



SAMM Benchmark Top 10 Lessons Learned

SAMM User Day September 25, 2024



SAMM Benchmark

Benchmark tab in Excel Toolbox and SAMMY tool



https://bit.ly/sammbenchmarksubmission

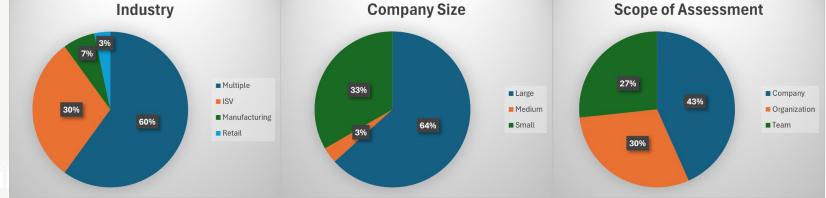




owaspsamm.org

Demographics



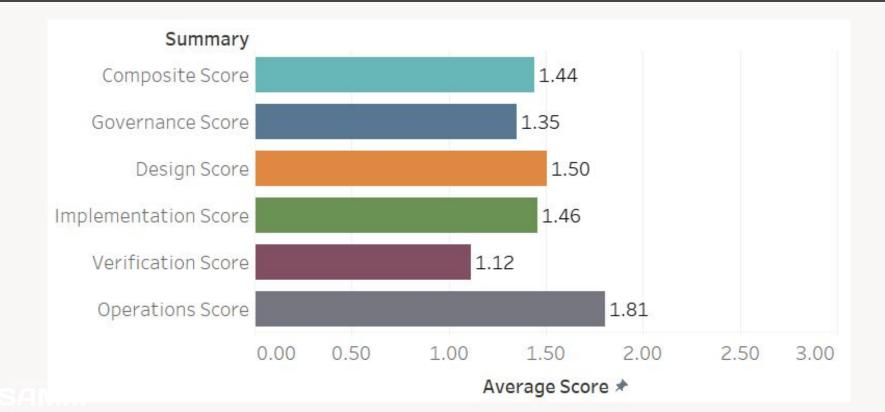


Demographics Highlights

- 30 datasets
 - Too few to provide more granular results
- Most assessments are done by a reputable third party
 - Higher quality data
- The majority of the companies are large multinationals
 Mid-sized companies are underrepresented
- Results averaging problems
 - Governance and Operations in multinationals vs small
- Assessment scope represents a nice mix



Overall Results: 30 datasets

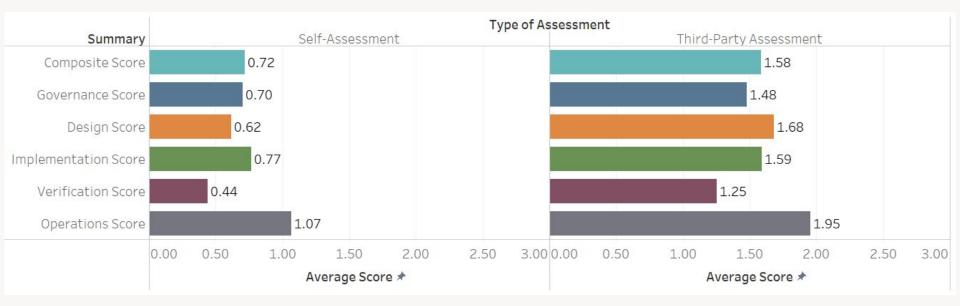


Overall Results

- Higher score on Operations
 - Expected especially for large multinationals
- Higher score for Implementation
 - The success of the Dev(Sec)Ops paradigm
- Lower Governance score is surprising
 - Arguably due averaging skewing
- Higher score on Design
 - "Shift left"
- Verification is too low



Overall results vs assessment type



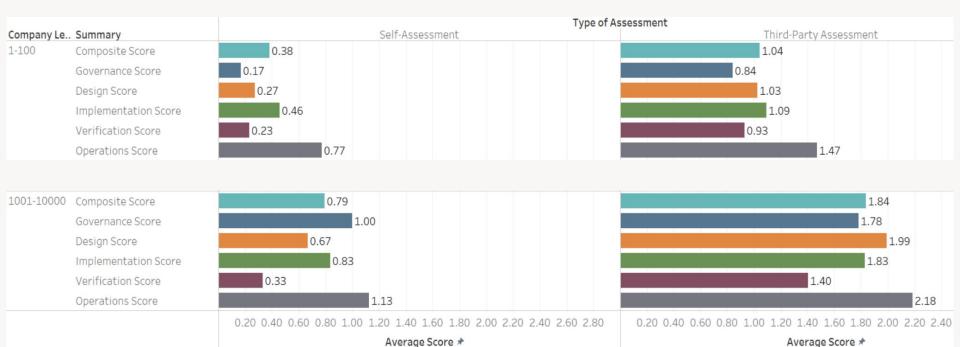
SAMM

Self vs third-party assessments

- Surprisingly low scores for self-assessments
 - Prepped third party assessments
 - Subjectivity factor in self-assessments
- Generally third-party assessments are considered to be more accurate or representative
- Third-party assessments will vary based on skill/knowledge
- Self-assessments will vary based on skill/knowledge and honesty



Overall results vs company size



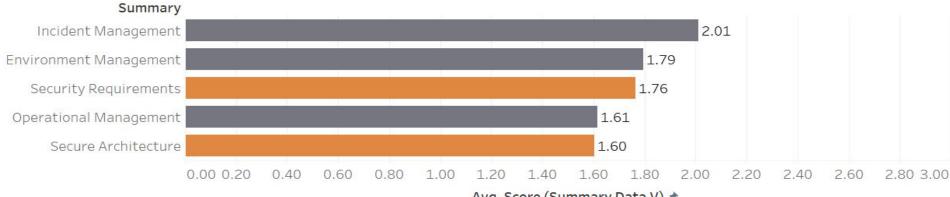
SAMN

Large vs small companies

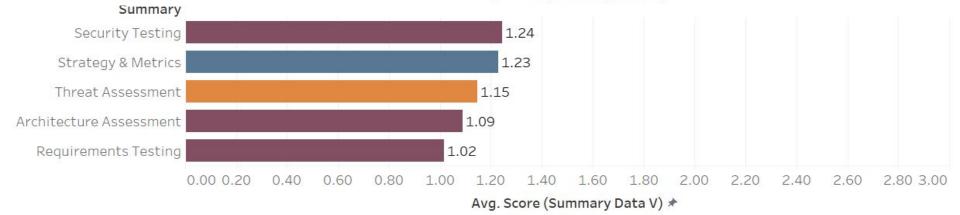
- Expected outcomes
 - Small companies score worse than large
 - Low score on governance for small companies
- Surprises
 - High score on Operations for small companies
 - Self-assessments have a much lower verification score



Top vs Bottom Scoring Activities



Avg. Score (Summary Data V) *



Top vs Bottom Scoring Activities

- Incident & Environment Management are historically handled well at large multinationals
- Deployment is thanks to Dev(Sec)Ops successes
- Security Requirements and Secure Architecture are probably thanks to the "Shift Left" paradigm



Top vs Bottom Scoring Activities

- Low scores on Requirements Testing and Architecture Assessment are surprising in combination with "Shift Left"
 - Did we do the right thing?
- Threat Assessment is historically a low scoring activity
- Low scores on Security Testing is surprising
 - Best practices for SAST/DAST usage
 - Pen testing lessons learned (L3)
- Low scores on Strategy & Metrics is perhaps surprising
 - Averaging issues
 - Metrics is a problematic topic in SAMM



Top 10 Scoring Questions

Question	Mat										
Do you respond to detected incidents?	1										0.86
Do you have a complete picture of your external compliance obligations?	1	12								0.78	
Do you protect and handle information according to protection requirem.	1									0.77	
Do you use a repeatable process for incident handling?	2									0.76	
Do stakeholders review vendor collaborations for security requirements	1									0.76	
Do you track all known security defects in accessible locations?	1	Ĩ								0.74	
Do you identify and patch vulnerable components?	1								0.	.72	
Do you evaluate the security quality of important technologies used for	1	1							0.	72	
Do you use repeatable deployment processes?	1	0							0.7	72	
Do you have and apply a common set of policies and standards througho	1								0.7	72	
		0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
						Av	g. Score	1			



Top Scoring Questions

- No surprises here
 - 9 top scoring questions are from maturity level 1
 - 1 is from maturity level 2 and related to incident handling



owaspsamm.org

Bottom 10 Scoring Questions

Question	Mat											
Do you regularly review and update the data catalog and your data prote	3				0.24							
Did you define Key Perfomance Indicators (KPI) from available applicatio	2		-		0.24							
Do you improve your security assurance program upon standardized met	2			0	.22							
Do you create abuse cases from functional requirements and use them to	2			0	.22							
Do you regularly report on adherence to external compliance obligations	3			0.2	21							
Do you automatically test applications for security regressions?	3			0.2	21							
Do you regularly update your reference architectures based on architect	3			0.16								
Do you regularly review and update the threat modeling methodology fo	3	1	0	.15								
Do you regularly evaluate the effectiveness of your security metrics so t	3		0.1	13								
Do you prevent build of software if it's affected by vulnerabilities in dep	3		0.08									
		0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
		Avg. Score 🖈										



Bottom Scoring Questions

- Most bottom scoring questions are from maturity level 3
- Surprising finding
 - We don't define KPIs, but we improve our AppSec program based on metrics and KPIs.
- Metrics and feedback is a low scorer for both levels 2 and 3
 - Setting up an effective metrics program is hard
- "Do you prevent build of software if it's affected by vulnerabilities in dependencies?"
 - Only few teams enforce "known good" dependencies



Top 5 Ranked Maturity 2 & 3 Questions

Question	Mat	Rank	
Do you use a repeatable process for incident handling?	2	4	0.76
Are vendors aligned with standard security controls and software devel.	3	11	0.71
Do you have a dedicated incident response team available?	3	14	0.70
Do vendors meet the security responsibilities and quality measures of se	2	14	0.70
Do you keep an overview of the state of security defects across the orga	2	18	0.68

- Looking at what at Maturity level 2 and 3 is being done
 - Incident Response is no surprise, as it's typically inherited from Ops
 - Vendor management is a bit of a surprise, but that may be from the current limited dataset
 - Defect management is a nice addition to this list

SAMM

Bottom 5 Ranked Maturity 1 Questions

Question	Mat	Rank	
Do you review the application architecture for mitigations of typical thre	1	48	0.46
Do you identify and manage architectural design flaws with threat modeli.	. 1	50	0.45
Do you manually review the security quality of selected high-risk compon	1	53	0.44
Do you use a set of metrics to measure the effectiveness and efficiency of .	. 1	64	0.36
Do you test applications using randomization or fuzzing techniques?	1	78	0.25

- Looking at what at Maturity level 1 is not being done
 - Randomized testing and fuzzing is largely not done
 - Basic Security Metrics are apparently a real struggle
 - Manual reviews of high-risk components
 - Lack of basic threat modeling is still present
 - Reviewing the architecture after deployment is uncommon
 - Basic metrics is just above this list at rank 46

Governance Insights

Activity	Question	0	0.25	0.5	1
	d Do you understand the enterprise-wide risk appetite for your applications ?	7%	21%	24%	48%
Promote	Do you have a strategic plan for application security and use it to make decisions?	31%	31%	3%	34%
× Me	Do you regularly review and update the Strategic Plan for Application Security?	31%	28%	10%	5170
6 Measure	Do you use a set of metrics to measure the effectiveness and efficiency of the application security pro	10%	41%	45%	3%
and Strate	Did you define Key Perfomance Indicators (KPI) from available application security metrics?	41%	21%	38%	
Timprove	Do you update the Application Security strategy and roadmap based on application security metrics a	52%	14%	3%	31%
g Policy &	Do you have and apply a common set of policies and standards throughout your organization?	14%	3%	24%	59%
B B E Standard	^S Do you publish the organization's policies as test scripts or run-books for easy interpretation by devel.	31%	31%	24%	14%
unan unan unan	Do you regularly report on policy and standard compliance, and use that information to guide complia	31%	48%	10%	10%
Complian complian complian complian complian complian complian	c Do you have a complete picture of your external compliance obligations?	7%	17%	3%	72%
	Do you have a standard set of security requirements and verification procedures addressing the organ.	28%	17%	28%	28%
o ment	Do you regularly report on adherence to external compliance obligations and use that information to g.	. 52%	28%	14%	7%
P Training	Do you require employees involved with application development to take SDLC training?	10%	17%	21%	52%
p and	Is training customized for individual roles such as developers, testers, or security champions?	17%	28%	34%	21%
Awarene	⁵⁵ Have you implemented a Learning Management System or equivalent to track employee training and c.	21%	10%	21%	48%
	ti Have you identified a Security Champion for each development team?	21%	17%	7%	55%
te on and Cu	Does the organization have a Secure Software Center of Excellence (SSCE)?	41%	17%	38%	3%
The ture	Is there a centralized portal where developers and application security professionals from difference	. 48%	24%	17%	10%
		0% 20% 40% 60% 80%	0% 20% 40% 60% 80%	0% 20% 40% 60% 80%	0% 20% 40% 60% 80%
		% of Total Count of Score			

SAMM

Design Insights

Activity	Question	0	0.25	Score	1
문 Applicati	Do you classify applications according to business risk based on a simple and predefined set of questio		24%	31%	34%
n Risk Pro	$^{ m f}$ Do you use centralized and quantified application risk profiles to evaluate business risk?	14%	31%	21%	34%
s ile	Do you regularly review and update the risk profiles for your applications?	41%	21%	10%	28%
∛ Threat	Do you identify and manage architectural design flaws with threat modeling?	14%	34%	31%	21%
Modeling	Do you use a standard methodology, aligned on your application risk levels?	52%	21%	14%	14%
두	Do you regularly review and update the threat modeling methodology for your applications?	66%	24%	3%	7%
j Software	Do project teams specify security requirements during development?	7%	21%	21%	52%
Requirem	^e Do you define, structure, and include prioritization in the artifacts of the security requirements gate.	21%	38%	17%	24%
un nts	Do you use a standard requirements framework to streamline the elicitation of security requirements	62%	14%	3%	21%
Supplier	Do stakeholders review vendor collaborations for security requirements and methodology?	10%	14%	7%	69%
Security	Do vendors meet the security responsibilities and quality measures of service level agreements define		10%	3%	66%
Sec	Are vendors aligned with standard security controls and software development tools and processes t.	17%	14%	3%	66%
Architect	u Do teams use security principles during design?	14%	38%	10%	38%
t re Design	Do you use shared security services during design?	17%	31%	17%	34%
chit	Do you base your design on available reference architectures?	31%	21%	17%	31%
	g Do you evaluate the security quality of important technologies used for development?	10%	7%	24%	59%
y Manage	Do you have a list of recommended technologies for the organization?	3%	21%	34%	41%
S ment	Do you enforce the use of recommended technologies within the organization?	28%	24%	28%	21%
		0% 20% 40% 60% 80%	0% 20% 40% 60% 80%	% 0% 20% 40% 60% 8	30% 0% 20% 40% 60% 80%
		% of Total Count of Score	% of Total Count of Score	% of Total Count of Sta	mo Woffetal South of Score

Implementation Insights

			Sc	core	
Activity	Question	0	0.25	0.5	1
Build		7%	14%	24%	55%
Process	Is the build process fully automated?	14%	21%	17%	48%
e Buil	Do you enforce automated security checks in your build processes?	31%	24%	28%	17%
Softwar	Do you have solid knowledge about dependencies you're relying on?	7%	17%	34%	41%
on e Deper	Do you handle 3rd party dependency risk by a formal process?	21%	31%	34%	14%
dencies	Do you prevent build of software if it's affected by vulnerabilities in dependencies?	79%	17%		3%
는 拦 Deployr		3%	17%	24%	55%
Deployr ent Prod ess	Are deployment processes automated and employing security checks?	28%	31%	24%	17%
	Do you consistently validate the integrity of deployed artifacts?	38%	28%	17%	17%
Secret	Do you limit access to application secrets according to the least privilege principle? Do you inject production secrets into configuration files during deployment? Do you practice proper lifecycle management for application secrets?		31%	14%	55%
Manage	Do you inject production secrets into configuration files during deployment?	7%	24%	34%	34%
- o ment	Do you practice proper lifecycle management for application secrets?	28%	14%	21%	38%
t Defect	Do you track all known security defects in accessible locations?	10%		31%	59%
E Trackin	Do you keep an overview of the state of security defects across the organization?	10%	17%	17%	55%
nag	Do you enforce SLAs for fixing security defects?	2104	17%	31%	31%
≥ Metrics	Do you use basic metrics about recorded security defects to carry out quick win improvement activities	24%	31%	7%	38%
to and Fee	Do you improve your security assurance program upon standardized metrics?	52%	28%	10%	10%
dback	Do you regularly evaluate the effectiveness of your security metrics so that its input helps drive your	66%	24%	7%	3%
		20% 40% 60% 80%	20% 40% 60% 80%	20% 40% 60% 80%	20% 40% 60% 80%
		% of Total Count of Score	% of Total Count of Score	% of Total Count of Sco: e	to of Total Count of Scare

Verification Insights

	A attivity	Question	0		ore 0.5	1
:		Question © Do you review the application architecture for key security objectives on an ad-hoc basis?	7%	0.25	21%	38%
Ses		¹ Do you regularly review the security mechanisms of your architecture?	10%	41%	34%	1406
AS	dation	Do you regularly review the effectiveness of the security controls?	2006	28%	24%	10%
cure	Archito	 Do you review the application architecture for mitigations of typical threats on an ad-hoc basis? 	14%	38%	24%	24%
tect					24%	14%
chit.	igation	Do you regularly evaluate the threats to your architecture?	34%	34%	17%	1110
A.		Do you regularly update your reference architectures based on architecture assessment findings?	66%	17%	10%	7%
IVe.	Control	2	7%	21%	34%	38%
LD-0	ion	$^{ m t}$ Do you consistently write and execute test scripts to verify the functionality of security requirements	24%	28%	31%	17%
-SUID	IUIT	Do you automatically test applications for security regressions?	45%	34%	17%	3%
	Misuse/	Do you test applications using randomization or fuzzing techniques?	48%	24%	17%	10%
5	Abuse	Do you create abuse cases from functional requirements and use them to drive security tests?	38%	48%	7%	7%
Inhay	Testing	Do you perform denial of service and security stress testing?	31%	31%	21%	17%
_	Scalable	e Do you scan applications with automated security testing tools?	7%	28%	21%	45%
5	Baselin	^e Do you customize the automated security tools to your applications and technology stacks?	41%	38%	10%	10%
D		Do you integrate automated security testing into the build and deploy process?	28%	38%	17%	17%
1ch	Deep Ur	Do you manually review the security quality of selected high-risk components?	10%	45%	24%	21%
	derstan ding	Do you perform penetration testing for your applications at regular intervals?	21%	24%	21%	34%
0	ding	Do you use the results of security testing to improve the development lifecycle?	31%	48%	7%	14%
			0% 20% 40% 60% 80%	0% 20% 40% 60% 80%	0% 20% 40% 60% 80	% 0% 20% 40% 60%
			% of Total Count of Score	% of Total Count of Score	% of Total Count of Scure	Got Total Count of Sci

Operations Insights

				S	core	
	Activity	Question	0	0.25	0.5	1
	Incident	Do you analyze log data for security incidents periodically?	14%	31%	17%	38%
	Detection	Do you follow a documented process for incident detection?	14%	10%	28%	48%
	ana	Do you review and update the incident detection process regularly?	28%	10%	28%	34%
(1)	≥ Incident	Do you respond to detected incidents?	3%	14%		83%
ctice	Response	Do you use a repeatable process for incident handling?	10%	7%	17%	66%
Prac	Inc	Do you have a dedicated incident response team available?	14%	10%	17%	59%
	configuration	Do you harden configurations for key components of your technology stacks?	7%	3%	41%	48%
Security	Hardening	Do you have hardening baselines for your components?	17%	21%	31%	31%
/ Se	nt N	Do you monitor and enforce conformity with hardening baselines?	34%	7%	28%	31%
Dera	Patching and	Do you identify and patch vulnerable components?	3%	21%	17%	59%
Opera	D Updating	Do you follow an established process for updating components of your technology stacks?	3%	28%	28%	41%
s Fu	Env	Do you regularly evaluate components and review patch level status?	21%	17%	17%	45%
nes	Data Protection	Do you protect and handle information according to protection requirements for data stored and proc.	3%	10%	24%	62%
Busi	впе	Do you maintain a data catalog, including types, sensitivity levels, and processing and storage lo atio	31%	28%	31%	10%
	ž –	Do you regularly review and update the data catalog and your data protection policies and procedures	48%	34%	3%	14%
	System	Do you identify and remove systems, applications, application dependencies, or services that are no lo		28%	17%	55%
	becomissioning/	Do you follow an established process for removing all associated resources, as part of decommissioni	17%	7%	34%	41%
	e Legacy Manage	Do you regularly evaluate the lifecycle state and support status of every software asset and underlyin	17%	17%	14%	52%
			0% 50% 1	00% 0% 50% 100%	6 0% 50% 1009	6 0% 50% 100%
			04 of Tatal Count of Co	01 - 67 - 1 - 1 C 1 - 6 C	0/ of Tatal Country 4	

% of Total Count of Score % of Total Count of Score % of Total Count of Score % of Total Count of Score





Thank you! owaspsamm.org