	Design Threat Assessment 1 Do you classify applications according to business risk based on a simple and predefined set of questions?	В	Answer Yes, most or all of them	1	1.000	Interview Notes	Rating
	An agreed-upon risk classification exists The application team understands the risk classification		res, most or all of trieffi		1.000	1	3.00
	The risk classification covers critical aspects of business risks the organization is facing The organization has an inventory for the applications in scope						3.00
Application Risk	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.	Α	Yes, for most or all of the applications	1	1.000		
Profile	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 3 Do you regularly review and update the risk profiles for your applications?	R	Yes, at least annually	1	1.000		
	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	ı.	ros, at least annually		1.000		
	Do you identify and manage architectural design flaws with threat modeling?	В	Yes, most or all of them	1			
Threat Modeling	You perform threat modeling for high-risk applications You use simple threat checklists, such as STRIDE		res, most of all of alem				
	You persist the outcome of a threat model for later use Do you use a standard methodology, aligned on your application risk levels?	A	Yes, for most or all of the applications	1			
	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 3 Do you regularly review and update the threat modeling methodology for your applications?	P	Yes, we review it at least annually	1			
	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		res, we review it at least aimain				
	You automate parts of your threat modeling process with threat modeling tools Security Requirements		Answer			Interview Notes	Rating
	Do project teams specify security requirements during development? Teams derive security requirements from functional requirements and customer or organization concerns	Α	Yes, for most or all of the applications	1	1.000		
	Security requirements are specific, measurable, and reasonable Security requirements are in line with the organizational baseline						3.00
	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	E	Yes, most or all of the time	1	1.000		
Software Requirements	Domain experts are involved in the requirements definition process You have an agreed upon structured notation for security requirements						
	Development learns have a security champion dedicated to reviewing security requirements and outcomes 3 Do you use a standard requirements framework to streamline the elicitation of security requirements?	A	Yes, for most or all of the applications	1	1.000		
	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						
	Do stakeholders review vendor collaborations for security requirements and methodology?	E	Yes, most or all of the time	1			
	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						
	Do vendors meet the security responsibilities and quality measures of service level agreements defined by the organization?	E	Yes, most or all of the time	1			
	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		res, most of all of the time				
Supplier	The organization has a templated agreement of responsibilities and service levels for key vendor security processes You measure key performance indicators						
Security	Are vendors aligned with standard security controls and software development tools and processes that the organization utilizes?						
	3	E	Yes, most or all of the time	1			
	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 metes 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						
	Secure Architecture		Answer		4.000	Interview Notes	Rating
	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	A	Yes, for most or all of the applications	1	1.000		3.00
	Relevant stakeholders understand security principles						0.00
Architecture	Do you use shared security services during design? You have a documented list of reusable security services, available to relevant stakeholders	A	Yes, for most or all of the applications	1	1.000		
Design	You have reviewed the baseline security posture for each selected service Your designers are trained to integrate each selected service following available guidance						
	Do you base your design on available reference architectures? You have one or more approve reference architectures documented and available to stakeholders You improve the reference architectures continuously based on insights and best practices	A	Yes, for most or all of the applications	1	1.000	-	
	You provide a set of components, libraries, and tools to implement each reference architecture						
	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	Α	Yes, for most or all of the applications	1			
	You nave a list of the most important technologies used in, or in support or, each application You identify and track technological risks You ensure the risks to these technologies are in line with the organizational baseline						
	Do you have a list of recommended technologies for the organization?	м	Yes, for most or all of the technology domains	1			
Technology	The list is based on technologies used in the software portfolio Lead architects and developers review and approve the list		uomans				
Management	You share the list across the organization You review and update the list at least yearly						
	Do you enforce the use of recommended technologies within the organization? You monitor applications regularly for the correct use of the recommended technologies	А	Yes, for most or all of the applications	1			
	You solve violations against the list accoranding to organizational policies You take action if the number of violations falls outside the yearly objectives						
	Implementation Secure Build		Answer			Interview Notes	Rating
	Is your full build process formally described? You have enough information to recreate the build processes	Α	Yes, for most or all of the applications	1	1.000		
	Your build documentation up to date Your build documentation is stored in an accessible location						3.00
	Produced artifact checksums are created during build to support later verification You harden the tools that are used within the build process						
Build Process	2 Is the build process fully automated? The build process itself doesn't require any human interaction	Α	Yes, for most or all of the applications	1	1.000		
	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						
	Do you enforce automated security checks in your build processes? Builds fail if the application doesn't meet a predefined security baseline	Α	Yes, for most or all of the applications	1	1.000		
	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						
	Do you have solid knowledge about dependencies you're relying on? You have a current bill of materials (BOM) for every application	Α	Yes, for most or all of the applications	1			
	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						
	Do you handle 3rd party dependency risk by a formal process? You keep a list of approved dependencies that meet predefined criteria	Α	Yes, for most or all of the applications	1			
Software	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						
Dependencies	You track and alert to usage of unmaintained dependencies You reliably detect and remove unnecessary dependencies from the software						
	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	Α	Yes, for most or all of the applications	1			
	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						
	Secure Deployment Do you use repeatable deployment processes?	A	Answer Yes, for most or all of the applications	1	1.000	Interview Notes	Rating
	You have enough information to run the deployment processes Your deployment documentation up to date	Ė	, a approaudiis				2.00
	Your deployment documentation is accessible to relevant stakeholders You ensure that only defined qualified personnel can trigger a deployment						3.00
	You harden the tools that are used within the deployment process 2 Are deployment processes automated and employing security checks?	Δ	Yes, for most or all of the applications	1	1.000		
Deployment Process	Deployment processes are automated on all stages Deployment includes automated security testing procedures	Ĺ	, ror most or an or the applications		1.000	1	
	Vou alert responsible staff to identified vulnerabilities You have logs available for your past deployments for a defined period of time						
	Do you consistently validate the integrity of deployed artifacts? You prevent or roll back deployment if you detect an integrity breach	А	Yes, for most or all of the applications	1	1.000		
	Too provers or roll back deproyment if you detect all integrity breated						
	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						
	The verification is done against signatures created during the build time if thecking displantures in the possible (e.g. activatel) build software), you introduce compensating measures 1 Do you limit access to application secrets according to the least privilege principle?		Yes, for most or all of the applications	1			

	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 Do you inject production secrets into configuration files during deployment?		Ver forward as all of the applications	1			_
Secret	Source code files no longer contain active application secrets	A	Yes, for most or all of the applications	1			
Management	Under normal circumstances, no humans access secrets during deployment procedures You log and alert when abnormal secrets access is attempted						
	3 Do you practice proper lifecycle management for application secrets? You generate and synchronize secrets using a vetted solution	Α	Yes, for most or all of the applications	1			
	Secrets are different between different application instances Secrets are regularly updated						
	Defect Management		Answer			Interview Notes	Rating
	Do you track all known security defects in accessible locations? You can easily get an overview of all security defects impacting one application	A	Yes, for most or all of the applications	1	1.000		
	You have at least a rudimentary classification scheme in place The process includes a strategy for handling false positives and duplicate entries						3.00
	The defect management system covers defects from various sources and activities 2 Do you keep an overview of the state of security defects across the organization?		Ver forward as all of the analizations	1	1.000		
Defect Tracking	A single severity scheme is applied to all defects across the organization	^	Yes, for most or all of the applications		1.000		
	The scheme includes SLAs for fixing particular severity classes You regularly report compliance to SLAs						
	3 Do you enforce SLAs for fixing security defects? You automatically alert of SLA breaches and transfer respective defects to the risk management process	A	Yes, for most or all of the applications	1	1.000		
	You integrate relevant tooling (e.g. monitoring, build, deployment) with the defect management system	1					4
	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	Α	Yes, for most or all of the applications	1			7
	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						
	2 Do you improve your security assurance program upon standardized metrics?	А	Yes, for most or all of the applications	1			1
Metrics and	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						
Feedback	You regularly share technical details about security defects among teams Do you regularly evaluate the effectiveness of your security metrics so that its input helps drive your security strategy?	_	Yes, for most or all of the applications	1			4
	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	Ê	res, for most or all of the applications				
	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						
	Verification						
	Architecture Assessment Do you review the application architecture for key security objectives on an ad-hoc basis?	A	Answer Yes, for most or all of the applications	1	1.000	Interview Notes	Rating
	You have an agreed upon model of the overall software architecture You include components, interfaces, and integrations in the architecture model						3.00
	You verify the correct provision of general security mechanisms You log missing security controls as defects						0.00
	Do you regularly review the security mechanisms of your architecture? You review compliance with internal and external requirements	Α	Yes, for most or all of the applications	1	1.000		
Architecture Validation	You systematically review each interface in the system You use a formalized review method and structured validation						
	You log missing security mechanisms as defects						
	3 Do you regularly review the effectiveness of the security controls? You evaluate the preventive, detective, and response capabilities of security controls	Α	Yes, for most or all of the applications	1	1.000		
	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						_
	1 Do you review the application architecture for mitigations of typical threats on an ad-hoc basis?	Α	Yes, for most or all of the applications	1			7
	You have an agreed upon model of the overall software architecture Security savvy staff conduct the review						
	Very analysis different transport in the first includes a single conduction of the c						1
	You consider different types of threats, including insider and data-related ones Do you regularly evaluate the threats to your architecture?	A	Yes, for most or all of the applications	1			-
Architecture	You consider different types of threats, including insider and data-related ones Do you regularly evaluate the threats to your architecture? You systematically review each threat identified in the Threat Assessment Tained or recovering cell could lead review exceptions.	A	Yes, for most or all of the applications	1			
Architecture Mitigation	Do you regularly evaluate the threats to your architecture? You systematically review each threat identified in the Threat Assessment	A	Yes, for most or all of the applications	1			_
	2 Do your 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 unhanded threats as defects 3 Do you regularly update your reference architectures based on architecture assessment findings?		Yes, for most or all of the applications Yes, for most or all of the applications	1			
	2 Do you regularly evaluate the threats to your architecture? You systematically review earth threat identified in the Threat Assessment Trained or experienced people lead review exercise You identify militagring design-level features for each identified threat You log unhanded threats as defects 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 trigeer are view of reference architectures.			1			_
	2 Do your 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 miligating design-level features for each identified threat You log unhanded threats as defects 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 were reference architecture updates to trigger reviews or ferevent shared solutions, in a risk-based manner		Yes, for most or all of the applications	1			-
	2 Do you regularly evaluate the threats to your architecture? You systematically review earth threat identified in the Threat Assessment Trained or experienced people lead review exercise You identify militagring design-level features for each identified threat You log unhanded threats as defects 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 or ference 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 Requirements Testing 1 Do you test applications for the correct functioning of standard security controls?			1	1.000	Interview Notes	Rating
	2 Do you regularly valuate the threats to your architecture? You systematically review earth threat identified in the Threat Assessment Trained or experienced people lead review exercise You identify militagring design-level features for each identified threat You log unhanded threats as defects You seems your architectures in a standardized, documented manner You assess your architectures in a standardized, documented manner You use recurring findings to trigger a review or freence architectures You independently review the quality of the architecture assessments on an ad-hoc basis You use reference architecture updates to trigger reviews or features thater doubtons, in a risk-based manner Requirements Teating 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.	A	Yes, for most or all of the applications Answer	1	1.000	Interview Notes	Rating 3.00
Mitigation	2 Do your 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 led with mighting design-level features for each identified threat You leg unhanded threats as defects 3 Do you gregularly update your reference architectures based on architecture assessment findings? You assess your architectures in a standardized, documented manner You use recruiting findings to fittinger a review of reference architectures You use recruiting findings to fittinger a review of reference architectures You use reference architecture updates to trigger reviews of relevant elements and advictors, in a risk-based manner You use reference architecture updates to trigger reviews of relevant elements disclores, in a risk-based manner Beguirements Teatter 1 Do you test applications for the correct functioning of standard security controls? Security testing at seast vertises the implementation of authentication, access control, nput validation, encoding and escaping data, and encryption controls.	В	Yes, for most or all of the applications Answer Yes, most or all of them	1		Interview Notes	
	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 mightaging design-level features for each identified threat. You log unhanded threats as defects 3 Do you orgularly 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 some your control of the properties of the properties of the properties of the properties of the your services of reviews that are discloses, in a risk-based manner 10 Do you test applications for the correct functioning of standard security controls? Security install, services the implementation of authentication, access control, injut validation, encoding and escaping data, and encryption controls. 2 Do you consistently write and execute test scripts to verify the functionality of security requirements? You take tests to each application and asset respected security functionality of security requirements? You take tests to each application and asset respected executive functionality of security requirements?	A	Yes, for most or all of the applications Answer	1	1.000	Interview Notes	
Mitigation	2 Do your 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 led unhanded threats as defects You long unhanded threats as defects 3 Do you orgularly 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 in a standardized, documented manner You use recurring findings to trigger a review of reference architectures You undependently review the quality of the architecture assessments on an ad-noc basis You use reference architectures updates to logger reviews of reviews the area of the control of the architecture assessments on a reference architecture updates to logger reviews of reviews thated solutions, in a risk-based manner 8 Requirements Testing Society is unique to the standardized, documented as a standardized framework that production of authoritecture, access control, input validation, encoding and escaping data, and encryption controls. 9 Society is useful great assessment or the control of the control of Society in the standardized framework or policient on dangers is use of the controls. 9 Do you consistently write and execute test scripts to verify the functionality of security requirements? You take treats to each application and asset respected security functionality. 10 Test use a standardized effortment of the Control of the cont	B	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them	1	1.000	Interview Notes	
Mitigation	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 milipating design-level features for each identified threat You log unhanded threats as defects 3 Do you gregularly 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 architectures assessments on an ad-hoc basis You use reference architecture updates to trigger review or ferevant sheet solutions, in a risk-based manner **Requirements** Testing 1 Do you test applications for the correct functioning of standard security controls? **Security senting at least verifies the implementation of authentication, access control, input validation, encoding and escaping data, and **Security testing executes whenever the application changes its use of the controls You to live test on each application and asset reported security functionality of security requirements? You consistently write and execute test scripts to verify the functionality of security requirements? You consistently write set of all condition. Tests use a standardized featuremook or DSL. 3 Do you automatically test applications for security regressions? You consistently write set of all identified busing possably according a pre-defined severity threshold)	B	Yes, for most or all of the applications Answer Yes, most or all of them	1		Interview Notes	
Mitigation	2 Do you regularly variable the threats to your architecture? You systematically review earth threat identified in the Threat Assessment Trained or experienced people lead review exercise You identify milegating design-level features for each identified threat You log unhanded threats as defects You assess your architectures in a standardized, documented threat You assess your architectures in a standardized, documented manner You are recurring findings to trigger a review or ference architectures You independently review the quality of the architecture assessments on an ad-hoc basis You use reference architecture updates to trigger review or ference architectures You independently review the quality of the architecture assessments on an ad-hoc basis You use reference architecture updates to trigger review or ference architectures Requirements Testing 1 Do you test applications for the correct functioning of standard security controls? Security testing a teast verifies the implementation of authentication, access control, input validation, encoding and escaping data, and encryption controls Security testing accustes whenever the application changes its use of the controls 2 Do you consistently write and execute test scripts to verify the functionality of security requirements? You tailor test to each application and assert expected security functionality You capture test results as a pass or fall condition Tests use a standardized framework or DSL. Do you stomatically test application for security repressions?	B	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them	1	1.000	Interview Notes	
Mitigation	2 Do your regularly evaluate the threats to your architecture? Vox systematically review each threat identified in the Threat Assessment Trained or experienced people lead review exercise You lead threat mighting design-level features for each identified threat You log unhanded threats as defects 3 Do you regularly update your reference architectures based on architecture assessment findings? You assess your architectures in a standardized, documented manner You see recurring findings to trigger a review of reference architectures You independently review the quality of the architecture assessments on an ad-hoc basis You see reference architecture updates to trigger eviews of reference hards described to the standardized. You see reference architecture updates to trigger eviews of reference hards described to the standard security controls? 8 Requirements Testing 1 Do you test applications for the correct functioning of standard security controls? Security lesting at least verifies the implementation of authentication, access control, input validation, encoding and escaping data, and encryption controls Security lesting are such asplication changes its use of the controls 2 Do you consistently write and execute test scripts to verify the functionality of security requirements? You tailor tests to each application and assent appeted security functionality Tests use a standardized firmenovic or DS. 3 Do you automatically test applications for security regressione? You collect security lests in a test suite that is part of the existing unit testing framework 1 Do you test applications using randomization or fuzzing techniques? Festing covers most or all of the applications and injured parameters.	B B	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them	1	1.000	Interview Notes	
Mitigation	2 Do your 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 lead or experienced people lead review exercise You lead through mighting design-level features for each identified threat You lead unhanded threats as defects 3 Do you gregularly update your reference architectures based on architecture assessment findings? You assess your architectures in a standardized, documented manner You see recurring findings to oftgee a review of reference architectures You see recurring findings to fittings a review of reference architectures You use reference architecture updates to trigger reviews of relevant elevations, in a risk-based manner You use reference architecture updates to trigger reviews of relevant elevations, in a risk-based manner Requirements Teating 1 Do you set applications for the correct functioning of standard security controls? Security stering a seast verties the implementation of authentication access control, riput validation, encoding and escaping data, and encryption controls. Security stering a seast verties the implementation of authentication access control of authentication access control of authentication access controls? You consistently write and execute test scripts to verify the functionality of security requirements? You consistently write and execute test scripts to verify the functionality of security requirements? You consistently write as for all scriptions for security regressions? You consistently test application and asset expected security functionality You colored a standardized direction and asset expected security functionality You colored the control of authentication or recurrity regressions? You consistently write sets for all scriptified tops (possibly exceeding a pre-defined severity threshold) You colored according report all signified tops (or vertified to the signified tops and the set such balls by a colored and inspect all application	B	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them Yes, for most or all of the applications Yes, for most or all of the applications	1 1 1 1	1.000	Interview Notes	
Mitigation Control Verification Misuse/Abuse	2 Do your regularly vealuate the threats to your architecture? You systematically review each threat identified in the Threat Assessment Trained or experienced people lead review exercise You led unhanded threats as defects 3 Do you gregularly update your reference architectures based on architecture assessment findings? You assess your architectures in a standardized, documented manner You see recurring fundings to trigger a review of reference architectures You be recurring fundings to trigger a review of reference architectures You be received as the standardized documented manner You see relevance architecture in publication of the standardized documented with the standardized of the standardized standardized of the standardized of the standardized standardized of the standardized of the standardized standar	B B	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them Yes, for most or all of the applications	1 1 1	1.000	Interview Notes	
Mitigation Control Verification	2 Do your regularly vealuate the threats to your architecture? You systematically review each threat identified in the Threat Assessment Trained or experienced people lead review exercise You led with mightaing design-level features for each identified threat You log unhanded threats as defects 3 Do you gregularly update your reference architectures based on architecture assessment findings? You assess your architectures in a standardized, documented manner You see recurring fundings to rigger a review of reference architectures You see recurring fundings to rigger a review of reference architectures You see recurring fundings to rigger a review of reference architectures You see receive the receive architecture in the reference architectures You see reference architecture puddes to rigger are view of reference architectures You see reference architecture suptains to rigger are view of reference architectures You see reference architecture puddes to rigger are view of reference architectures. You therefore a reference puddes to rigger a review of reference architectures. You see the reference architecture puddes to rigger are view of reference architectures. You can be referenced as the reference architecture architecture. Security seeing at least verifies the implementation of architecture assessments on an advance or reference architecture. Security seeing as called verifies the implementation of architectures. Security seeing as least verifies the implementation of architectures. Security seeing as called verifies to review the application and asset respected security functionality. You consistently write and execute test scripts to verify the functionality of security requirements? You consistently write sets or all condition Tests us a standardized arrhimetor. Architecture architecture architecture architecture architecture architecture. You consistently write sets or all identified bugs (assable vasceding a pre-defined severity freshold) You collect security tests in a test such that is part of the exis	B B	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them Yes, for most or all of the applications Yes, for most or all of the applications Yes, most or all of the time	1 1 1 1 1 1	1.000	Interview Notes	
Mitigation Control Verification Misuse/Abuse	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 led unhanded threats as defects You long unhanded threats as defects 3 Do you gregularly update your reference architectures based on architecture assessment findings? You assess your architectures in a standardized, documented manner You see recurring findings to trigger a review or freence architectures You be recurring findings to trigger a review or freence architectures You undependently review the quality of the architecture assessments on an ad-noc basis You use reference architectures updates to logging reviews or freence architectures You be reference architecture updates for logging reviews or freence architectures 1 Do you test applications for the correct functioning of standards security controls? 2 Do you consistently write and execute test scripts to verify the functionality of security requirements? You use free tests to each application and assest respected security functionality You capture test results as a pass or fall condition Tests use a standardized farmework or DSL. 3 Do you automatically test applications for security regressions? You consistently write set of a identified bogs (possibly exceeding a pre-defined severity threshold) You collect security tests in a test such that is part of the existing unit testing framework 1 Do you test applications using randomization or fuzzing techniques? 1 Festing covers most or all of the applications may input parameters 2 Important paper and the properties of the security regressions? 2 Important paper and the security remains an earth or force security tests in a test such that is part of the existing unit testing framework 2 Do you perform dentified sessions as executive greatesting as well than the part of the existing unit testing framework. 3 Do you perform dentified sessions as executive greatesting? 3 Do you perform dentified sessions	B	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them Yes, for most or all of the applications Yes, for most or all of the applications	1 1 1 1	1.000	Interview Notes	
Mitigation Control Verification Misuse/Abuse	2 Do you regularly vealuate the threats to your architecture? You systematically review earth threat identified in the Threat Assessment Trained or experienced people leaf review exercise You lead threat mighting designate-level features for each identified threat You log unhanded threats as defects 3 Do you regularly update your reference architectures based on architecture assessment findings? You assess your architectures in a standardized, documented manner You see recurring findings to trigger a review or ference architectures You independently review the quality of the architecture assessments on an ad-hoc basis You see reference architecture updates to trigger eviews or ferevant shared solutions, in a risk-based manner Requirements Testing 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. 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 passo of fall condition You consistently write tests for a passo of all conditions 3 Do you automatically test and execute test security regressions? You consistently write tests for as all dentified bugs (possibly exceeding a pre-defined severity finished) You collect exocity fests in a least such that is pain judge techniques? Testing owns most of all of the applications for description with less finished framework. 1 Do you sationatically test the section of the excellent unit testing framework. 2 Do you continued the section of the section of the excellent put it lessing framework. 2 Do you continued the section of the section of the excellent on the test of the testing on the testing framework.	B B	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them Yes, for most or all of the applications Yes, for most or all of the applications Yes, most or all of the time	1 1 1 1 1 1	1.000	Interview Notes	
Mitigation Control Verification Misuse/Abuse	2 Do you regularly vealuate the threats to your architecture? You splanntacilly review earth threat identified in the Threat Assessment Trained or experienced people leaf review exercise You long urhanded threats as defects You long urhanded threats as defects You long urhanded threats as defects You assess your architectures in a standardized, documented manner You see requirally update your reference architectures based on architecture assessment findings? You assess your architectures in a standardized, documented manner You be recurring findings to trigger a review of reference architectures You independently review the quality of the architecture assessments on an ad-hoc basis You see reference architecture updates to trigger eviews of relevant shared solutions, in a risk-based manner Requirements Testing 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 lesting executes whenever the application of anges its use of the controls 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 consistently write and execute test scripts to verify the functionality You consistently write tests for a said identified bugs (possibly exceeding a pre-defined severity threshold) You collect execute the security as seasor of all conditions 1 Do you sutomatically test applications for security regressions? You consistently write tests for all identified bugs (possibly exceeding a pre-defined severity threshold) You collect executy tests in a less stude that is a principle and in the security sets of the exceeding unit lesting framework. 1 Do you sutomatically test a set such that is a principlement and use them to drive security tests? Important business functionally has corresponding a	B B	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them Yes, for most or all of the applications Yes, for most or all of the applications Yes, most or all of the time	1 1 1 1 1 1	1.000	Interview Notes	
Mitigation Control Verification Misuse/Abuse	2 Do your regularly vealuate the threats to your architecture? You systematically review each threat identified in the Threat Assessment Trained or experienced people lead review exercise You length mighting design-level features for each identified threat You log unhanded threats as defects 3 Do you gregularly update your reference architectures based on architecture assessment findings? You assess your architectures in a standardized, documented manner You are contring findings to ortigen a review of reference architectures You are contring findings to fittinger a review of reference architectures You use reference architectures updates to trigger reviews of relevant shared solutions, in a risk-based manner You use reference architecture updates to trigger reviews of relevant shared solutions, in a risk-based manner Requirements Teating 1 Do you set applications for the correct functioning of standard security controls? Security stering at seast vertices the implementation of authentication, access control or, input validation, encoding and escaping data, and encryption controls. Security stering a seast vertices the implementation of authentication, access control or, input validation, encoding and escaping data, and encryption controls. Security stering a seast vertice to each application and assest respected security functionality of security requirements? You copius tests to each application and assest respected security functionality. You copius tests to each application and assest respected security functionality. You copius tests to each application and assest septed security functionality. You collect security results as a pass or fall condition. Tests use a standardized direction and assest septed assecting vertices and the security of the security security regressions? You collect security feats in a set such that is part of the excelleng and testing assessment of the sequilication and security setting assessment of the application ransin input parameters. You build abuse stories and unique relati	B B A A E E	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them Yes, for most or all of the applications Yes, for most or all of the applications Yes, most or all of the time	1 1 1 1 1 1	1.000		3.00
Mitigation Control Verification Misuse/Abuse	2 Do your regularly vealuate the threats to your architecture? You systematically review each threat identified in the Threat Assessment Trained or experienced people lead review exercise You length mighting designationed leathers for each identified threat You log unhanded threats as defects 3 Do you gregularly update your reference architectures based on architecture assessment findings? You assess your architectures in a standardized, documented manner You see recurring findings to originar enview of reference architectures You see recurring findings to trigger a review of reference architectures You use reference architectures updates to trigger reviews of relevant shared solutions, in a risk-based manner You use reference architecture updates to trigger reviews of relevant shared solutions, in a risk-based manner Requirements Teating 1 Do you set applications for the correct functioning of standard security controls? Security stering at seast vertices the implementation of authentication, access control or, input validation, encoding and escaping data, and encryption controls. Security stering a security resists the implementation of authentication, access control or, input validation, encoding and escaping data, and encryption controls. Security stering a security seek the implementation of authentication, access control or, input validation, encoding and escaping data, and encryption controls. 2 Do you consistently write and execute test scripts to verify the functionality of security requirements? You copier test results as a pass or fall condition. Tests use a standardized farience of a discribited by the controls. 3 Do you automatically test applications for security regressions? You collect socioly feets in a set such but is part of the excelleng and testing framework. 1 Do you sutomatically test applications for security regressions? You social and impact all application crashes for security intentional value in the security tests? Important business functionally has corresponding abuse cases Y	A B B B B B B B B B B B B B B B B B B B	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them Yes, most or all of the applications Yes, for most or all of the applications Yes, most or all of the time Yes, most or all of the time Answer	1 1 1 1 1 1 0	1.000		3.00
Control Verification Misuse/Abuse Testing	2 Do your regularly vealuate the threats to your architecture? You systematically review each threat identified in the Threat Assessment Trained or experienced people lead review exercise You led with mightaing design-level features for each identified threat You log unhanded threats as defects 3 Do you gregalant yudeta your reference architectures based on architecture assessment findings? You assess your architectures in a standardized, documented manner You see recurring fundings to rigger a review of reference architectures You see recurring fundings to rigger a review of reference architectures You see recurring fundings to rigger a review of reference architectures You see receiving fundings to rigger a review of reserved and the standardized, documented manner You see reference architectures updates to rigger review of reviews of several shared solutions, in a risk-based manner You see reference architectures updates to rigger review of reviews of several shared solutions, in a risk-based manner Security retirence architectures updates to rigger review of reviews of several shared solutions, in a risk-based manner You see reference architectures updates to rigger a review of reviews of several shared solutions, in a risk-based manner Security retirency and reviews of several security controlor? Socially setting at least unfiles the implementation of authentication, access controlor? Socially setting as excess whenever the application and seaset repected security functionality of security requirements? You consistently write and accessed test set stripts to verify the functionality of security requirements? You consistently write and accessed security functionality of security requirements? You consistently write and execute test scripts to verify the security functionality of security requirements? You consistently write and execute test scripts to verify the functionality of security requirements? You consistently write as for all identified bugs glocosably exceeding a pre-defined severity threshold) Yo	B B A A E E	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them Yes, for most or all of the applications Yes, for most or all of the applications Yes, most or all of the time	1 1 1 1 1 1	1.000		3.00
Misuse/Abuse Testing	2 Do you regularly vealuate the threats to your architecture? You speaminately review each threat identified in the Threat Assessment Trained or experienced people lead review exercise You identify militagrid equiti-purel estures for each identified threat You log unhanded threats as defects You sees your architectures in a standardized, documented marner You see requiratly update you reference architectures based on architecture assessment findings? You assess your architectures in a standardized, documented marner You see recurring findings to trigger a review or ference architectures You independently review the quality of the architectures assessments on an ad-hoc basis You we reference architecture updates to trigger reviews or freely athered southors, in a risk-based manner Requirements Testing 1 Do you test applications for the correct functioning of standard security controls? Security setting at least verifies the implementation of authentication, access control, input validation, encoding and escaping data, and Security testing executes whenever the application changes its use of the controls Security testing executes whenever the application changes its use of the controls You to be used to be a standardized framework or DSL. 2 Do you consistently write and execute test scripts to verify the functionality of security requirements? You copture test results as a pass or fall condition. Tests use a standardized framework or DSL. 3 Do you automatically test applications for security regressions? You consistently write sets for all conditions. Tests use a standardized framework or DSL. 4 Do you cutomatically test applications for security regressions? You copture test results as a pass or fall condition. Tests use a standardized framework or DSL. 5 Do you cutomatically test applications are standardized framework or DSL. 5 Do you copture test results as a pass or fall condition and passed as a pass of the scartify tests and testing unit testing framework 6 DSL over a copture test results as a pass	A B B B B B B B B B B B B B B B B B B B	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them Yes, most or all of the applications Yes, for most or all of the applications Yes, most or all of the time Yes, most or all of the time Answer	1 1 1 1 1 1 0	1.000		3.00
Control Verification Misuse/Abuse Testing	2 Do you regularly evaluate the threats to your architecture? You speamatically review each threat identified in the Threat Assessment Trained or experienced people lead review exercise You led unhanded threats as defects You led with mightaing design-level features for each identified threat You log unhanded threats as defects 3 Do you gregularly update your reference architectures based on architecture assessment findings? You assess your architectures in a standardized, documented manner You see recurring findings to trigger a review of reference architectures You independently review the quality of the architectures assessments on an ad-hoc basis You were reference architecture updates to trigger reviews or frelevant shared solutions, in a risk-based manner Requirements Testing 1 Do you test applications for the correct functioning of standard security controls? Security leasting at least verifies the implementation of authentication, access control, input validation, encoding and escaping data, and expert the security in the security are security in the security requirements? 1 Do you consistently write and execute test scripts to verify the functionality of security requirements? 1 To you consistently write and execute test scripts to verify the functionality of security requirements? 1 Do you automatically test applications for security regressions? 2 Do you automatically test applications for security regressions? 2 You consistently write test for all identified bugs possably acceeding a pre-diffied severity threshold) 2 Do you consistently write test for all identified bugs possably acceeding a pre-diffied severity threshold; 3 Do you provide the security security and provide the security security in the secu	A B B B B B B B B B B B B B B B B B B B	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them Yes, most or all of the applications Yes, for most or all of the applications Yes, most or all of the time Yes, most or all of the time Answer	1 1 1 1 1 1 0	1.000		3.00
Control Verification Misuse/Abuse Testing	2 Do you regularly evaluate the threats to your architecture? You speamatically review each threat identified in the Threat Assessment Trained or experienced people lead review exercise You led unhanded threats as defects You assess your architectures in a standardized, documented marrier You are requirantly update your reference architectures based on architecture assessment findings? You assess your architectures in a standardized, documented marrier You be receiving findings to trigger a review or freference architectures You independently review the quality of the architecture assessments on an ad-hoc basis You use reference architecture updates to trigger reviews or freference architectures You independently review the quality of the architecture assessments on an ad-hoc basis You use reference architecture updates to trigger reviews or freferent abards adultion, in a risk-based manner Requirements Testing 1 Do you test applications for the correct functioning of standard security controls? Security lesting a faset verifies the implementation of authentication, access control, input validation, encoding and escaping data, and escurity lesting as faset verifies the implementation of authentication, access control, input validation, encoding and escaping data, and escurity lesting as faset verifies the implementation of authentication, access control, input validation, encoding and escaping data, and escurity lesting as faset verifies the implementation of authentication access control, input validation, encoding and escaping data, and escurity lesting as a standardized efficiency expensions? 1 Do you consistently write and executs test scripts to verify the functionality of security requirements? 1 Do you automatically test applications assert expected security functionality 2 Do you automatically test applications processed to verification assert expected escaping assert expected escaping asser	B B B B B B B B B B B B B B B B B B B	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them Yes, for most or all of the applications Yes, for most or all of the applications Yes, most or all of the time Yes, most or all of the time Answer	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1.000		3.00
Control Verification Misuse/Abuse Testing	2 Do you regularly vealuate the threats to your architecture? You speamatically review each threat identified in the Threat Assessment Trained or experienced people lead review exercise You led unhanded threats as defects You led unhanded threats as defects You log unhanded threats as defects You assess your architectures in a standardized, documented marrier You se requirally update your reference architectures based on architecture assessment findings? You assess you architectures in a standardized, documented marrier You independently review the quality of the architecture sessessments on an ad-hoc basis You ser reference architecture updates to trigger reviews or frelevant shared solutions, in a risk-based manner Requirements Testing 1 Do you test applications for the correct functioning of standard security controls? Security leasing as least verifies the implementation of authentication, access control, input validation, encoding and escaping data, and excryption controls 2 Do you consistently write and executs test scripts to verify the functionality of security requirements? You believe the six of the scripts to verify the functionality of security requirements? You consistently write and executs test scripts to verify the functionality of security requirements? You consistently write and executs test scripts to verify the functionality of security requirements? You consistently write and executs test scripts to verify the functionality of security requirements? You consistently write and executs test scripts to verify the functionality of security requirements? You consistently write and executs test scripts to verify the functionality of security requirements? You consistently write test for all identified tops gone and provided the scripts of the control of the scripts of the scri	B B B B B B B	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them Yes, for most or all of the applications Yes, for most or all of the applications Yes, most or all of the time Yes, most or all of the time Answer	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1.000		3.00
Control Verification Misuse/Abuse Testing	2 Do your regularly vealuate the threats to your architecture? You systematically review each threat identified in the Threat Assessment Trained or experienced people lead review exercise You length mightaging design-level features for each identified threat You log unhanded threats as defects You log unhanded threats as defects You assess your architectures in a standardized, documented manner You are courting fundings four reference architectures based on architecture assessment findings? You assess your architectures in a standardized, documented manner You see recurring fundings to trigger a review of reference architectures You assess your architectures in a standardized, documented manner You see recurring fundings to trigger a review of relevant shared solutions, in a risk-based manner You se reference architectures updates to trigger reviews of relevant shared solutions, in a risk-based manner Review of the standard shared security controls? Security itseling at least vurifies the implementation of authentication, access controls or security in the standard security controls? Security itseling as cleast vurifies the implementation of authentication, access controls, sput validation, encoding and escaping data, and encyption controls. Security itseling executes whenever the application changes its use of the controls Security itseling executes whenever the application and senset respected security functionality of security requirements? You consistently write safe condition. The security is security of the controls. 3 Do you automatically test applications and sesset respected security functionality. You copiect security tests is a set stude that is part of the exciting unit testing framework. 1 Do you automatically test applications for security regressions? You collect security tests in a test stude that is part of the exciting unit testing framework. 2 Do you create abuse cases from functional requirements and use them to drive security tests? Important business functionally has corresponding abuse	B B B B B B B	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them Yes, for most or all of the applications Yes, for most or all of the applications Yes, most or all of the time Yes, most or all of the time Answer Yes, most or all of them	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1.000		3.00
Control Verification Misuse/Abuse Testing	2 Do you regularly vealuate the threats to your architecture? You systematically review each threat identified in the Threat Assessment Trained or experienced people lead review exercise You led with mightaing design-level features for each identified threat You log urhanded threats as defects 3 Do you gregularly update your reference architectures based on architecture assessment findings? You assess your architectures in a standardized, documented manner You see recurring findings to rigger a review of reference architectures You independently review the quality of the architecture assessments on an ad-noc basis You use relevance architecture updates to togger reviews or reference architectures You independently review the quality of the architecture assessments on an ad-noc basis You use relevance architecture updates to togger reviews or relevant abused solutions, in a risk-based manner 8 Requirements Testing 1 Do you test applications for the correct functioning of standards security controls? Security leasing a state werenever the application of hanges its use of the controls Security leasing assessment wherever the application changes its use of the controls 2 Do you consistently write and execute test scripts to verify the functionality of security requirements? You consistently write and execute test scripts to verify the functionality of security requirements? You consistently write and execute test scripts to verify the functionality Testis use a standardized fermework or OSL. 3 Do you automatically test applications and assert special security functionality You copius reserves as a pass or fail condition Tests use a standardized fermework or OSL. 4 Do you test applications using randomization or fuzzing techniques? You consistently write less for all conditions You collect security tests in a test suite that is part of the existing unit testing framework 1 Do you sear applications using randomization or fuzzing techniques? 1 Do you test applications using randomization or fuzzing techniqu	A A A A B B B B B B B B B B B B B B B B	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them Yes, for most or all of the applications Yes, for most or all of the applications Yes, for most or all of the applications Yes, most or all of the time Yes, most or all of the time Yes, most or all of them Yes, most or all of them Yes, most or all of them	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1.000		3.00
Control Verification Misuse/Abuse Testing Scalable Baseline	2 Do you regularly vealuate the threats to your architecture?	A A A A B B B B B B B B B B B B B B B B	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them Yes, for most or all of the applications Yes, for most or all of the applications Yes, most or all of the time Yes, most or all of the time Answer Yes, most or all of them	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1.000		3.00
Control Verification Misuse/Abuse Testing Scalable Baseline	2 Do you regularly vealuate the threats to your architecture? You systematically review each threat identified in the Threat Assessment Trained or experienced people lead review exercise You long urhanded threats as defects You long urhanded threats as defects You long urhanded threats as defects You assess your architectures in a standardized, documented manner You see requirant yudate your reference architectures based on architecture assessment findings? You assess your architectures in a standardized, documented manner You see receiving fundings to trigger a review or freerence architectures You independently review the quality of the architecture assessments on an ad-hoc basis You use relevance architecture updates to trigger review or freerence architectures You independently review the quality of the architecture assessments on an ad-hoc basis You use relevance architecture updates to trigger review or freely and hadre societies, in a risk-based manner 1 Do you test applications for the correct functioning of standards security controls? Security sating a lasst verifies the implementation of authentication, access control, input validation, encoding and escaping data, and Security sating ask lass verifies the implementation of authentication, access control, input validation, encoding and escaping data, and Security setting ask lass verifies the implementation of authentication, access control, input validation, encoding and escaping data, and Security setting ask lass verifies the implementation of authentication, access control, input validation, encoding and escaping data, and Security setting ask lass verifies the implementation of authentications. You copium test in each application and assert special descript functionality of security requirements? You copium test results as a pass of fall condition. 2 Do you automatically test applications for security regressions? You copium test application with a security test propriate ask lass that the propriate and test ask lass that is part of the existi	A A A A B B B B B B B B B B B B B B B B	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them Yes, for most or all of the applications Yes, for most or all of the applications Yes, for most or all of the applications Yes, most or all of the time Yes, most or all of the time Yes, most or all of them Yes, most or all of them Yes, most or all of them	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1.000		3.00
Control Verification Misuse/Abuse Testing Scalable Baseline	2 Do you regularly vealuate the threats to your architecture? You speamentably review earth residentified in the Threat Assessment Trained or experienced people lead review exercise You long urhanded threats as defects You long urhanded threats as defects You long urhanded threats as defects You assess your architectures in a standardized, documented manner You are requirantly quidate you reference architectures based on architecture assessment findings? You assess your architectures in a standardized, documented manner You see receiving fundings 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 review or frevenus that have a facility of the architecture assessments on an ad-hoc basis You use reference architecture updates to trigger review or frevenus that have a facility or the company of the architecture assessments on an ad-hoc basis You use reference architecture updates to trigger review or frevenus that have a facility or the company of the architecture assessments on an ad-hoc basis You be reference architecture updates to trigger are trigger or deview or frevenus that and security controls? Security setting assessment wherever the application of abaset representations, access control, input validation, encoding and escaping data, and Security setting assessment wherever the application changes its use of the controls 2 Do you consistently write set of an expectation and assett speciated security functionality of security requirements? You conjust retart results as a pass or fall condition 3 Do you automatically test applications and assett speciated security functionality. 1 Do you set application with a set of all condition 1 Do you set application with a set of a identified bug gossably exceeding a pre-defined severity threshold) 1 Do you set application with a set set such that is part of the existing unit testing framework 2 Do you contained the provision o	A A A A B B B B B B B B B B B B B B B B	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them Yes, for most or all of the applications Yes, for most or all of the applications Yes, for most or all of the applications Yes, most or all of the time Yes, most or all of the time Yes, most or all of them Yes, most or all of them Yes, most or all of them	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1.000		3.00
Control Verification Misuse/Abuse Testing Scalable Baseline	2 Do your controllers with the threats to your architecture? You systematically review each threat identified in the Threat Assessment Trained or experienced people lead review exercise You long unhanded threats as defects You long unhanded threats as defects 3 Do you gregalanty update your reference architectures based on architecture assessment findings? You assess your architectures in a standardized, documented manner You see recurring fundings to rigger a review of reference architectures You see recurring fundings to rigger a review of reference architectures You see recurring fundings to rigger a review of reference architectures You see recurring fundings to rigger a review of reference architectures You see receives a reference understood to rigger a review of reference architectures You see reference architectures updates to rigger are view of reference architectures You see reference architectures updates to rigger are view of reference architectures You to reference architectures updates to rigger are view of reference architectures. **Recurrier of the reference architectures updates to rigger are view of reference architectures updates or rigger are view of reference architectures updates to rigger are view of reference architectures updates or rigger are view of reference architectures. **Security setting a least verifies the implementation of architecture accurring controlor? **Security setting are called verifies the implementation of architecture accurring reference architectures. **Security setting architecture where the application and asset repected security functionality of security requirements? **You consistently write and accordance architecture for the receiver of the results are a pass or fall condition. **Tests use a standardized arrhivenous or advantage architecture architecture. **To you accordance architecture architecture. **To you consistently write architecture and security regressions? **You collect security tests in a test state that is part of the existing understanc	B B B B B B A A A A A A	Yes, for most or all of the applications Answer Yes, most or all of them Yes, most or all of them Yes, for most or all of the applications Yes, for most or all of the applications Yes, most or all of the time Yes, most or all of the time	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1.000		3.00