Herein the Herein Herei	Domain	Section	Stream	Questions
Committee   Comm	Governance	Education and Guidance	•	Do you require employees involved with application development to take SDLC training?
Part				Do your team know who to speak to if they need security guidance from outside the product team?
Hand the second processes and responsibilities clearly defined within the development fleam?  Threat Assessment  Software Requirements  Process  Software Dependencies  Software Process  Software Process  Becurity Architecture  Software Process  Becurity Architecture  Software Dependencies  Software Process  Software Dependencies  Software Process  Becurity Architecture  Software Dependencies  Software Process  Software Dependencies  Software Process  Becurity Architecture  Software Dependencies  Software Dependencies  Software Dependencies  Software Dependencies  Software Process  Becurity Architecture  Software Dependencies  Do you use repeatable deployment processes?  Do you use repeatable deployment processes and unmaded and employing security checks?  Do you use repeatable deployment processes and unmade and employing security checks?  Do you use repeatable deployment processes and unmade and employing security checks?  Do you use repeatable deployment processes and unmade and employing security checks?  Do you use repeatable deployment processes and unmade and employing security checks?  Do you use repeatable deployment processes and unmade and employing security checks?  Do you use repeatable deployment processes and unmade and employing security checks?  Do you use force SLAs for fixing security defects in accessible locations?  Do you use basis metrics about recorded security defects to carry out quick win improvement devolvities?  Do you use basis metrics about recorded security defects to carry out quick win improvement devolvities?  Do you use patient management for application architecture for key security defects to carry out quick win improvement devolvities?  Do you use patient management for accessible locations?  Do you use prome demanded and providence and security stress testing?  Do you use patient management for accessed providence			_	Have you identified a Security Champion for each development team?
Period Assessment Requirements Properties and specify security requirements during development?    Security Architecture   Architecture   Dosign   Do teams use security principles during design?   Do you base your design on available reference architectures?   Secure Build   Process   Build Process   Do you have solid knowledge about dependencies you're relying on?   Do you up revent build of software if it's affocied by vulnorabilities in dependencies?   Do you up revent build of software if it's affocied by vulnorabilities in dependencies?   Do you up revent build of software if it's affocied by vulnorabilities in dependencies?   Do you up revent build of software if it's affocied by vulnorabilities in dependencies?   Do you up revent build of software if it's affocied by vulnorabilities in dependencies?   Do you up revent build of software if it's affocied by vulnorabilities in dependencies?   Do you up revent build of software if it's affocied by vulnorabilities in dependencies?   Do you up revent build of software if it's affocied by vulnorabilities in dependencies?   Do you up revent build process automated and employing security checks?   Do you up revent build process automated and employing security checks?   Do you up revent build process automated and employing security defects   Dosignaries activities?   Do you up revent build process automated security defects by according to process?   Do you up revent build process fully and process   Dosignaries activities?   Dosignaries activi				Are roles and responsibilties clearly defined within the development team?
Purplementation  Processor  Proce	Design	Threat Assessment	Threat Modelling	Do you identify and manage architectural design flaws with threat modeling?
Security Architecture   Decision   Decisio				Do project teams specify security requirements during development?
Design   Doyou use shared security errices during design?   Do you base your design on available reference architectures?   Is your full build process formally described?   Is the build process formally described proper formally?   Is the build and deploy process?   Is the build process for the correct functioning of standard security testing tools?   Is the build		Security Architecture		Do teams use security principles during design?
Secure Build   Secure Build   Secure Build   Secure Secure   Secure Security Secure Security Securit				Do you use shared security services during design?
Secure Build   Secu				Do you base your design on available reference architectures?
Part   Process	Implementation	Secure Build	Build Process	Is your full build process formally described?
Pacification   Paci				Is the build process fully automated?
Secure Build   Software   Dependencies   Do you have solid knowledge about dependencies you're retying on?   Do you prevent build of software if it's affected by vulnerabilities in dependencies?   Do you use repeatable deployment processes?   Are deployment processes?   Are deployment processes?   Are deployment processes automated and employing security checks?   Do you inject production secrets into configuration files during deployment?   Defect Management   Defect Tracking   Defect Tracking   Do you track all known security defects in accessible locations?   Do you enforce SLAs for fixing security defects?   Do you enforce SLAs for fixing security defects to carry out quick win improvement activities?   Do you review the application architecture for key security objectives on an ad-hoc basis?   Do you regularly evaluate the threats to your architecture?   Do you regularly evaluate the threats to your architecture?   Do you test applications for the correct functioning of standard security controls?   Do you gentland place in the process of the correct functioning of standard security controls?   Do you gentland place in the process of the correct functioning of standard security controls?   Do you gentland place in the process of the correct functioning of standard security controls?   Do you gentland place in the process of the correct functioning of standard security controls?   Do you gentland place in the process of the correct functioning of standard security stress testing?   Do you gentland place in the process of the correct functioning of standard security stress testing?   Do you gentland place in the process of the correct functioning of standard security stress testing?   Do you manually review the security stress testing?   Do you manually review the security stress testing?   Do you manually review the security quality of selected high-risk components?   Do you perform penetration testing for your applications are integrated with the organisation's SIEM solution?   Do you have hardening base				Do you enforce automated security checks in your build processes?
Secure Build   Dependencies   Do you prevent build of software if it's affected by vulnerabilities in dependencies?				Is code being stored securely?
Deployment   Process   Do you prevent build of software if it's affected by vulnerabilities in dependencies?				Do you have solid knowledge about dependencies you're relying on?
Process   Are deployment processes automated and employing security checks?				Do you prevent build of software if it's affected by vulnerabilities in dependencies?
Process   Are deployment processes automated and employing security checks?			Deployment	Do you use repeatable deployment processes?
Defect Management  Defect Management  Defect Tracking  Defect Tracking  Defect Management  Metrics & Feedback  Architecture Assessment  Architecture Assessment  Partition Testing  Description Testing  Security Testing  Incident Management  Operations  Descriptions  Defect Management  Defect Management  Defect Tracking  Do you use basic metrics about recorded security defects to carry out quick win improvement activities?  Do you review the application architecture for key security objectives on an ad-hoc basis?  Do you regularly evaluate the threats to your architecture?  Do you test applications for the correct functioning of standard security controls?  Misuse/Abuse Testing  Do you test applications using randomization or fuzzing techniques?  Do you perform denial of service and security testing tools?  Do you integrate automated security testing into the build and deploy process?  Do you amanually review the security quality of selected high-risk components?  Do you perform penetration testing for your applications are integrated with the organisation's SIEM solution?  Do you harden configurations for key components of your technology stacks?  Do you have hardening baselines for your components?				Are deployment processes automated and employing security checks?
Do you track all known security defects in accessible locations?  Do you use fix a fixing security defects in accessible locations?  Do you use fix a fixing security defects in accessible locations?  Do you use fix a fixing security defects in accessible locations?  Do you use basic metrics about recorded security defects to carry out quick win improvement activities?  Do you use basic metrics about recorded security defects to carry out quick win improvement activities?  Do you use basic metrics about recorded security defects to carry out quick win improvement activities?  Do you regularly evaluate the threats to your architecture?  Do you test applications for the correct functioning of standard security controls?  Do you perform denial of service and security stress testing?  Do you use an applications with automated security testing into the build and deploy process?  Do you untegrate automated security testing into the build and deploy process?  Do you perform penetration testing for your applications are integrated with the organisation's SIEM solution?  Do you harden configurations for key components of your technology stacks?  Do you have hardening baselines for your components?  Do you identify and patch vulnerable components?			Secrets	Do you inject production secrets into configuration files during deployment?
Defect Management  Metrics & Feedback  Metrics & Feedback  Architecture Assessment  Verification  Verification  Verification  Verification  Per Understanding  Incident Management  Operations  Operations  Defect Management  Metrics & Feedback  Metrics & Feedback  Architecture Assessment  Architecture Assessment  Architecture Validation  Do you review the application architecture for key security objectives on an ad-hoc basis?  Do you regularly evaluate the threats to your architecture?  Do you test applications for the correct functioning of standard security controls?  Do you perform denial of service and security stress testing?  Do you perform denial of service and security stress testing?  Do you integrate automated security testing into the build and deploy process?  Do you manually review the security quality of selected high-risk components?  Do you perform penetration testing for your applications at regular intervals?  Do you ensure that newly deployed applications are integrated with the organisation's SIEM solution?  Do you have hardening baselines for your components?  Do you components?  Do you identify and patch vulnerable components?			Management	Do you practice proper lifecycle management for application secrets?
Defect Management    Defect Management   Defect Management		Defect Management	Defect Tracking	Do you track all known security defects in accessible locations?
Metrics & Feedback   Do you use basic metrics about recorded security defects to carry out quick win improvement activities?				Do you enforce SLAs for fixing security defects?
Architecture Assessment Validation Do you regularly evaluate the threats to your architecture?  Requirements Testing Verification  Requirements Testing  Misuse/Abuse Testing Do you test applications for the correct functioning of standard security controls?  Do you test applications using randomization or fuzzing techniques? Do you perform denial of service and security stress testing?  Do you scan applications with automated security testing tools? Do you integrate automated security testing into the build and deploy process?  Do you manually review the security quality of selected high-risk components? Do you perform penetration testing for your applications at regular intervals?  Incident Management  Incident Detection  Do you ensure that newly deployed applications are integrated with the organisation's SIEM solution?  Do you have hardening baselines for your components?  Do you identify and patch vulnerable components?				
Verification  Requirements Testing  Po you test applications for the correct functioning of standard security controls?  Do you test applications using randomization or fuzzing techniques?  Do you perform denial of service and security stress testing?  Do you perform denial of service and security testing tools?  Do you integrate automated security testing into the build and deploy process?  Do you manually review the security quality of selected high-risk components?  Do you perform penetration testing for your applications at regular intervals?  Incident Management  Do you ensure that newly deployed applications are integrated with the organisation's SIEM solution?  Do you have hardening baselines for your components?  Do you dentify and patch vulnerable components?	Verification	Architecture Assessment		Do you review the application architecture for key security objectives on an ad-hoc basis?
Verification   Requirements Testing   Do you test applications for the correct functioning of standard security controls?				Do you regularly evaluate the threats to your architecture?
Nerification   Nerification   Nerification   Nerification   Do you test applications using randomization or fuzzing techniques?		Requirements Testing		Do you test applications for the correct functioning of standard security controls?
Do you perform denial of service and security stress testing?    Scalable Baseline				Do you test applications using randomization or fuzzing techniques?
Security Testing  Do you integrate automated security testing into the build and deploy process?  Do you manually review the security quality of selected high-risk components?  Do you perform penetration testing for your applications at regular intervals?  Incident Management  Incident Management  Do you ensure that newly deployed applications are integrated with the organisation's SIEM solution?  Configuration Hardening  Do you have hardening baselines for your components?  Do you have hardening baselines for your components?  Do you identify and patch vulnerable components?				Do you perform denial of service and security stress testing?
Security Testing  Deep Understanding  Do you integrate automated security testing into the build and deploy process?  Do you manually review the security quality of selected high-risk components?  Do you perform penetration testing for your applications at regular intervals?  Do you ensure that newly deployed applications are integrated with the organisation's SIEM solution?  Configuration Hardening  Do you harden configurations for key components of your technology stacks?  Do you have hardening baselines for your components?  Patching and Updating  Do you identify and patch vulnerable components?		Security Testing		Do you scan applications with automated security testing tools?
Deep Understanding Do you manually review the security quality of selected high-risk components?  Incident Management Detection Do you ensure that newly deployed applications are integrated with the organisation's SIEM solution?  Configuration Hardening Do you harden configurations for key components of your technology stacks?  Do you have hardening baselines for your components?  Patching and Updating Do you identify and patch vulnerable components?				Do you integrate automated security testing into the build and deploy process?
Incident Management  Incident Detection  Do you ensure that newly deployed applications are integrated with the organisation's SIEM solution?  Configuration Hardening  Do you harden configurations for key components of your technology stacks?  Do you have hardening baselines for your components?  Patching and Updating  Do you identify and patch vulnerable components?			•	Do you manually review the security quality of selected high-risk components?
Operations  Detection  Do you ensure that newly deployed applications are integrated with the organisation's SIEM solution?  Configuration Hardening  Do you harden configurations for key components of your technology stacks?  Do you have hardening baselines for your components?  Patching and Updating  Do you identify and patch vulnerable components?				Do you perform penetration testing for your applications at regular intervals?
Operations  Environment Management  Do you have hardening baselines for your components?  Patching and Updating  Do you identify and patch vulnerable components?	Operations	Incident Management		Do you ensure that newly deployed applications are integrated with the organisation's SIEM solution?
Operations  Do you have hardening baselines for your components?  Patching and Updating  Do you identify and patch vulnerable components?		Environment Management	_	Do you harden configurations for key components of your technology stacks?
Updating Do you identify and patch vulnerable components?				Do you have hardening baselines for your components?
Do you operate separate Dev/Test/Production environments?			_	Do you identify and patch vulnerable components?
		Operational Management	Data Protection	Do you operate separate Dev/Test/Production environments?
Operational Management Data Protection Do you protect web facing applications and API's using a Web Application Firewall?				Do you protect web facing applications and API's using a Web Application Firewall?
Do you ensure that all devloper workstations are secured adequately?				Do you ensure that all devloper workstations are secured adequately?