	1			

Secret Management		You store production secrets protected in a secured location Developers do not have access to production secrets Production secrets are not available in non-production environments						
	2	**Do you inject production secrets into configuration files during deployment?** Source code files no longer contain active application secrets Under normal circumstances, no humans access secrets during deployment procedures You log and alert when abnormal secrets access is attempted	A	**Yes, for most or all of the applications**	1			
	3	**Do you practice proper lifecycle management for application secrets?** You generate and synchronize secrets using a vetted solution Secrets are different between different application instances Secrets are regularly updated	A	**Yes, for most or all of the applications**	1			
		Defect Management		**Answer**			**Interview Notes**	**Rating**
Defect Tracking	1	**Do you track all known security defects in accessible locations?** You can easily get an overview of all security defects impacting one application You have at least a rudimentary classification scheme in place The process includes a strategy for handling false positives and duplicate entries The defect management system covers defects from various sources and activities	A	**Yes, for most or all of the applications**	1	1.000		**3.00**
	2	**Do you keep an overview of the state of security defects across the organization?** A single severity scheme is applied to all defects across the organization The scheme includes SLAs for fixing particular severity classes You regularly report compliance to SLAs	A	**Yes, for most or all of the applications**	1	1.000		
	3	**Do you enforce SLAs for fixing security defects?** You automatically alert of SLA breaches and transfer respective defects to the risk management process You integrate relevant tooling (e.g. monitoring, build, deployment) with the defect management system	A	**Yes, for most or all of the applications**	1	1.000		
Metrics and Feedback	1	**Do you use basic metrics about recorded security defects to carry out quick win improvement activities?** You analyzed your recorded metrics at least once in the last year At least basic information about this initiative is recorded and available You have identified and carried out at least one quick win activity based on the data	A	**Yes, for most or all of the applications**	1			
	2	**Do you improve your security assurance program upon standardized metrics?** You document metrics for defect classification and categorization and keep them up to date Executive management regularly receives information about defects and has acted upon it in the last year You regularly share technical details about security defects among teams	A	**Yes, for most or all of the applications**	1			
	3	**Do you regularly evaluate the effectiveness of your security metrics so that its input helps drive your security strategy?** You have analyzed the effectiveness of the security metrics at least once in the last year Where possible, you verify the correctness of the data automatically The metrics is aggregated with other sources like threat intelligence or incident management You derived at least one strategic activity from the metrics in the last year	A	**Yes, for most or all of the applications**	1			
Verification								
		Architecture Assessment		**Answer**			**Interview Notes**	**Rating**
Architecture Validation	1	**Do you review the application architecture for key security objectives on an ad-hoc basis?** You have an agreed upon model of the overall software architecture You include components, interfaces, and integrations in the architecture model You verify the correct provision of general security mechanisms You log missing security controls as defects	A	**Yes, for most or all of the applications**	1	1.000		**3.00**
	2	**Do you regularly review the security mechanisms of your architecture?** You review compliance with internal and external requirements You systematically review each interface in the system You use a formalized review method and structured validation You log missing security mechanisms as defects	A	**Yes, for most or all of the applications**	1	1.000		
	3	**Do you regularly review the effectiveness of the security controls?** You evaluate the preventive, detective, and response capabilities of security controls You evaluate the strategy alignment, appropriate support, and scalability of security controls You evaluate the effectiveness at least yearly You log identified shortcomings as defects	A	**Yes, for most or all of the applications**	1	1.000		
Architecture Mitigation	1	**Do you review the application architecture for mitigations of typical threats on an ad-hoc basis?** You have an agreed upon model of the overall software architecture Security savvy staff conduct the review You consider different types of threats, including insider and data-related ones	A	**Yes, for most or all of the applications**	1			
	2	**Do you regularly evaluate the threats to your architecture?** You systematically review each threat identified in the Threat Assessment Trained or experienced people lead review exercise You identify mitigating design-level features for each identified threat You log unhandled threats as defects	A	**Yes, for most or all of the applications**	1			
	3	**Do you regularly update your reference architectures based on architecture assessment findings?** You assess your architectures in a standardized, documented manner You use recurring findings to trigger a review of reference architectures You independently review the quality of the architecture assessments on an ad-hoc basis You use reference architecture updates to trigger reviews of relevant shared solutions, in a risk-based manner	A	**Yes, for most or all of the applications**	1			
		Requirements Testing		**Answer**			**Interview Notes**	**Rating**
Control Verification	1	**Do you test applications for the correct functioning of standard security controls?** Security testing at least verifies the implementation of authentication, access control, input validation, encoding and escaping data, and encryption controls Security testing executes whenever the application changes its use of the controls	B	**Yes, most or all of them**	1	1.000		**3.00**
	2	**Do you consistently write and execute test scripts to verify the functionality of security requirements?** You tailor tests to each application and assert expected security functionality You capture test results as a pass or fail condition Tests use a standardized framework or DSL	B	**Yes, most or all of them**	1	1.000		
	3	**Do you automatically test applications for security regressions?** You consistently write tests for all identified bugs (possibly exceeding a pre-defined severity threshhold) You collect security tests in a test suite that is part of the existing unit testing framework	A	**Yes, for most or all of the applications**	1	1.000		
Misuse/Abuse Testing	1	**Do you test applications using randomization or fuzzing techniques?** Testing covers most or all of the application's main input parameters You record and inspect all application crashes for security impact on a best-effort basis	A	**Yes, for most or all of the applications**	1			
	2	**Do you create abuse cases from functional requirements and use them to drive security tests?** Important business functionality has corresponding abuse cases You build abuse stories around relevant personas with well-defined motivations and characteristics You capture identified weaknesses as security requirements	E	**Yes, most or all of the time**	1			
	3	**Do you perform denial of service and security stress testing?** Stress tests target specific application resources (e.g. memory exhaustion by saving large amounts of data to a user session) You design tests around relevant personas with well-defined capabilities (knowledge, resources) You feed the results back to the Design practices	E	**Yes, most or all of the time**	1			
		Security Testing		**Answer**			**Interview Notes**	**Rating**
Scalable Baseline	1	**Do you scan applications with automated security testing tools?** You dynamically generate inputs for security tests using automated tools You choose the security testing tools to fit the organization's architecture and technology stack, and balance depth and accuracy of inspection with usability of findings to the organization	B		0	0.500		**2.50**
	2	**Do you customize the automated security tools to your applications and technology stacks?** You tune and select tool features which match your application or technology stack You minimize false positives by silencing or automatically filter irrelevant warnings or low probability findings You minimize false negatives by leverage tool extensions or DSLs to customize tools for your application or organizational standards	B	**Yes, most or all of them**	1	1.000		
	3	**Do you integrate automated security testing into the build and deploy process?** Management and business stakeholders track and review test results throughout the development cycle You merge test results into a central dashboard and feed them into defect management	X	**Yes, most or all of it**	1	1.000		
Deep Understanding	1	**Do you manually review the security quality of selected high-risk components?** Criteria exist to help the reviewer focus on high-risk components Qualified personnel conduct reviews following documented guidelines You address findings in accordance with the organization's defect management policy	G	**Yes, for most or all of the components**	1			
	2	**Do you perform penetration testing for your applications at regular intervals?** Penetration testing uses application-specific security test cases to evaluate security Penetration testing looks for both technical and logical issues in the application Stakeholders review the test results and handle them in accordance with the organization's risk management Qualified personnel performs penetration testing	A	**Yes, for most or all of the applications**	1			
	3	**Do you use the results of security testing to improve the development lifecycle?** You use results from other security activities to improve integrated security testing during development You review test results and incorporate them into security awareness training and security testing playbooks Stakeholders review the test results and handle them in accordance with the organization's risk management	Y	**Yes, we improve it at least annually**	1			