usenix LISA14

Developers and Application Security: Who is Responsible?

SURVEY RESULTS, November 2014

Mark Miller, Senior Storyteller

Mark Miller

Trusted Software Alliance

Thoughts, Ideas and Trends in Application Security

OWASP 24/7

The WebGoat Project with Rick Lawson and Jason White

8 days

#owasp

TheNexus

A Community Project

- Central Status
- oss.Sonatype.org Status
- Security Advisory Archives

Survey Sponsors

TSWA

cigital

DEVOPS WEEKLY
A weekly slice of devops news

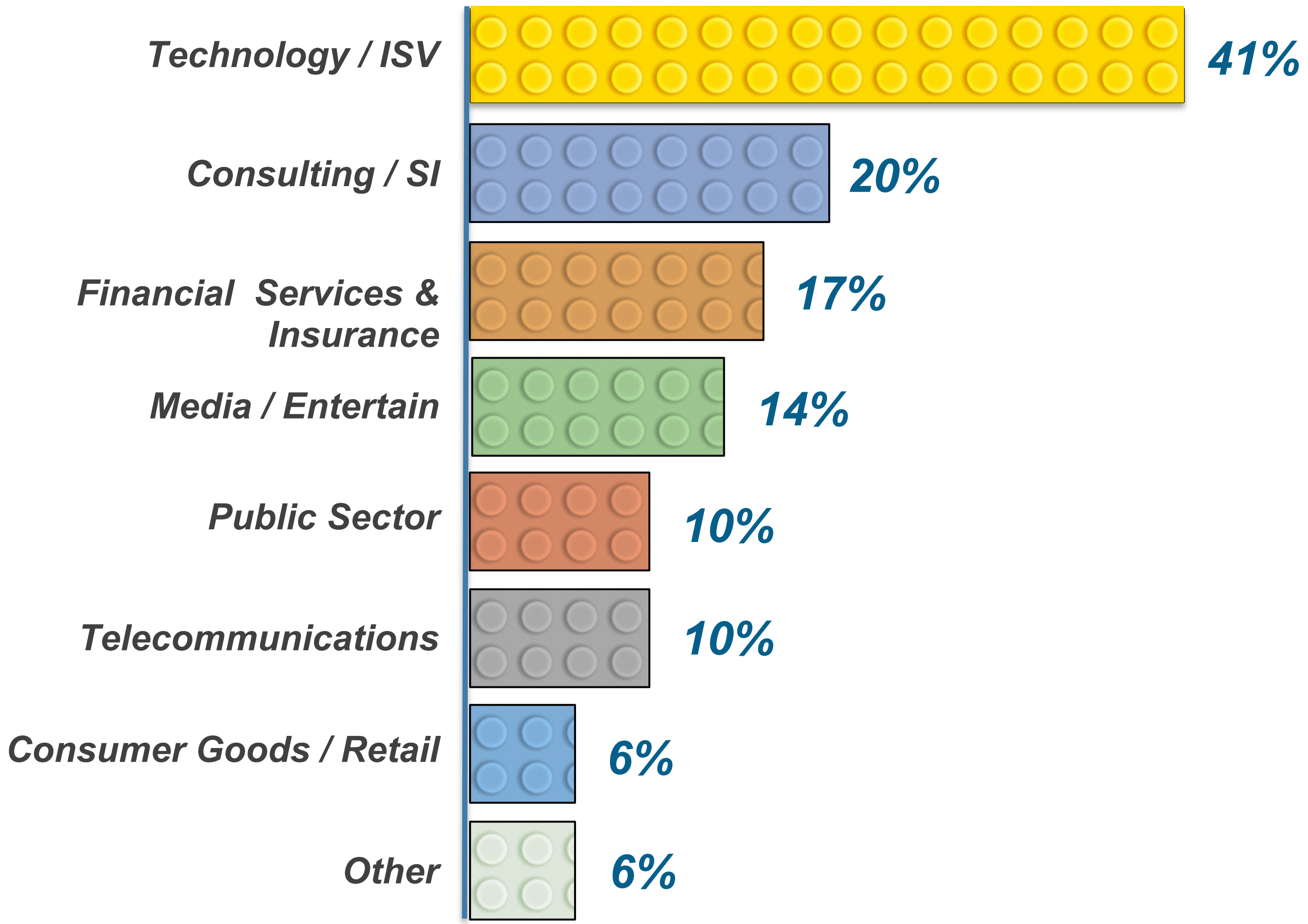
DevOps Days

hp

Sonatype

DevOps Cafe

Q5 - In what industry does your business operate?



Q1 – What is your role within your current organization?

DevOps

30%

Development

26%

Operations

25%

Security

16%

Other

3%

Q3 – What is your responsibility level?

Practitioner

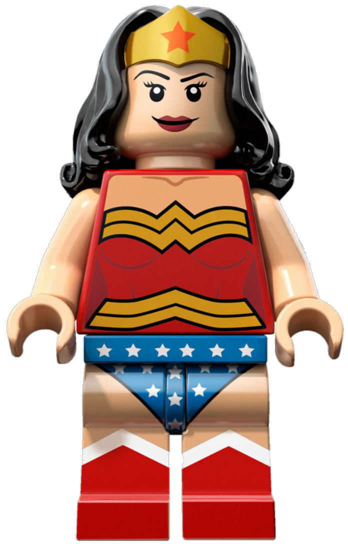
46%

Manager

40%

Senior Management

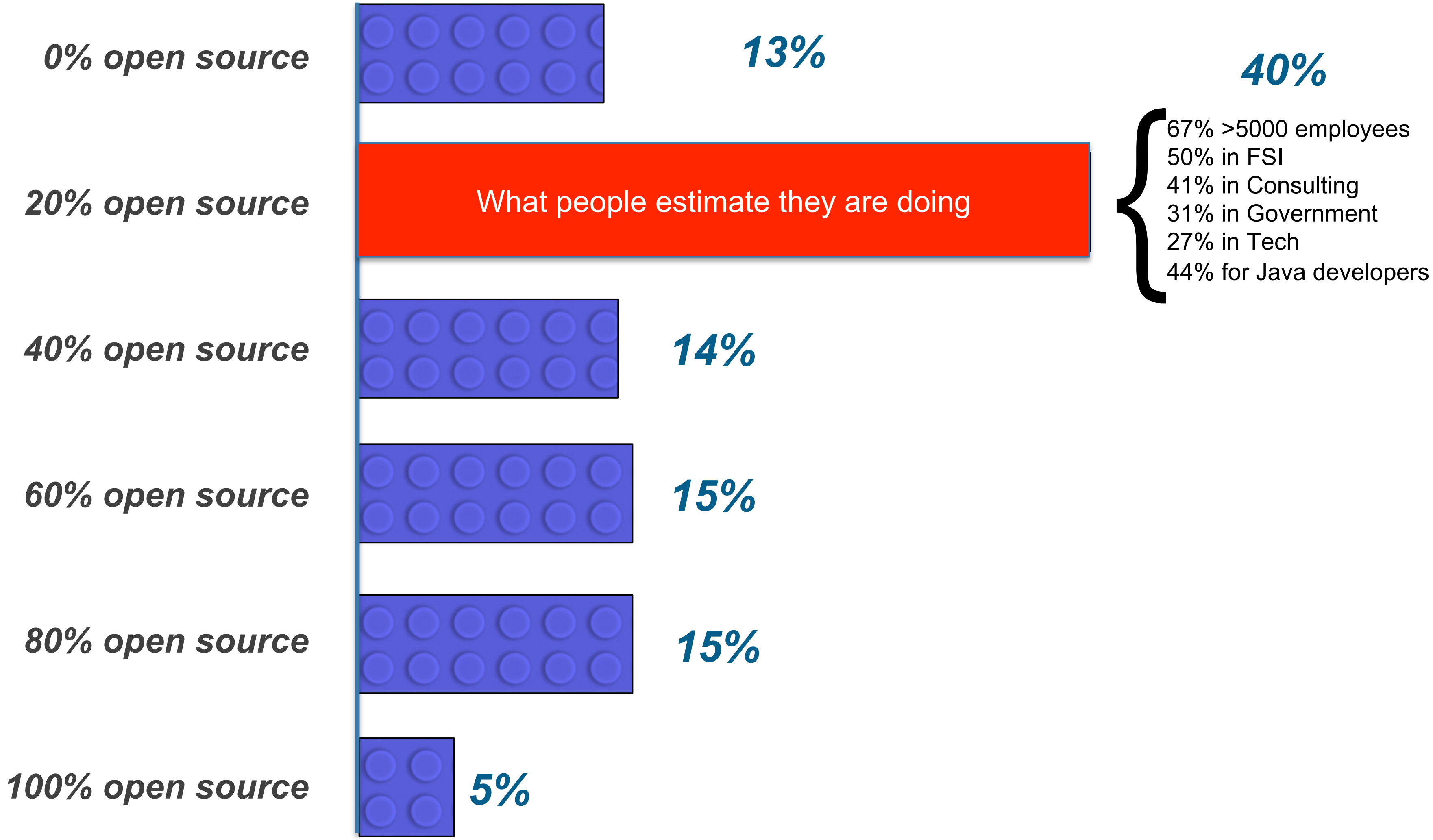
8%



Executive Management

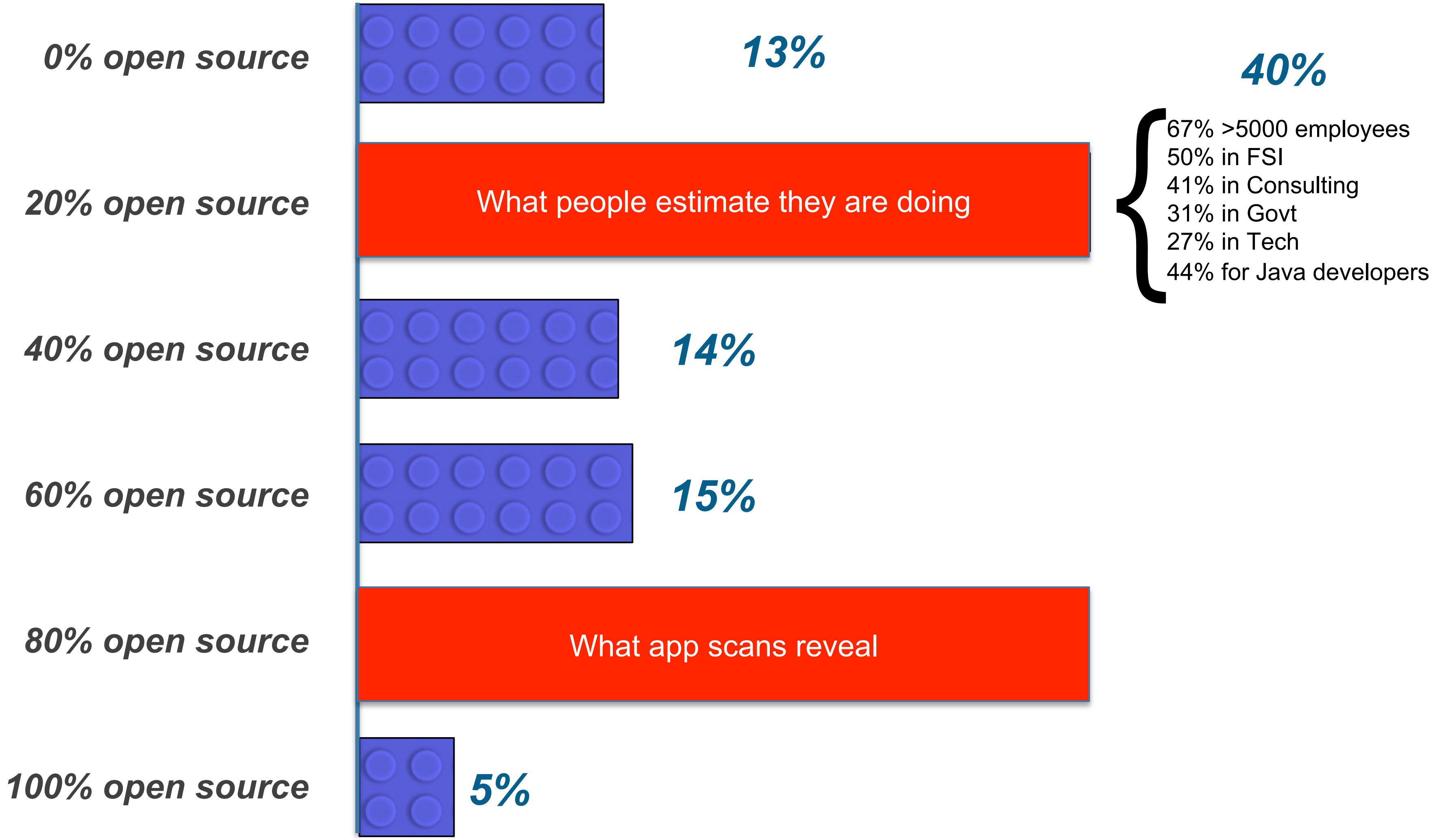
6%

Q9 - Percentage of open source software?



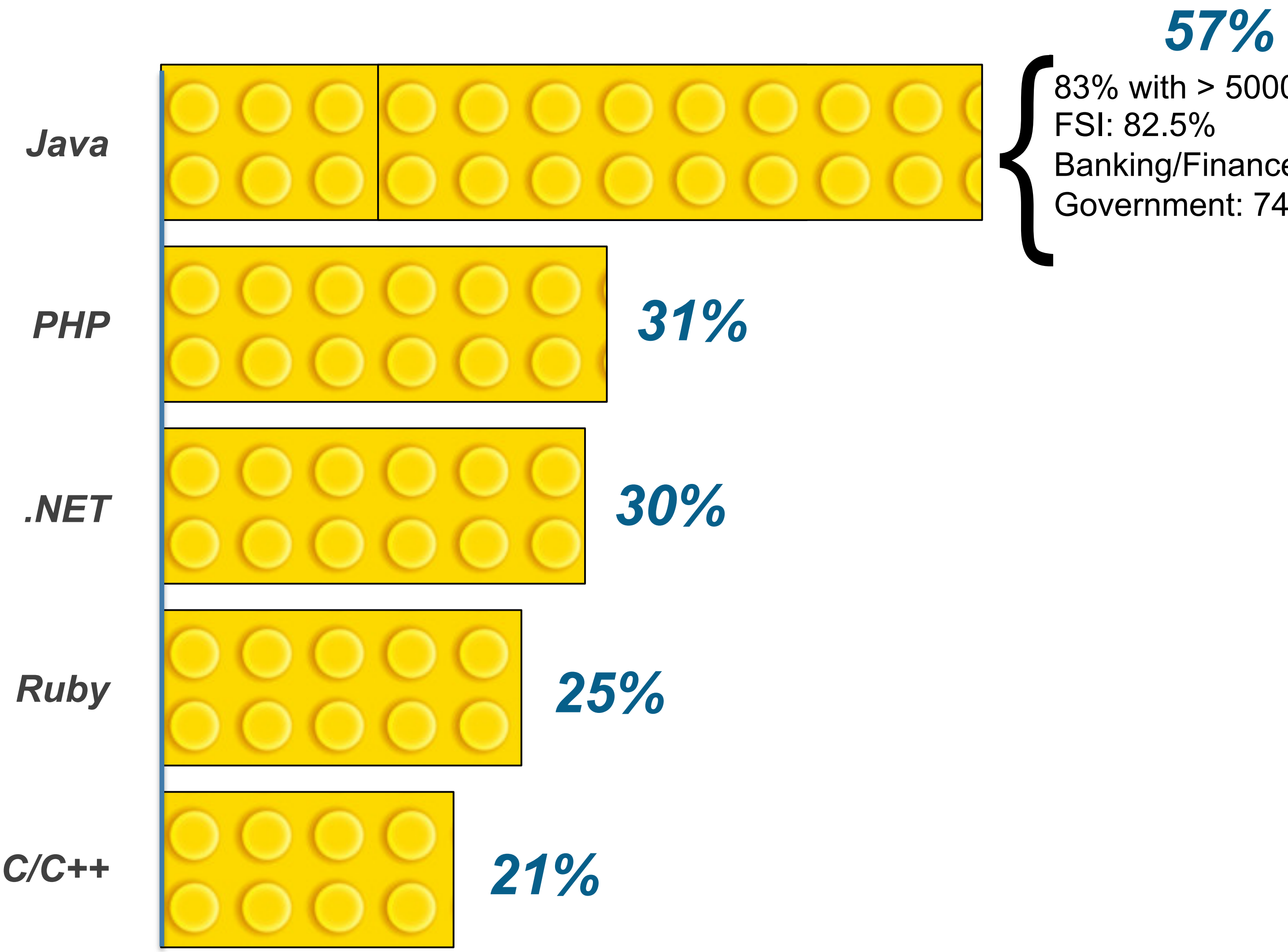
67% >5000 employees
50% in FSI
41% in Consulting
31% in Government
27% in Tech
44% for Java developers

Q9 - Percentage of open source software?



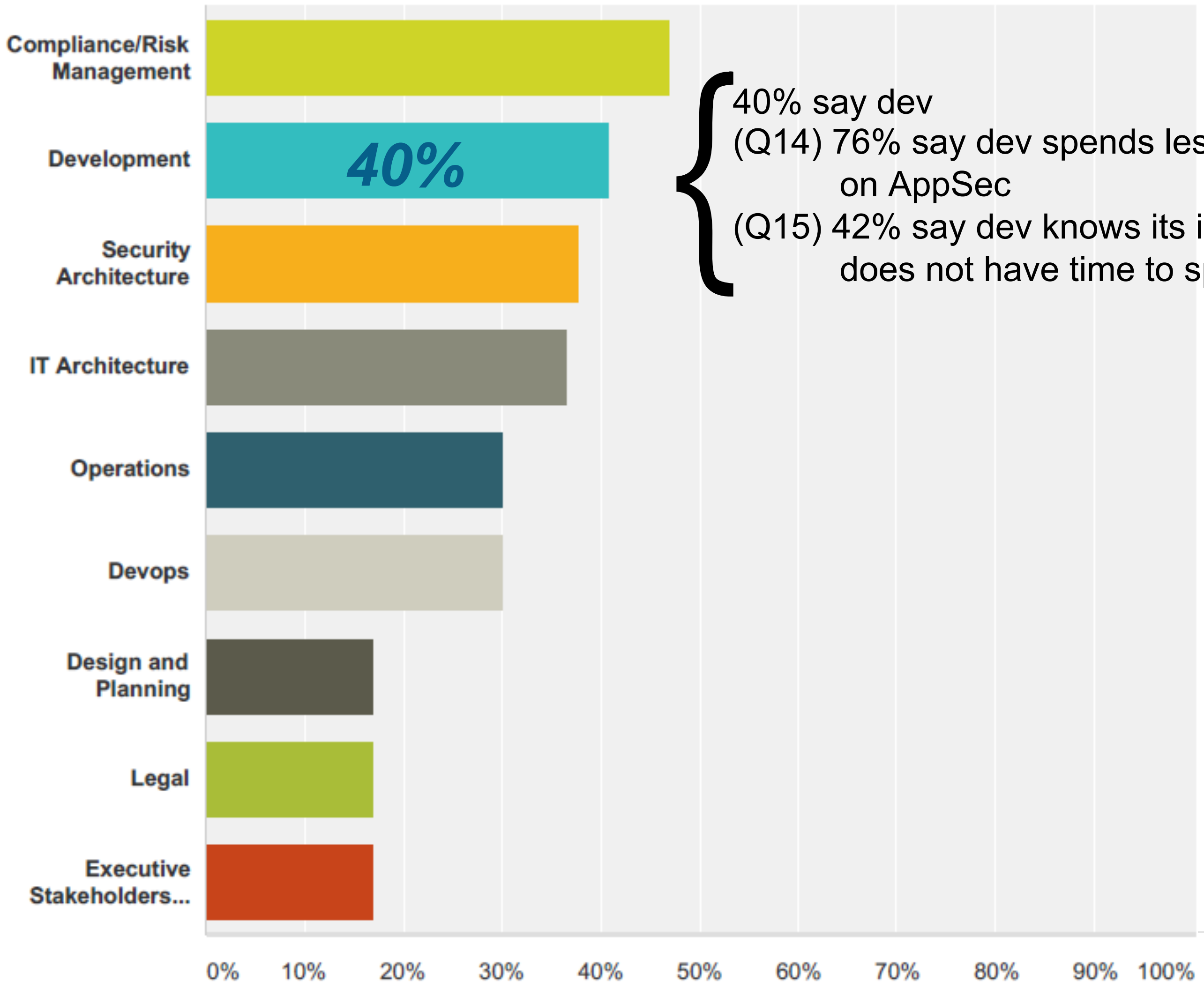
67% >5000 employees
50% in FSI
41% in Consulting
31% in Govt
27% in Tech
44% for Java developers

Q10 - For custom development, what languages are used?



83% with > 5000 employees
FSI: 82.5%
Banking/Finance: 88%
Government: 74%

Q11 - Who is the primary driver behind AppSec initiatives?

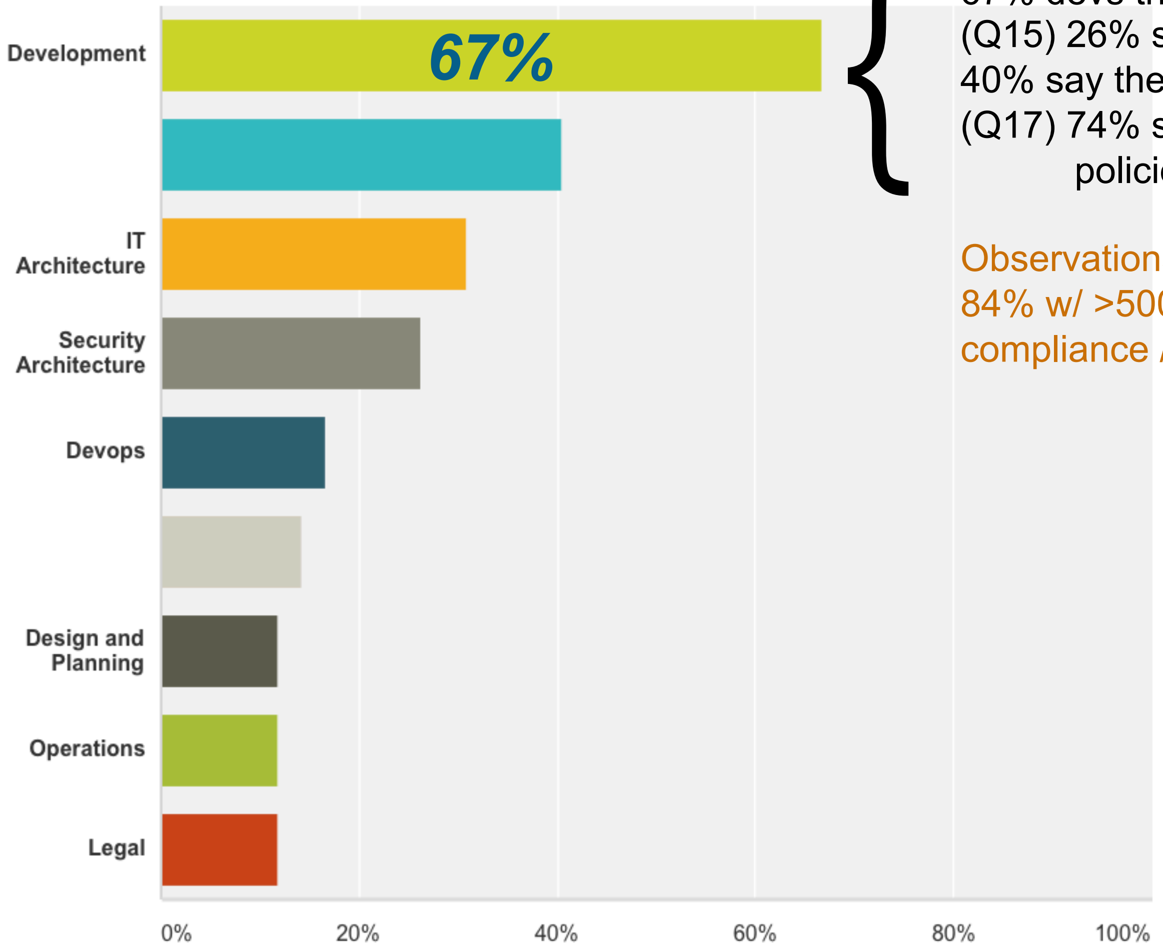


40% say dev

(Q14) 76% say dev spends less than 15% time on AppSec

(Q15) 42% say dev knows its important but does not have time to spend on it

Q11 - Who primarily drives AppSec initiatives? (filtered for developers only)



67% devs think they are the primary driver; (Q15) 26% say security is not their focus, 40% say they have no time to spend on it; (Q17) 74% state we have no policies or policies are not effectively enforced

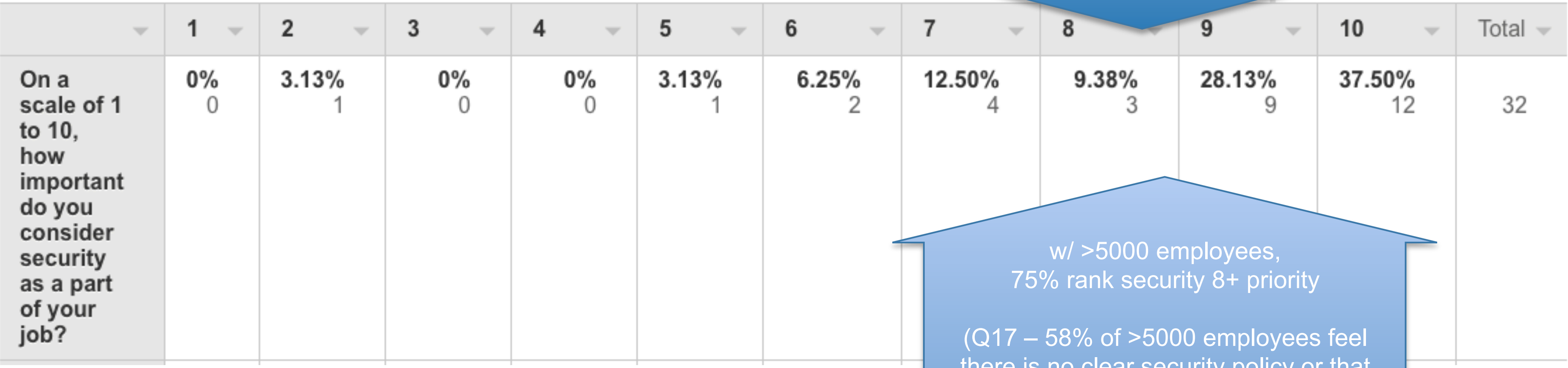
Observations:
84% w/ >5000 employees think it's compliance / risk management

Q12 – Your role in AppSec? (1=not at all, 10 = highest priority)

w/ 101 – 1000 employees,
76% rank security 8+ priority

Q17 – 67% employees feel there is no clear security policy or that policy is not effectively enforced.

Q13 - 74% state adherence to internal security policies is a top concern



	1	2	3	4	5	6	7	8	9	10	Total
On a scale of 1 to 10, how important do you consider security as a part of your job?	0% 0	3.13% 1	0% 0	0% 0	3.13% 1	6.25% 2	12.50% 4	9.38% 3	28.13% 9	37.50% 12	32

w/ >5000 employees,
75% rank security 8+ priority

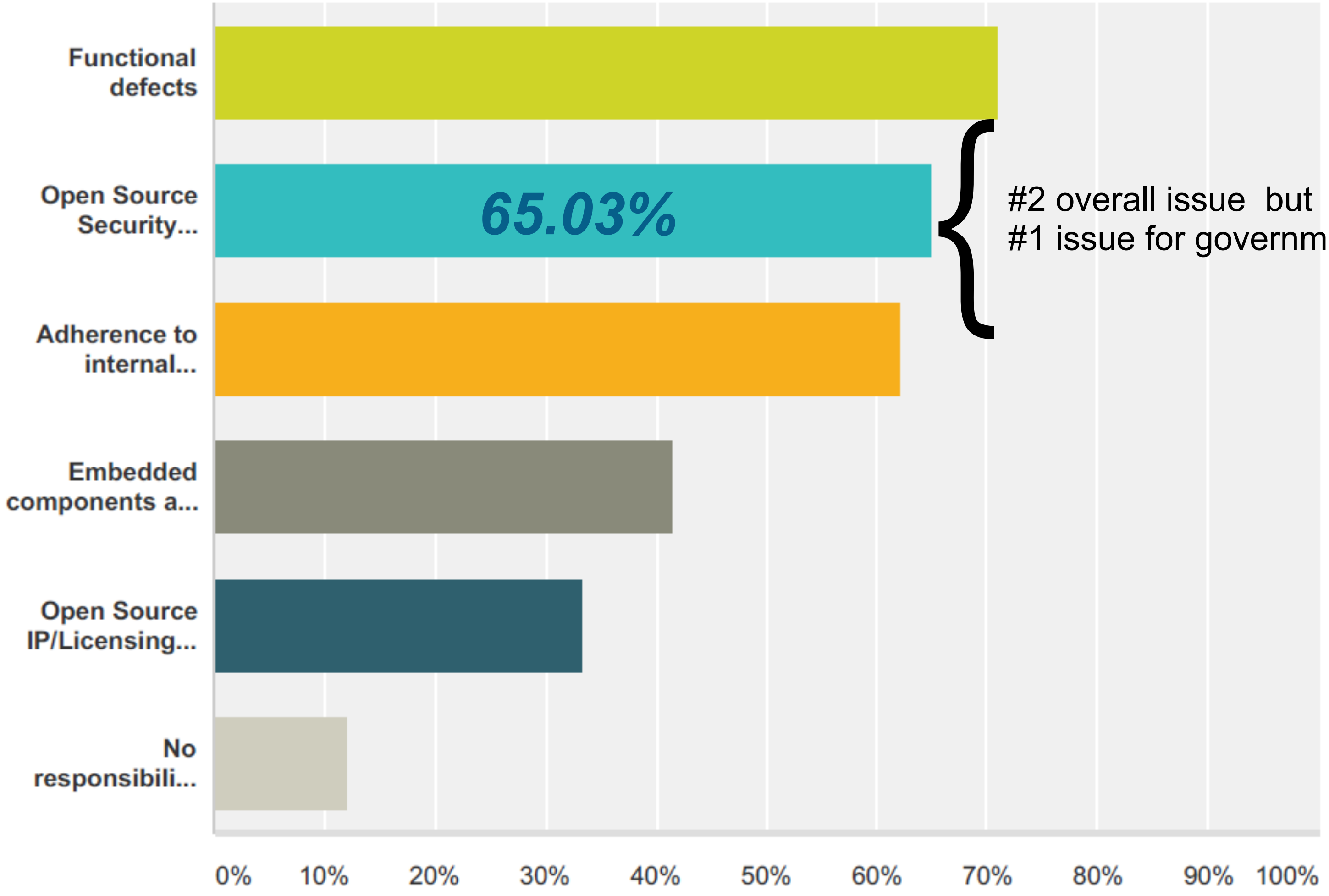
(Q17 – 58% of >5000 employees feel there is no clear security policy or that policy is not effectively enforced; 18% we don't have clear policies

81% state Adherence to internal security policies is a top concern

Conclusion: strong personal sense of responsibility, but little to not policies to enforce security standards; people make up their own standards

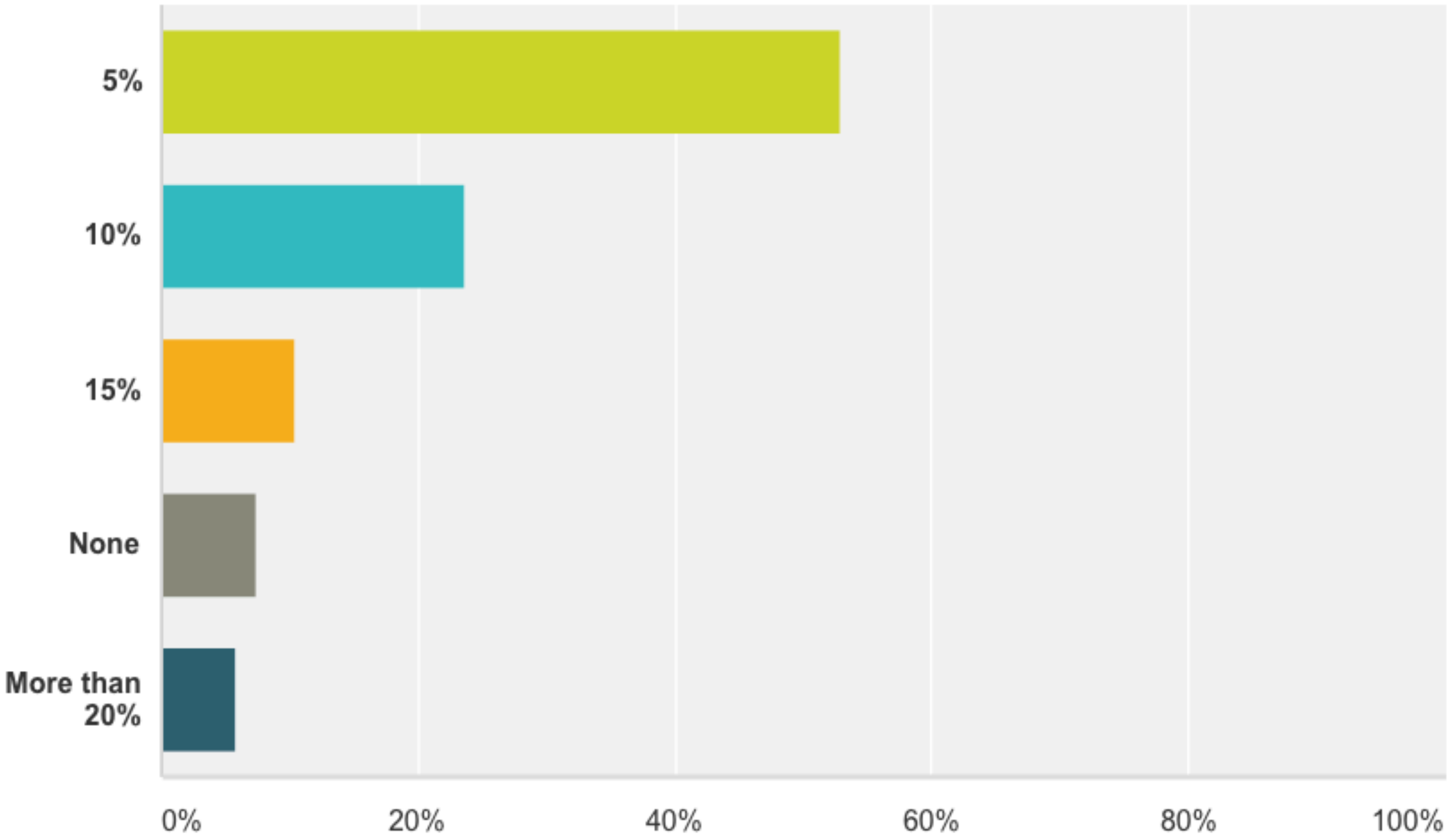
Conclusion:
"App Sec is important to me but we lack corporate policies so I'll determine my own."

Q13 - Are any of these security concerns?

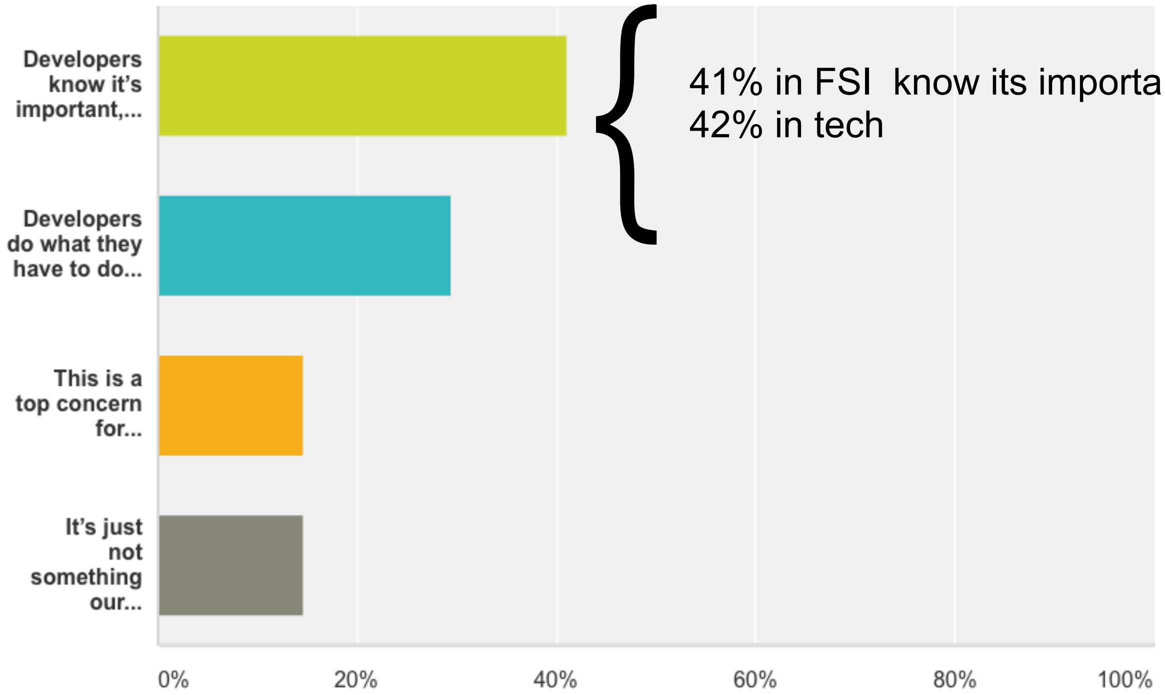


#2 overall issue but only 31% test it
#1 issue for government

Q14 - How much time to developers spend on security?

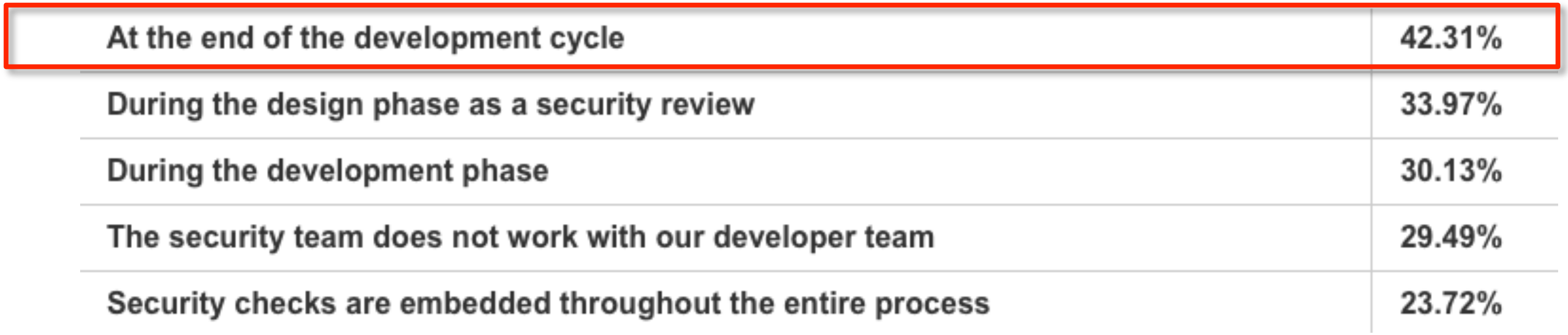


Q15 - Interest of in-house developers in regard to AppSec



41% in FSI know its important but don't spend time
42% in tech

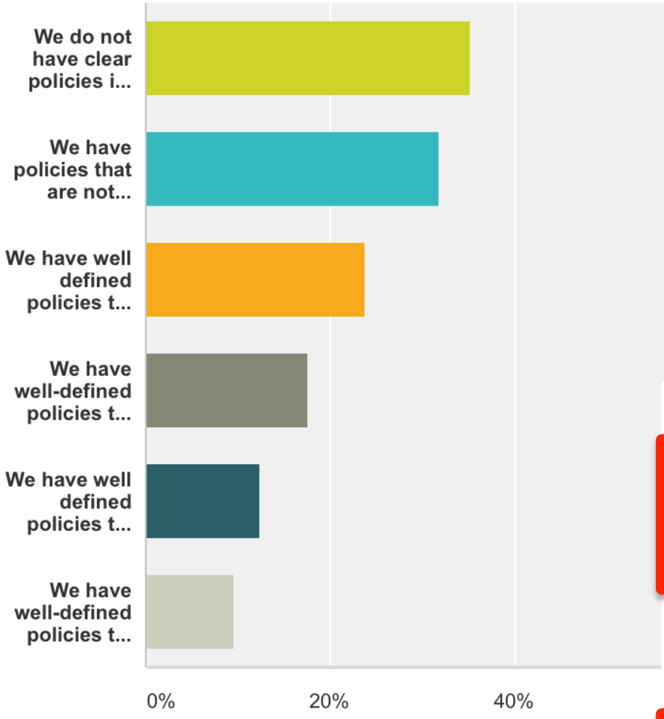
Q16 - When does App Dev spend time with security group?



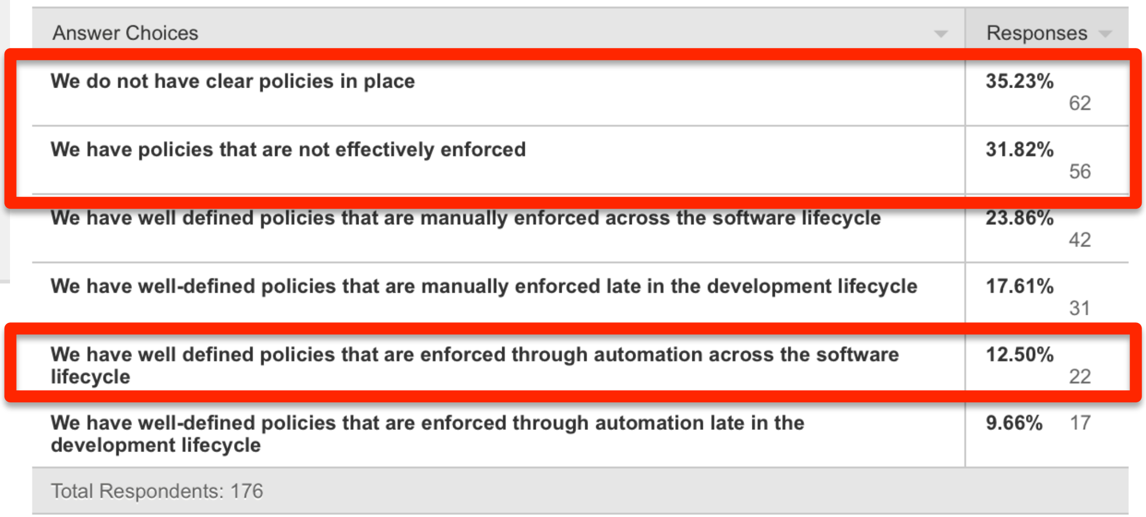
At the end of the development cycle	42.31%
During the design phase as a security review	33.97%
During the development phase	30.13%
The security team does not work with our developer team	29.49%
Security checks are embedded throughout the entire process	23.72%

Observations:
23% say security checks happen, but (Q17) Only 12% have automated
End of development cycle - 62% in government (#1 answer), 47% in financial services
Historically, ‘end of development cycle’ is the most expensive option

Q17 - Describe your current app security policies (Overall)

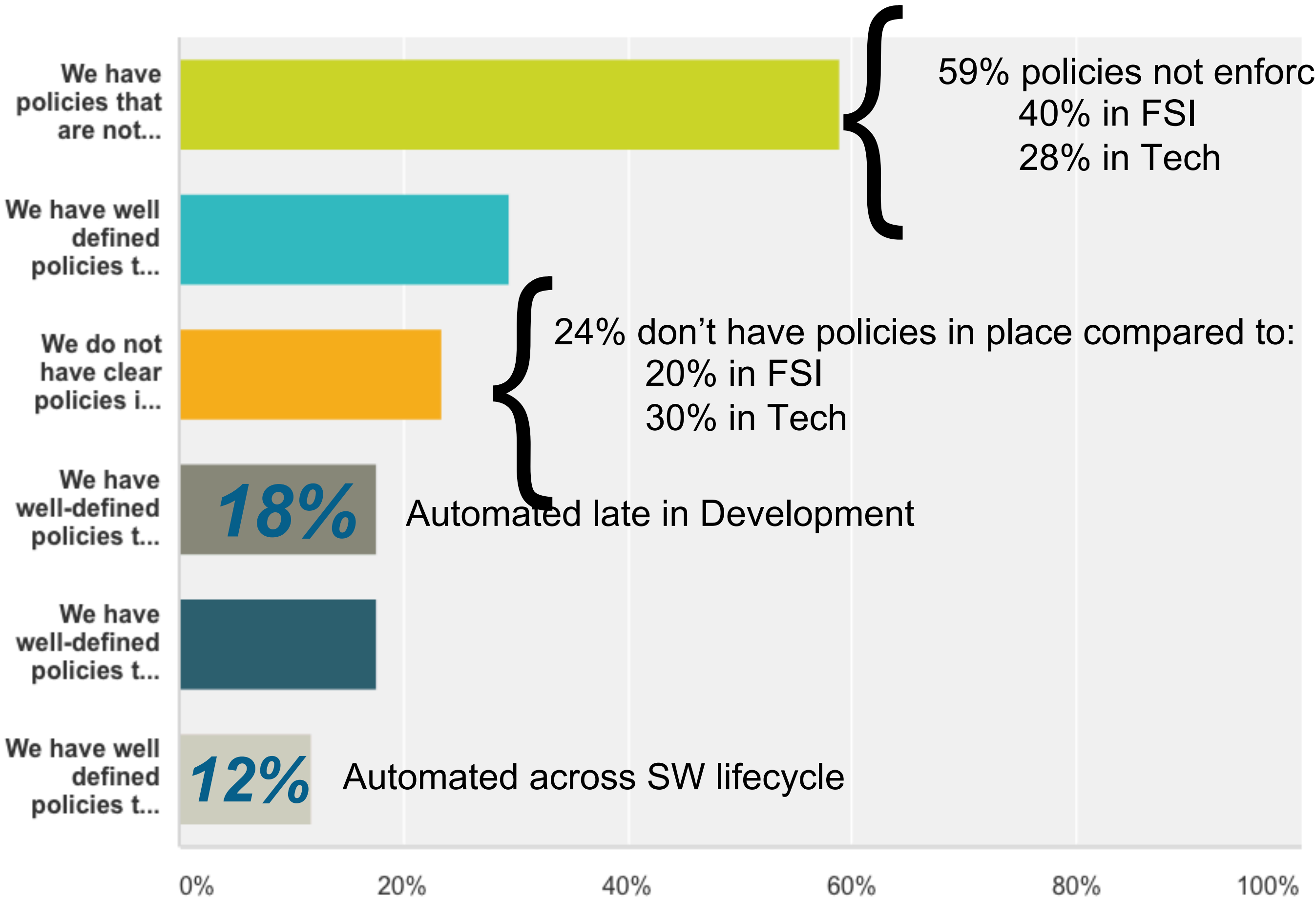


Observations:
67.05% do not have clear, well defined, enforced policies
12.5% have well defined, automated policies



Answer Choices	Responses	
We do not have clear policies in place	35.23%	62
We have policies that are not effectively enforced	31.82%	56
We have well defined policies that are manually enforced across the software lifecycle	23.86%	42
We have well-defined policies that are manually enforced late in the development lifecycle	17.61%	31
We have well defined policies that are enforced through automation across the software lifecycle	12.50%	22
We have well-defined policies that are enforced through automation late in the development lifecycle	9.66%	17
Total Respondents: 176		

Q17 - Describe your current app security policies (filtered for government)



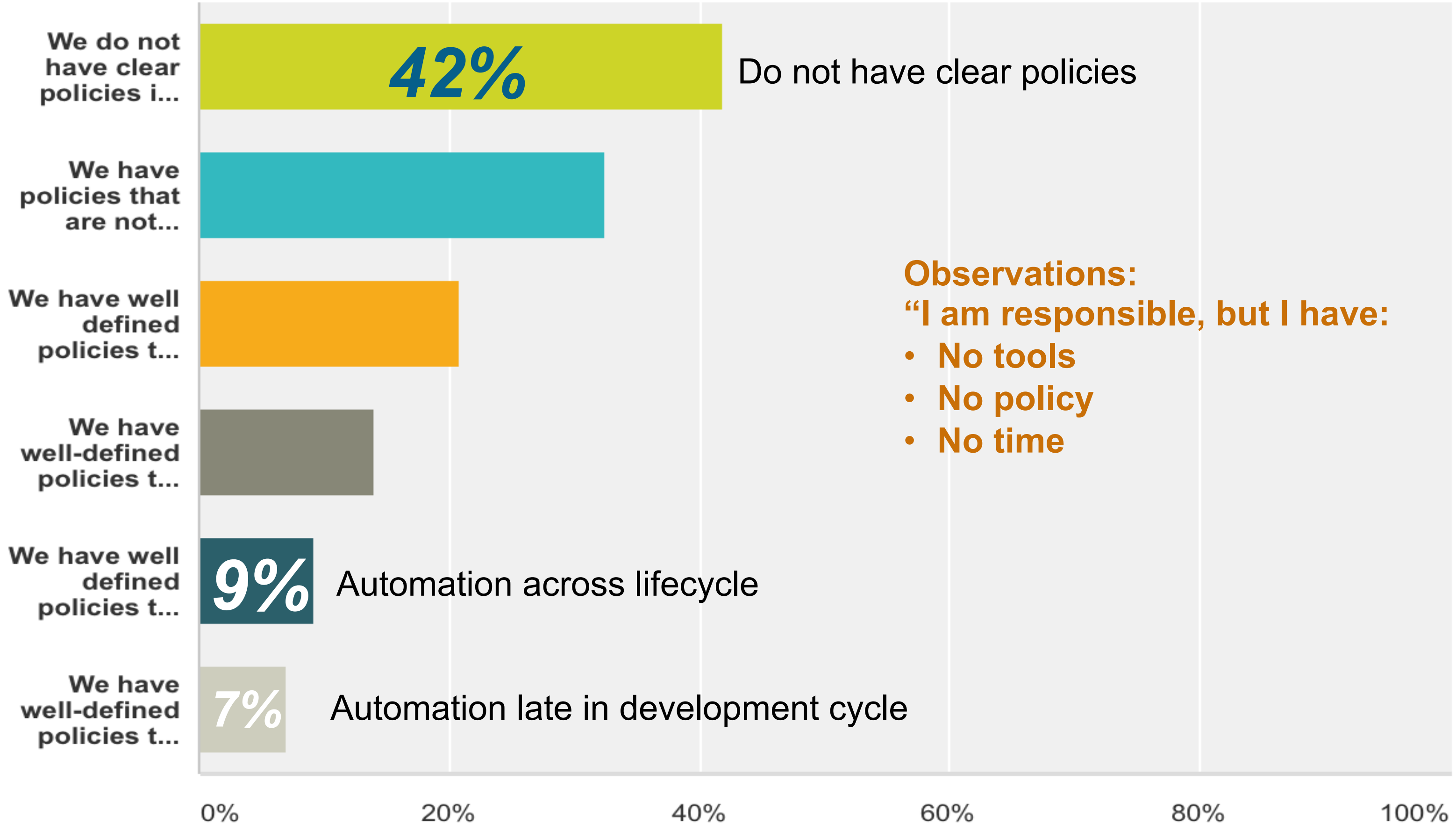
59% policies not enforced compared to:
40% in FSI
28% in Tech

24% don’t have policies in place compared to:
20% in FSI
30% in Tech

Automated late in Development

Automated across SW lifecycle

Q17 - Describe your current app security policies (Developers only)



Do not have clear policies

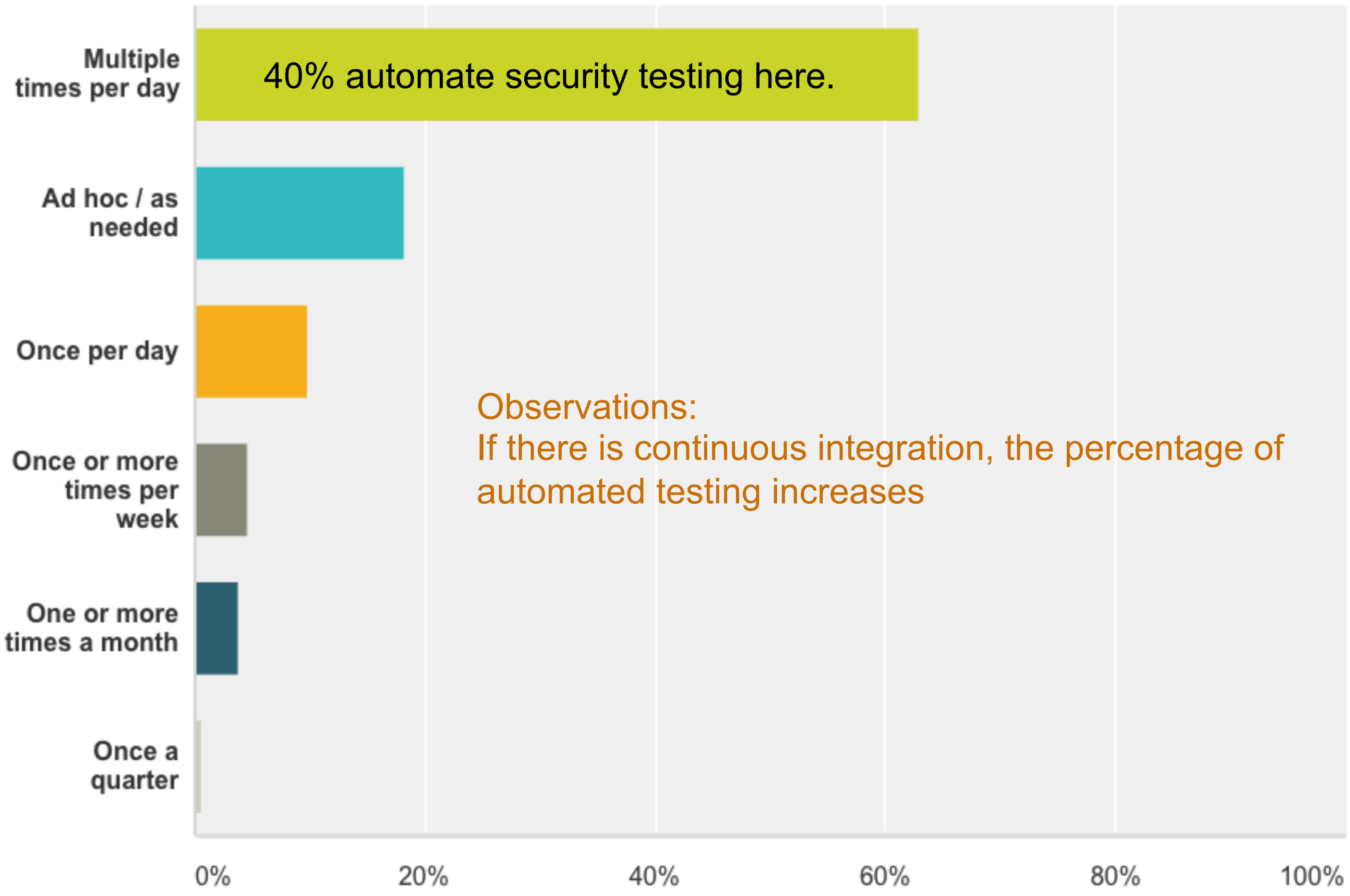
Automation across lifecycle

Automation late in development cycle

Observations:
"I am responsible, but I have:

- **No tools**
- **No policy**
- **No time**

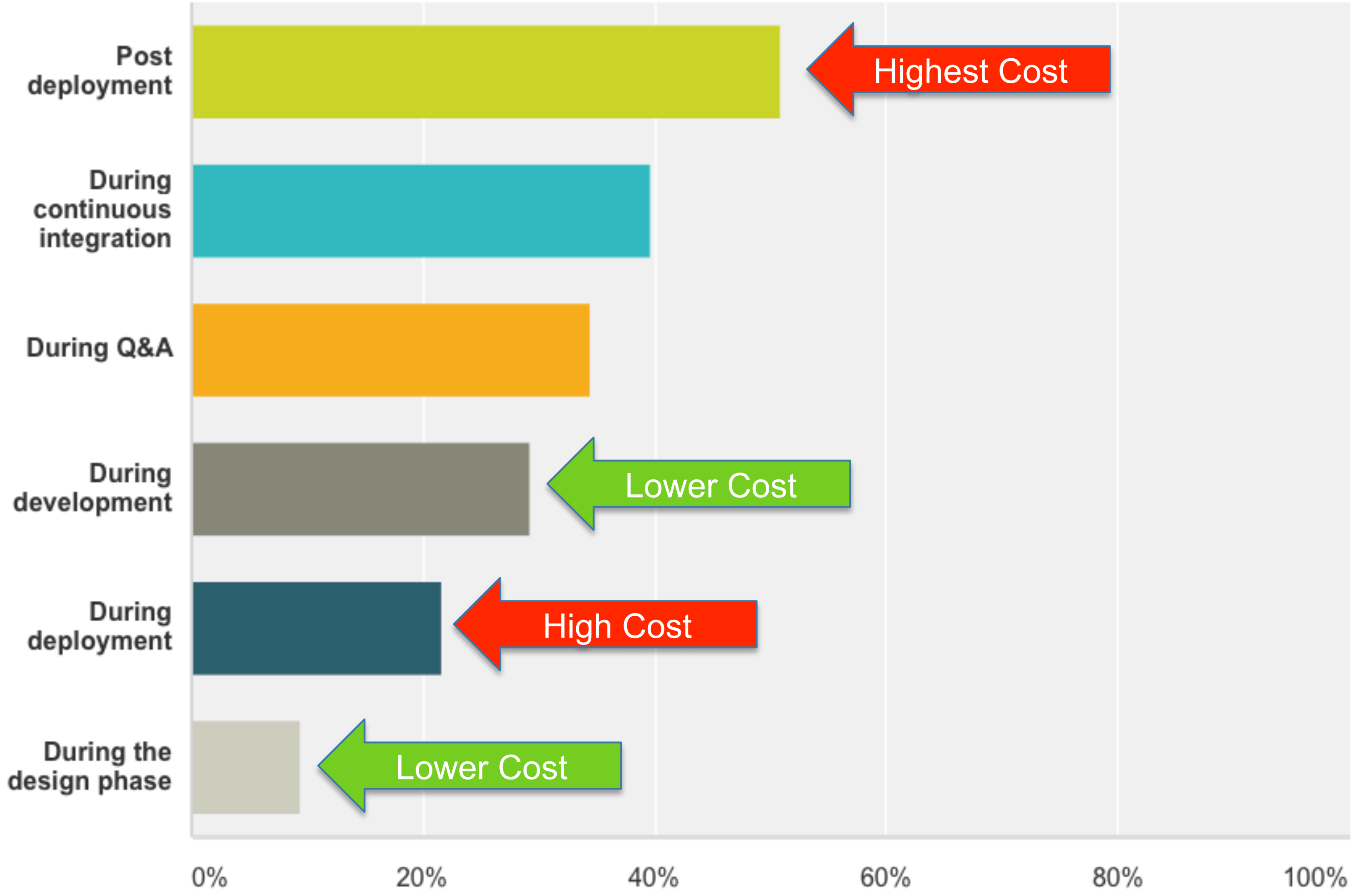
Q20 - If doing CI, how often is code compiled?



40% automate security testing here.

Observations:
If there is continuous integration, the percentage of automated testing increases

Q23 - Where is security testing automated?



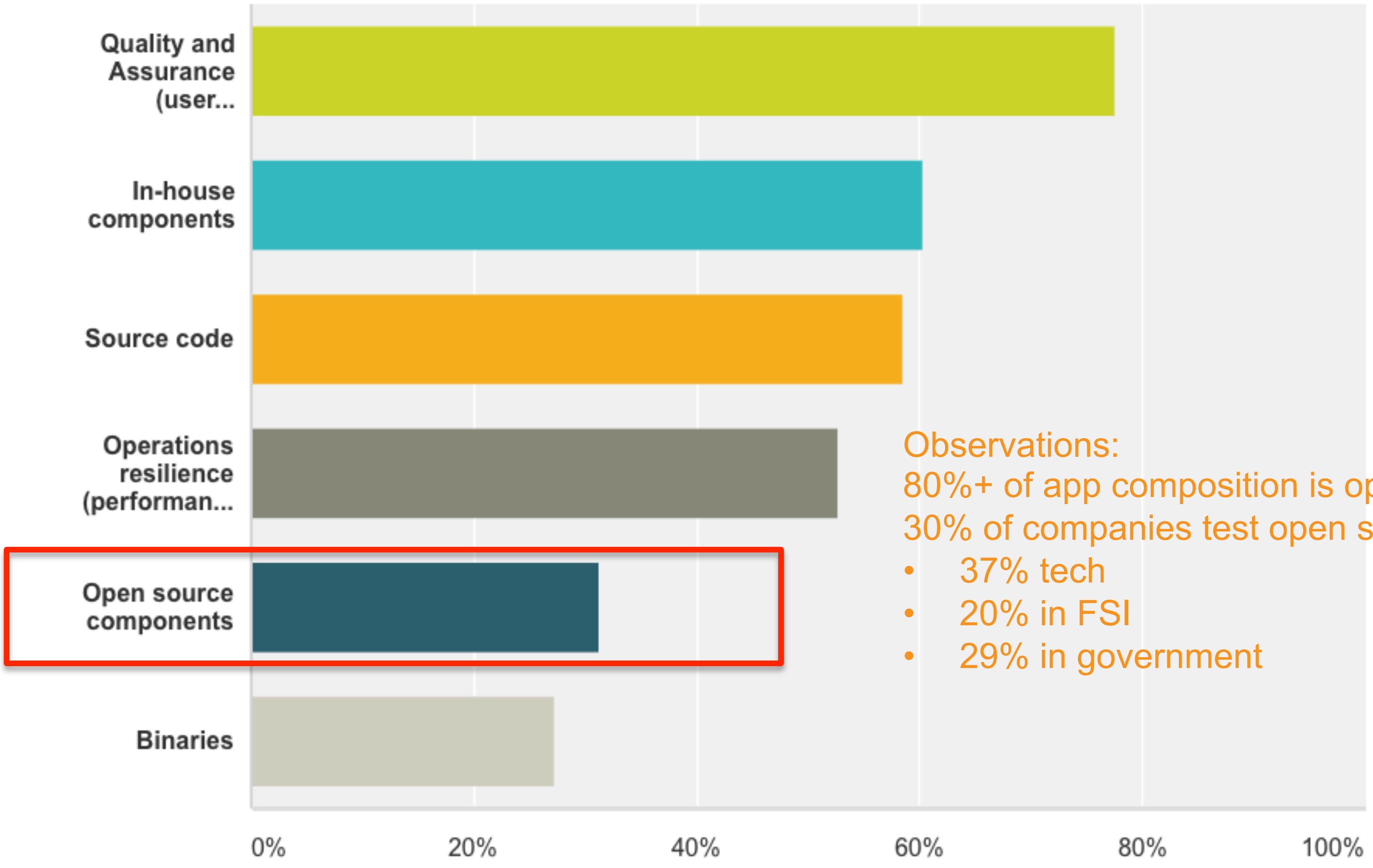
Highest Cost

Lower Cost

High Cost

Lower Cost

Q18 - What are you testing?



Observations:
80%+ of app composition is open source
30% of companies test open source

- 37% tech
- 20% in FSI
- 29% in government

Summary

Get the deck right now, within seconds

Community@Sonatype.com

Survey Sponsors

TSWA

cigital

DEVOPS WEEKLY
A weekly slice of devops news

DevOps Days

hp

Sonatype

DevOpsCafe

usenix
LISA14

Mark Miller, Senior Storyteller

Developers and Application Security: Who is Responsible?

SURVEY RESULTS, November 2014