APPSEC BEST PRACTICES FOR 3RD PARTY SUPPLY CHAIN MANAGEMENT

NAVIGATING THE RISK

AGENDA

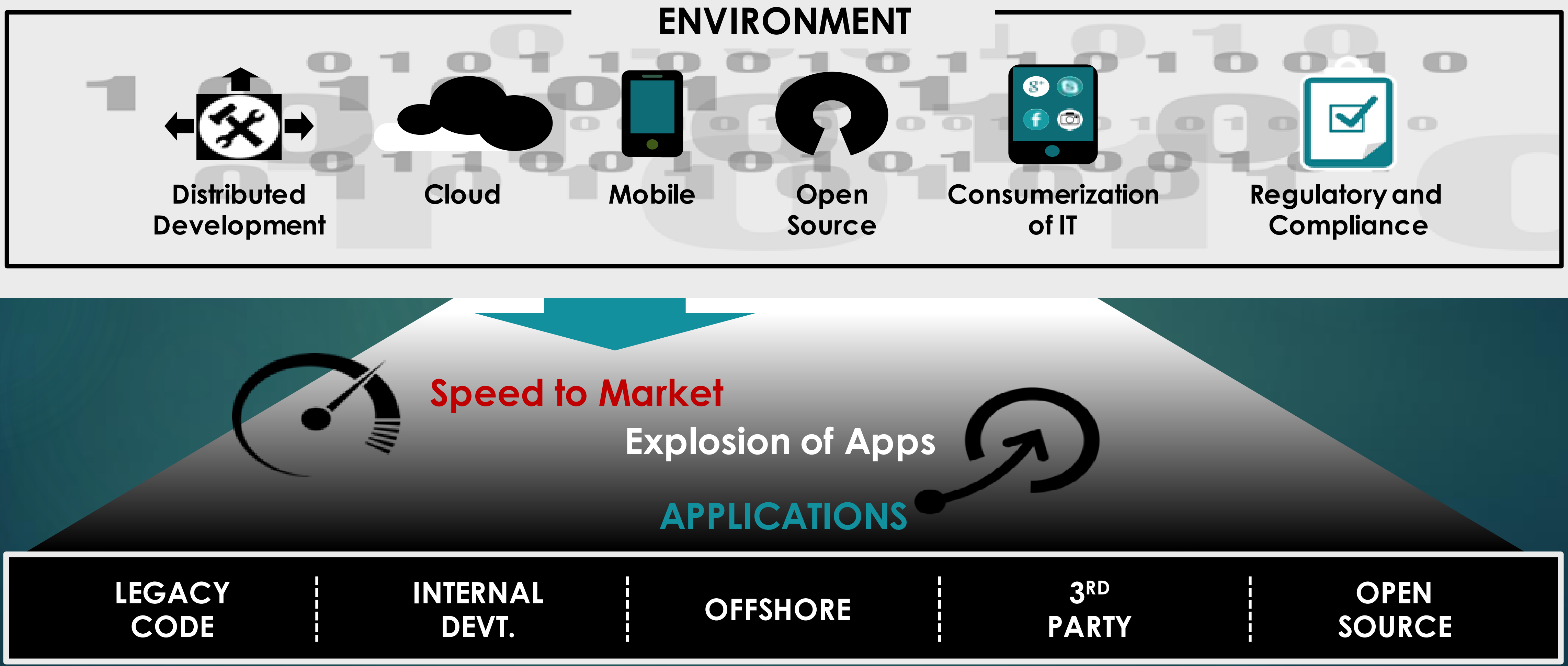
- The Current State of Software Security
- The People
- The Processes
- The Policy
- Closing

THE CURRENT STATE OF SOFTWARE SECURITY

SOFTWARE POWERS EVERY COMPANY

APPLICATION SECURITY IS A MONSTER PROBLEM

Increasingly Complex



ENVIRONMENT

Distributed Development

Cloud

Mobile

Open Source

Consumerization of IT

Regulatory and Compliance

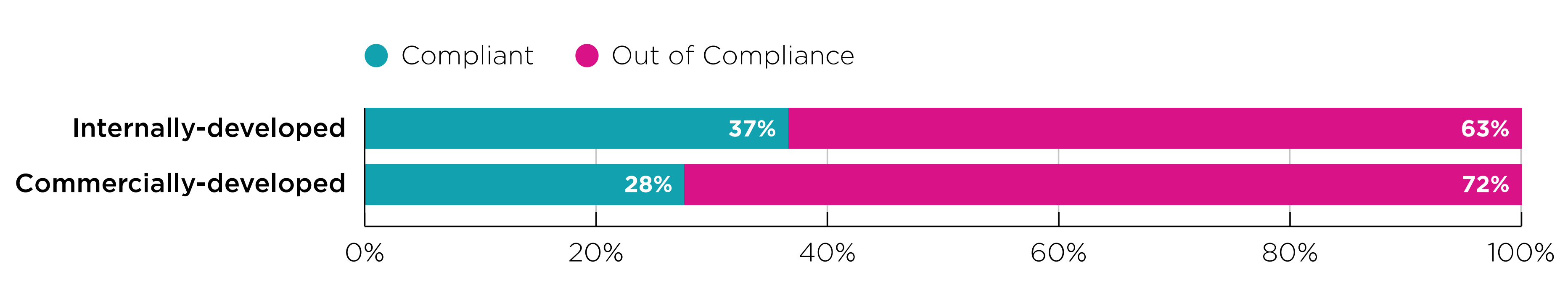
Speed to Market

Explosion of Apps

APPLICATIONS

LEGACY CODE	INTERNAL DEVT.	OFFSHORE	3RD PARTY	OPEN SOURCE

3rd PARTY TO INTERNALLY DEVELOPED APPLICATIONS COMPARISON



Source: SoSS Volume 6 Report

- Supply chain introduces significant risk
- Nearly 3 out of 4 applications produced by third parties fail OWASP Top 10

Compliance to OWASP Top 10 by Industry

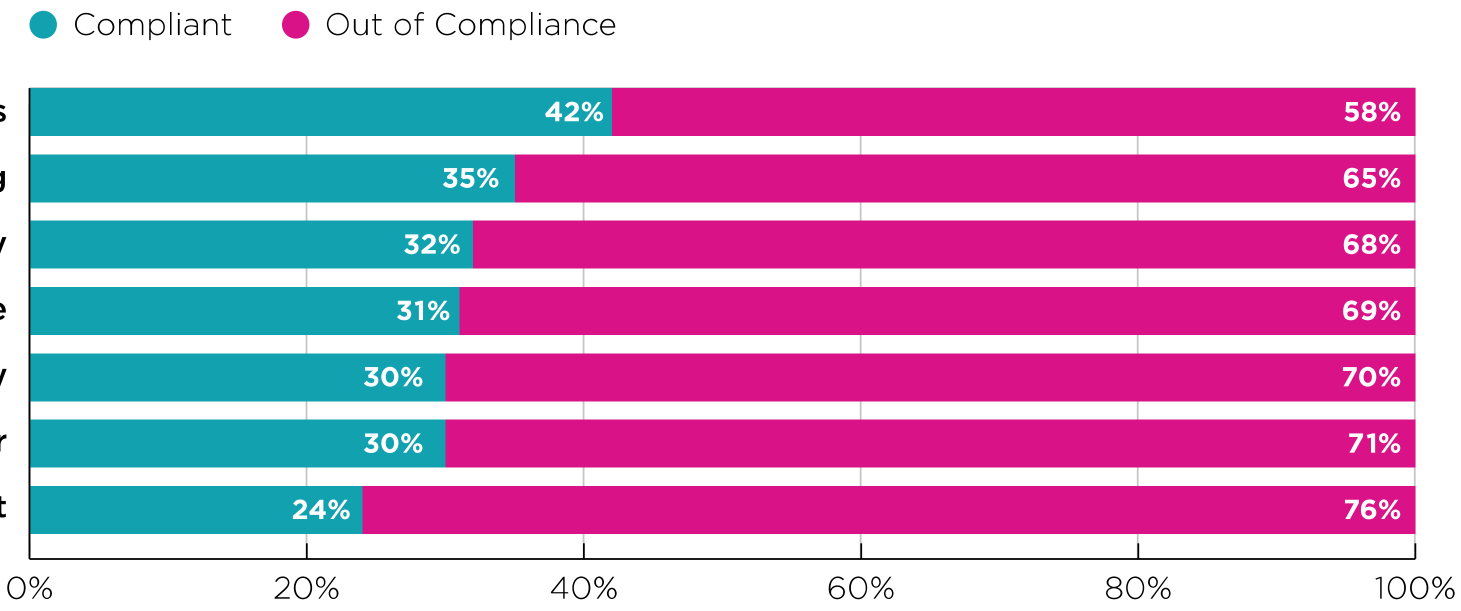


Figure 1: Compliance with OWASP Top 10 Policy on First Risk Assessment, by Industry Vertical

Source: SoSS V olume 6 Report

CHARACTERISTICS OF A WORLD-CLASS PROGRAM

Architecture Review in Design

Threat modeling of applications

- Vendor Analysis

Centralized Application Security Inventory

- Applications
  - Client Server
  - Web Application
  - Mobile
- Components
  - 3rd Party
  - Vendor

Much Broader Scale than "business critical" apps

- Internally Developed
- Vendor Supplied
- Downloaded

Multiple Testing Techniques

- Static Analysis
- Dynamic Analysis
- Penetration Testing
- Mobile

Risk Based

- Security sets the Policies

Developer Coaching

- Remediation Guidance
- eLearning

Integration into the SDLC

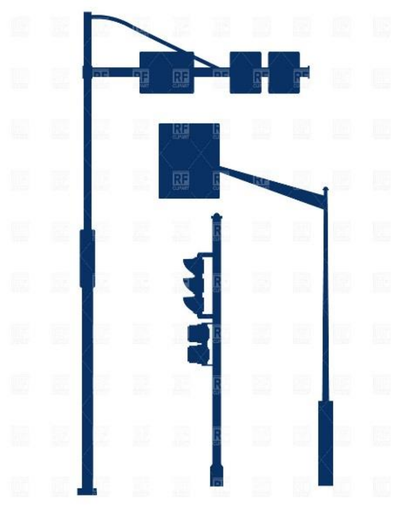
Developer Self Service

Remediate/Mitigate

Other

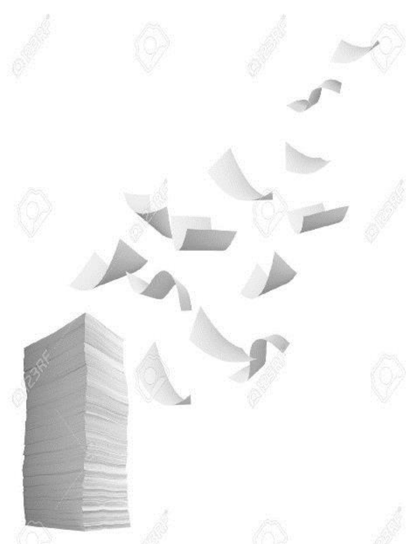
- Web Discovery
- Software Composition Analysis

WORLD-CLASS PROGRAM DEVELOPMENT CHALLENGES



Governance

- No collaborative forum to discuss project risks, action items, and process/product change requests
- Each LOB has process autonomy without overall management and documentation



Standardization

- Program scalability is not possible with multiple documentation standards
- Varying terminology increases likelihood of incorrect actions by program participants

Communications

- Communication protocols are defined and vary by project
- No standardized glossary adopted by all stakeholders
- No documented communication plan or escalation procedures

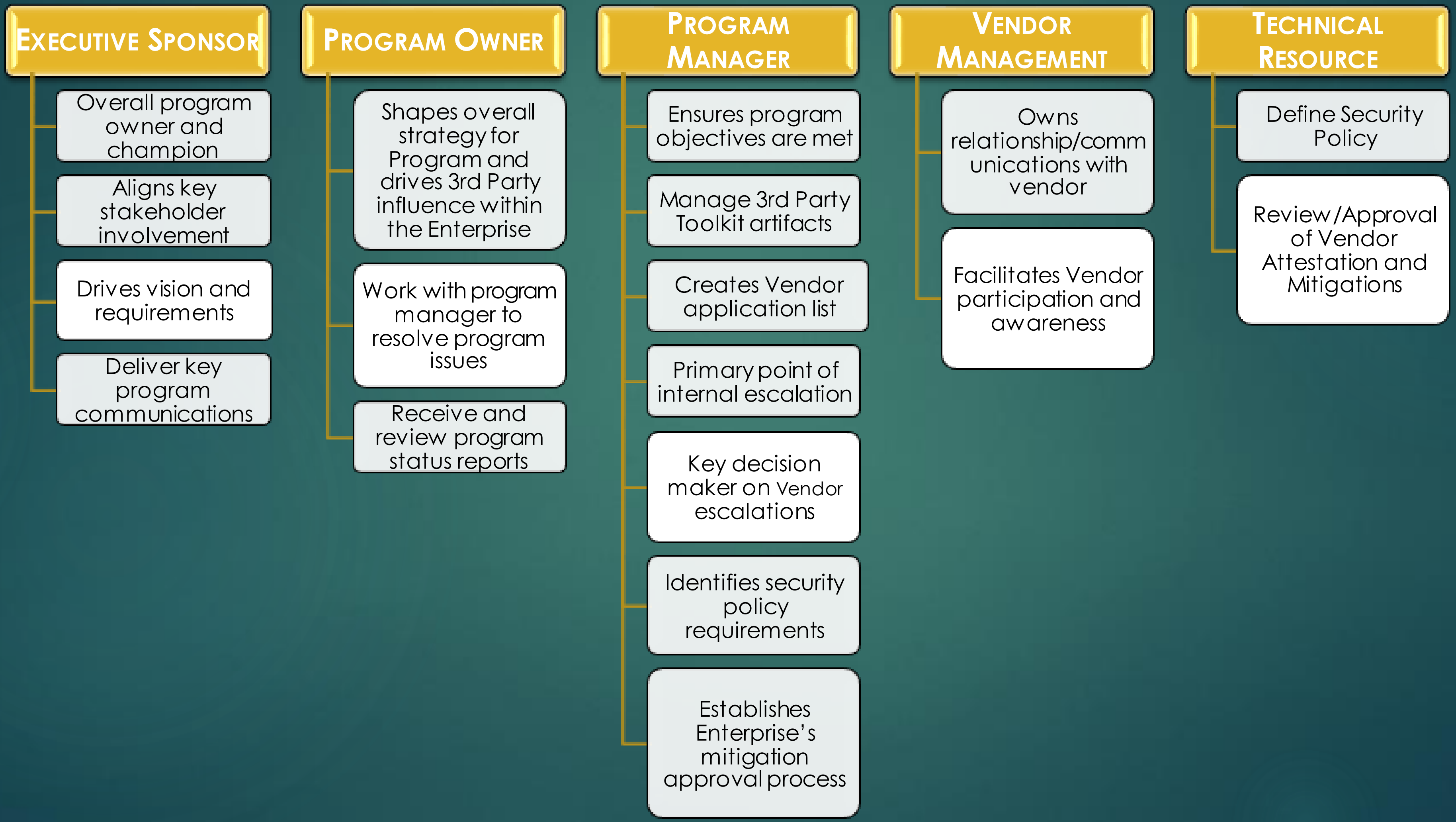
Unclear Roles and Responsibilities

- Absence of Enterprise-level Management Plan leaves gaps in roles and responsibilities;
- Vendor confusion on 3rd-Party program decision making authority

THE PEOPLE

Photo by Tim Gouw, Head of Tales & Stories @IdeationKings – url: https://hd.unsplash.com/photo-1453799527828-cf1bd7b2f682

ENTERPRISE CORE TEAM



Executive Sponsor

- Overall program owner and champion
- Aligns key stakeholder involvement
- Drives vision and requirements
- Deliver key program communications

Program Owner

- Shapes overall strategy for Program and drives 3rd Party influence within the Enterprise
- Work with program manager to resolve program issues
- Receive and review program status reports

Program Manager

- Ensures program objectives are met
- Manage 3rd Party Toolkit artifacts
- Creates Vendor application list
- Primary point of internal escalation
- Key decision maker on Vendor escalations
- Identifies security policy requirements
- Establishes Enterprise's mitigation approval process

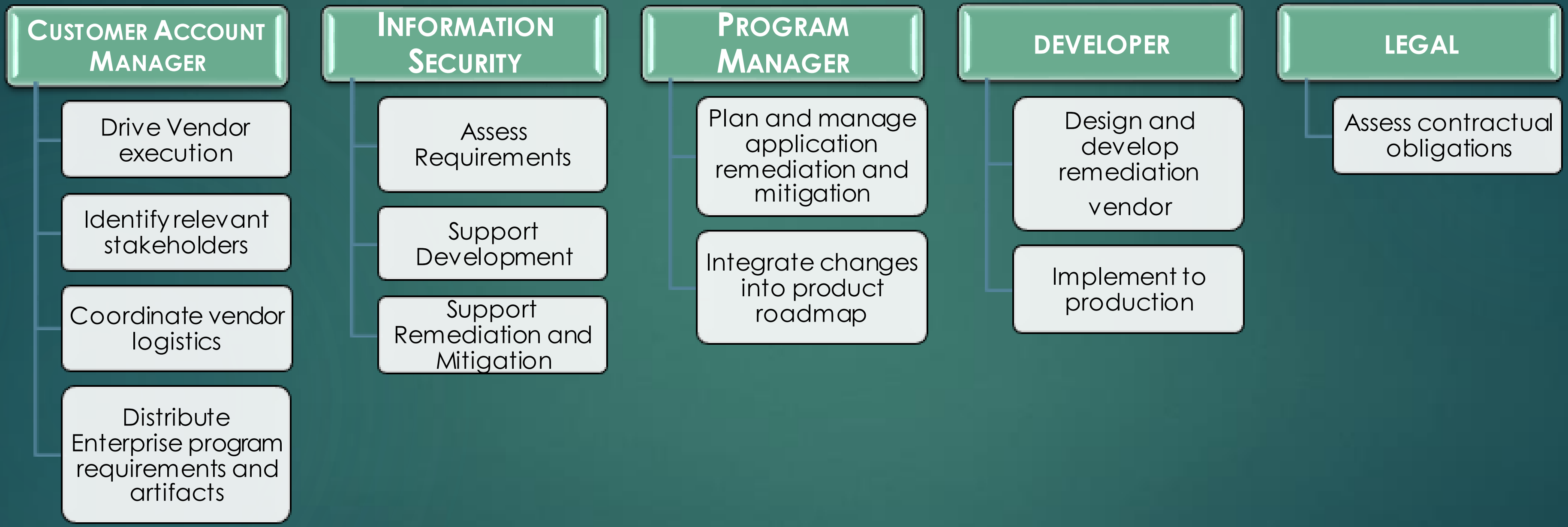
Vendor Management

- Owns relationship/communications with vendor
- Facilitates Vendor participation and awareness

Technical Resource

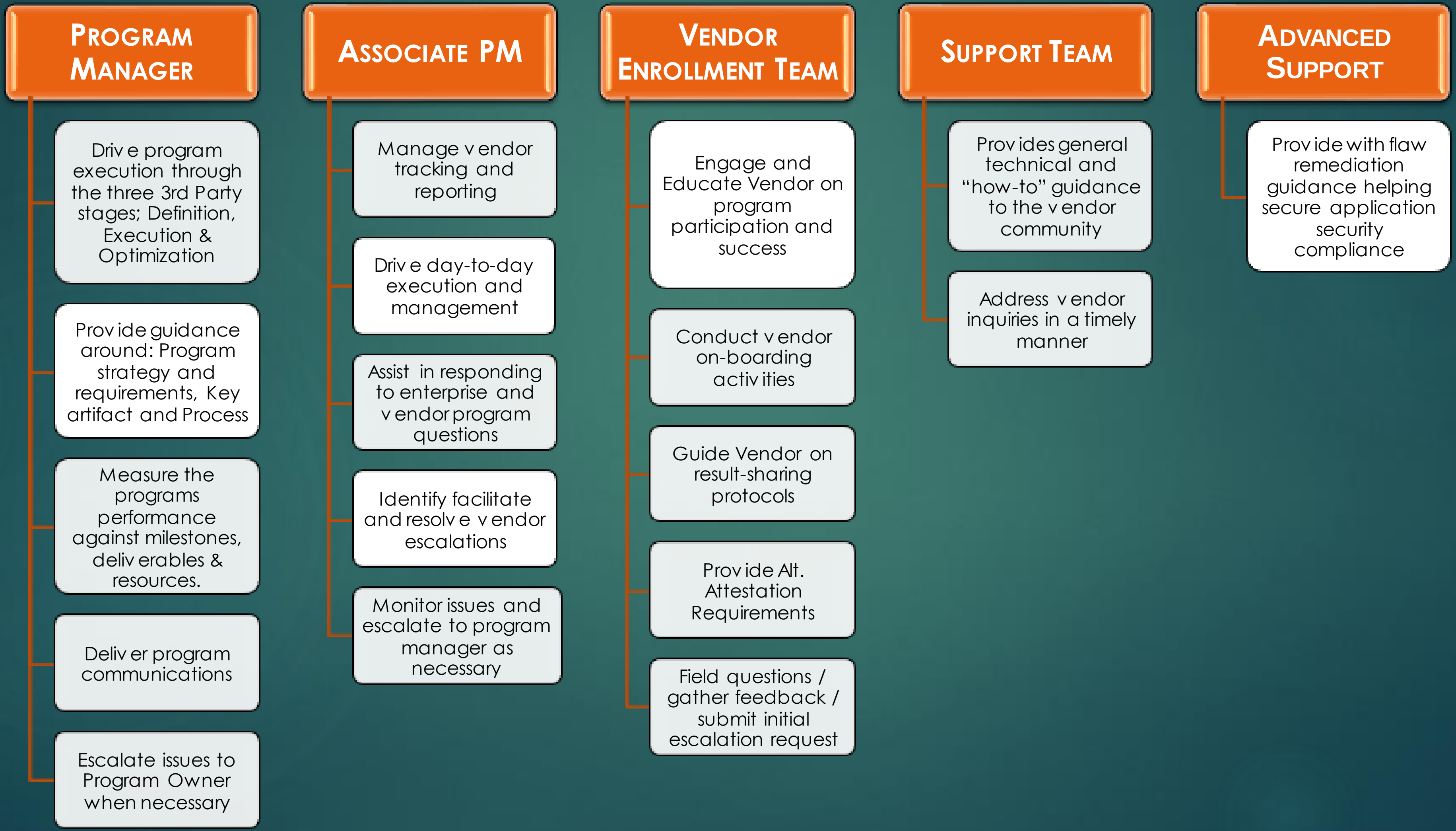
- Define Security Policy
- Review/Approval of Vendor Attestation and Mitigations

VENDOR CORE TEAM



- **Customer Account Manager**
  - Drive Vendor execution
  - Identify relevant stakeholders
  - Coordinate vendor logistics
  - Distribute Enterprise program requirements and artifacts
- **Information Security**
  - Assess Requirements
  - Support Development
  - Support Remediation and Mitigation
- **Program Manager**
  - Plan and manage application remediation and mitigation
  - Integrate changes into product roadmap
- **DEVELOPER**
  - Design and develop remediation vendor
  - Implement to production
- **LEGAL**
  - Assess contractual obligations

SECURITY TESTING SERVICE PROVIDER CORE TEAM



Program Manager

- Drive program execution through the three 3rd Party stages; Definition, Execution & Optimization
- Provide guidance around: Program strategy and requirements, Key artifact and Process
- Measure the programs performance against milestones, deliverables & resources.
- Deliver program communications
- Escalate issues to Program Owner when necessary

Associate PM

- Manage vendor tracking and reporting
- Drive day-to-day execution and management
- Assist in responding to enterprise and vendor program questions
- Identify facilitate and resolve vendor escalations
- Monitor issues and escalate to program manager as necessary

Vendor Enrollment Team

- Engage and Educate Vendor on program participation and success
- Conduct vendor on-boarding activities
- Guide Vendor on result-sharing protocols
- Provide Alt. Attestation Requirements
- Field questions / gather feedback / submit initial escalation request

Support Team

- Provides general technical and "how-to" guidance to the vendor community
- Address vendor inquiries in a timely manner

Advanced Support

- Provide with flaw remediation guidance helping secure application security compliance

THE PROCESSES

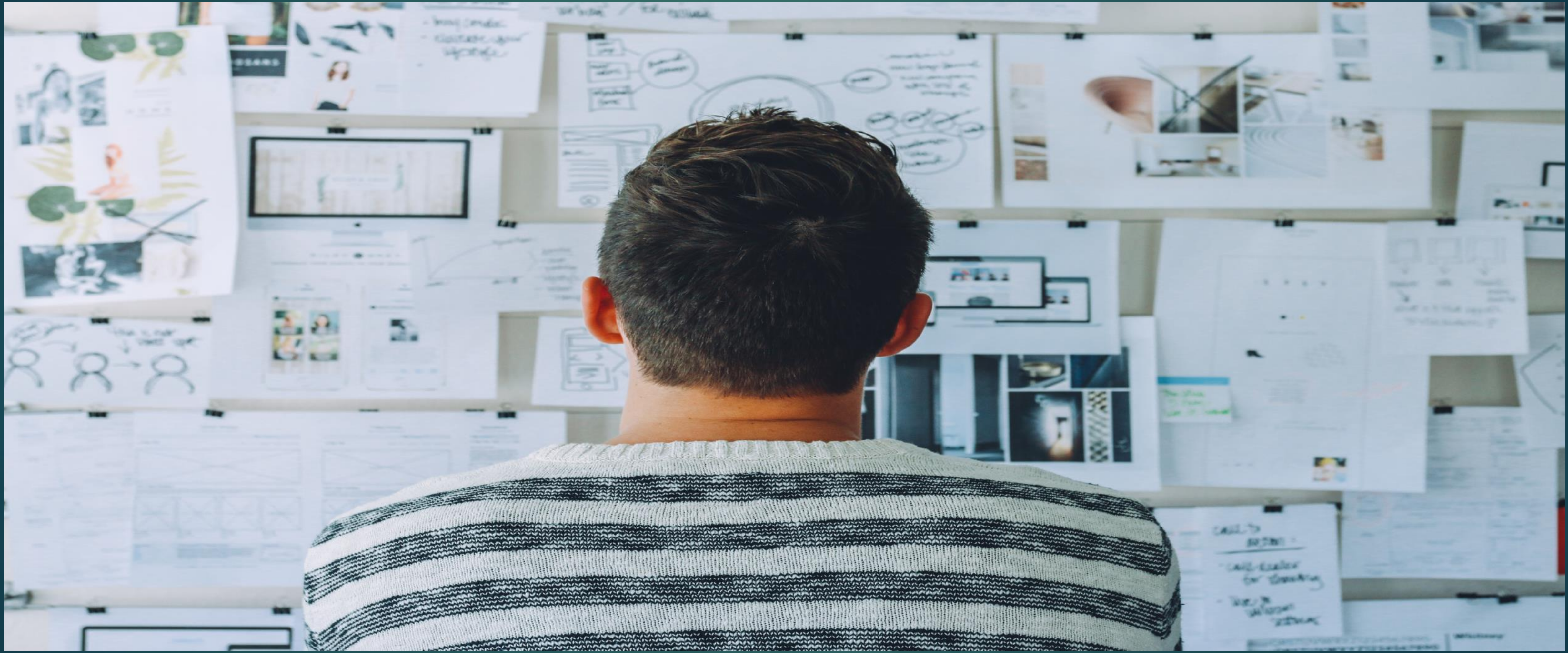
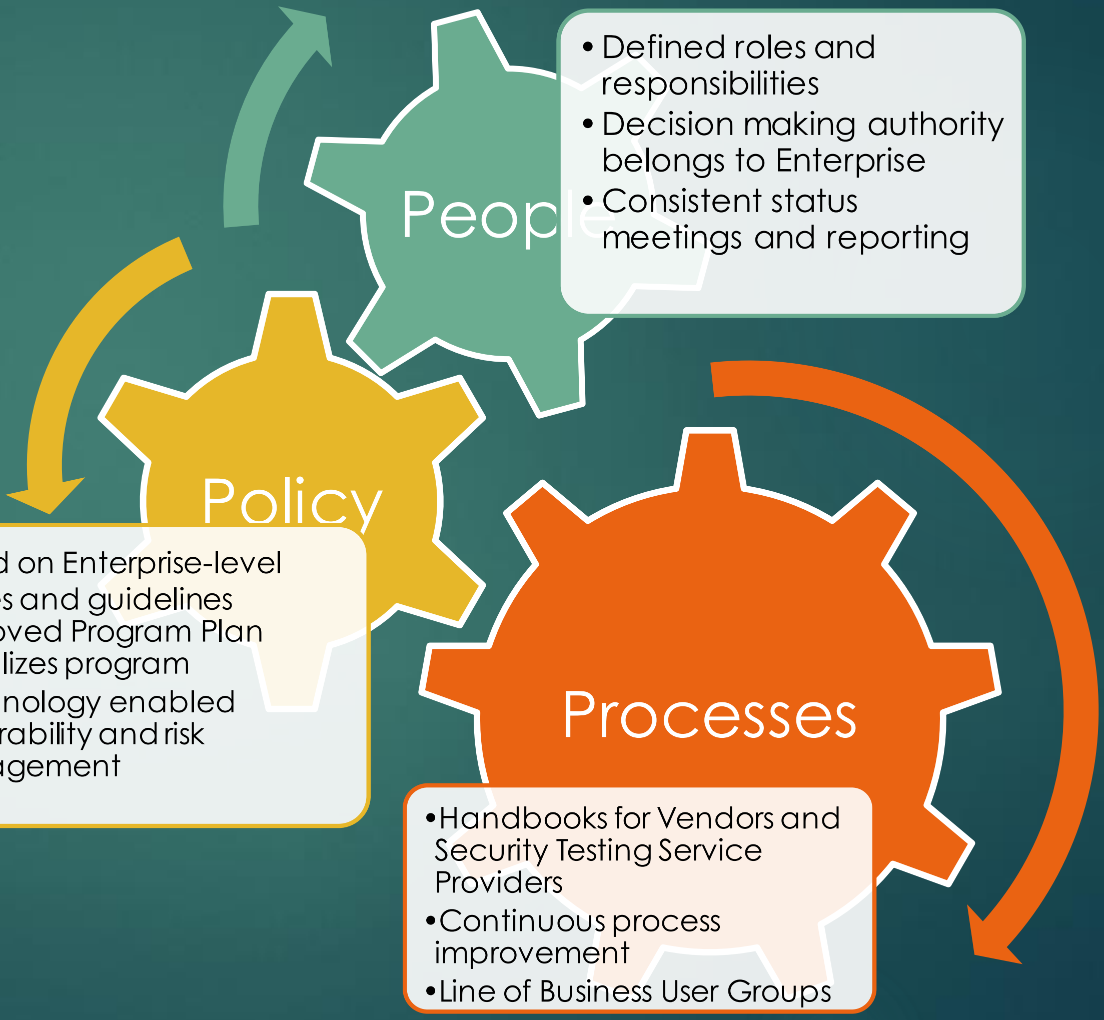


Photo by Startup Stock Photos, a *project by* *@estrattonbailey* *and* *@wearesculpt* –
url: https://s3.amazonaws.com/StartupStockPhotos/uploads/20160503/6.jpg

BALANCE IS KEY

- Application Security Consultants
- Support Engineers
- Security Program Manager

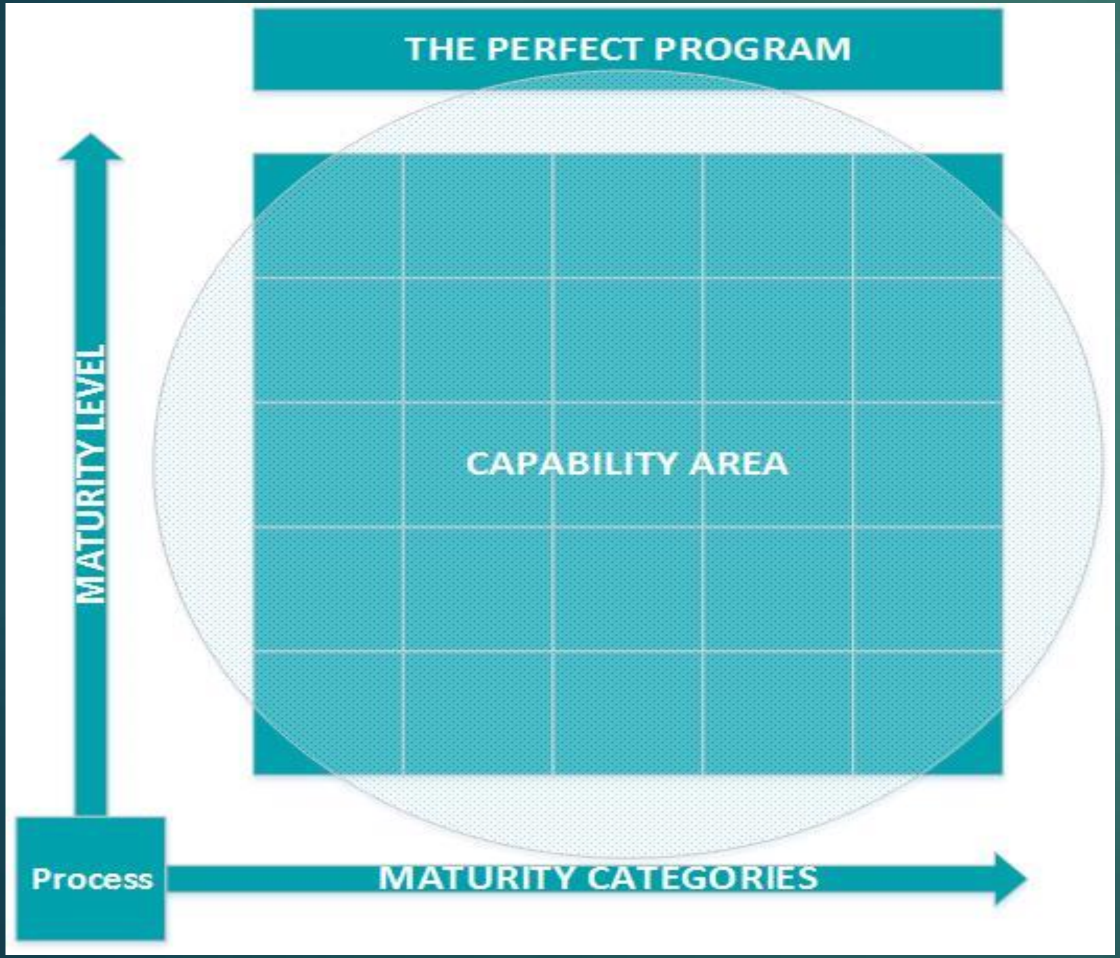


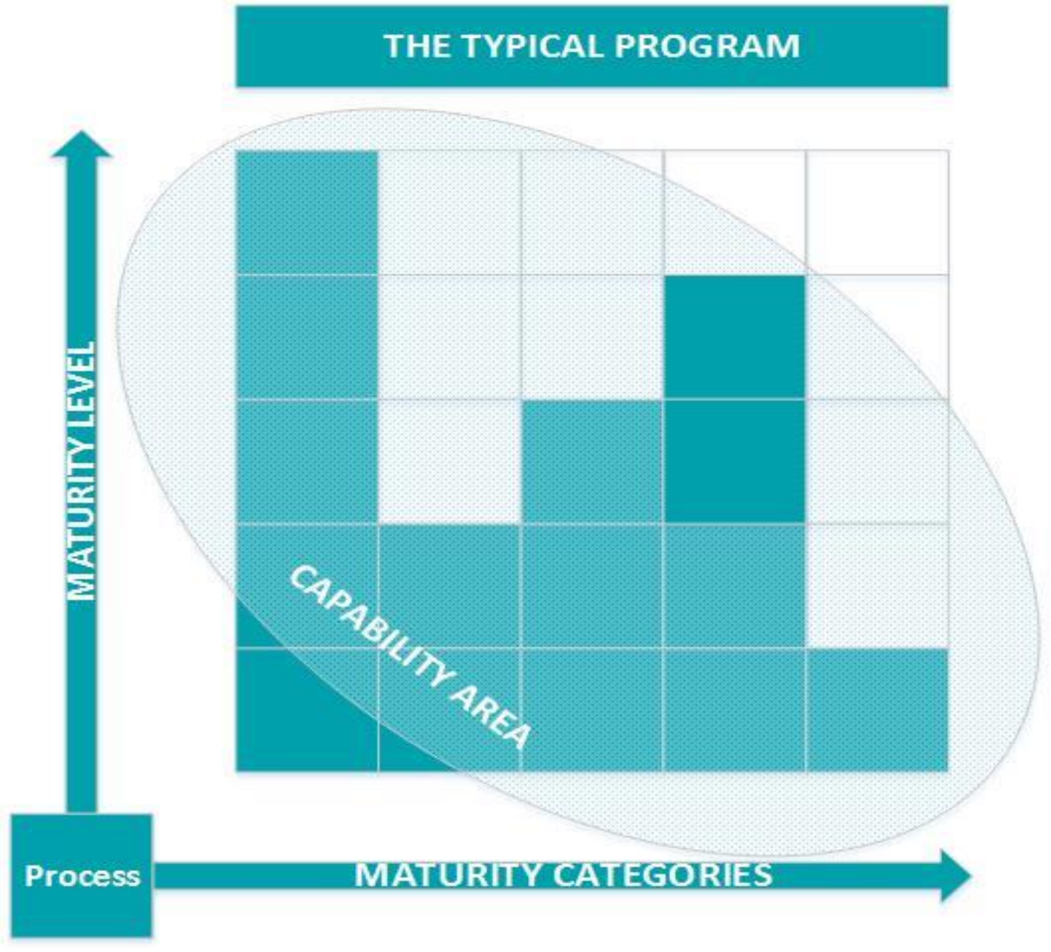
- Defined roles and responsibilities
- Decision making authority belongs to Enterprise
- Consistent status meetings and reporting

•Based on Enterprise-level policies and guidelines
Approved Program Plan formalizes program
•Technology enabled vulnerability and risk management

•Handbooks for Vendors and Security Testing Service Providers
•Continuous process improvement
•Line of Business User Groups

MATURITY MODEL BASICS

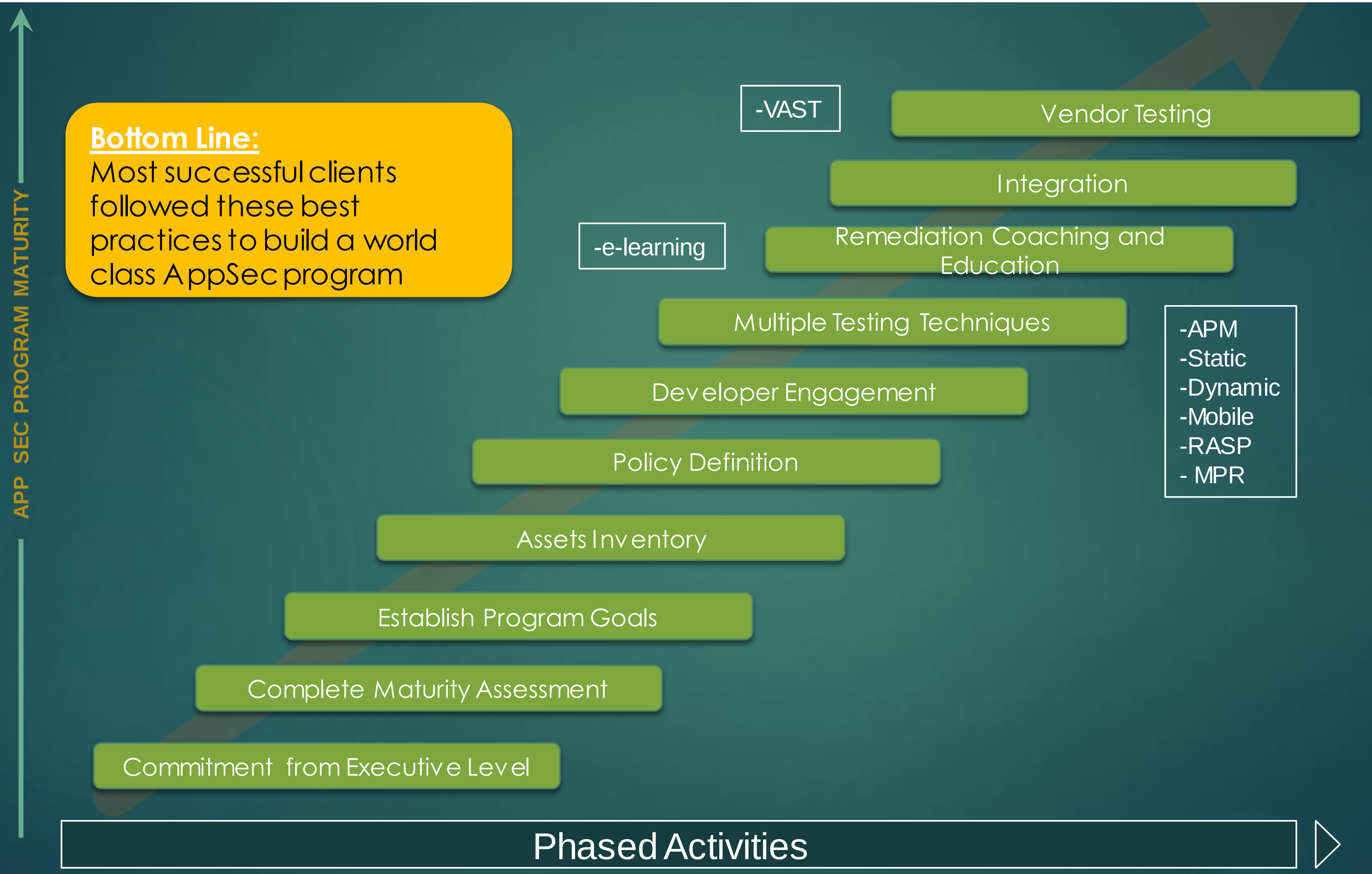




3RD PARTY PROGRAM MATURITY AREA EXAMPLES

- Enterprise 3rd Party AppSec Maturity
- Strength of Mandate
- Strength of Education and Awareness Program
- Level of Enterprise Investment
- Application Inventory Maturity
- Internal Support Programs Maturity
- Extenuating Criteria

START WHERE YOU ARE



Bottom Line:
Most successful clients followed these best practices to build a world class AppSec program

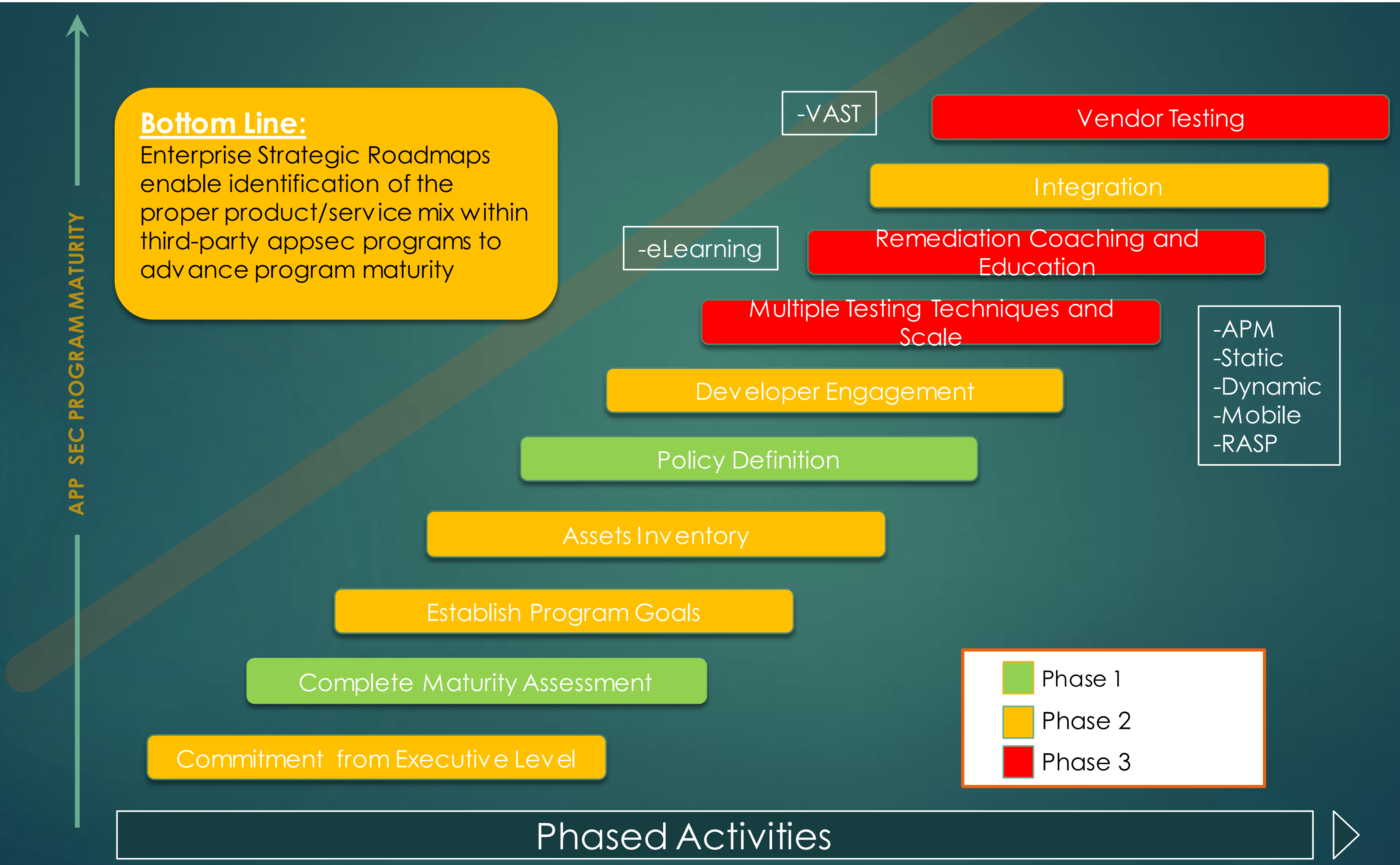
APP SEC PROGRAM MATURITY

- Commitment from Executive Level
- Complete Maturity Assessment
- Establish Program Goals
- Assets Inventory
- Policy Definition
- Developer Engagement
- Multiple Testing Techniques
  - -APM
  - -Static
  - -Dynamic
  - -Mobile
  - -RASP
  - - MPR
- Remediation Coaching and Education
  - -e-learning
- Integration
- Vendor Testing
  - -VAST

Phased Activities

MATURE FROM THERE

Bottom Line:
Enterprise Strategic Roadmaps enable identification of the proper product/service mix within third-party appsec programs to advance program maturity



APP SEC PROGRAM MATURITY

-VAST

Vendor Testing

Integration

-eLearning

Remediation Coaching and Education

Multiple Testing Techniques and Scale

-APM
-Static
-Dynamic
-Mobile
-RASP

Developer Engagement

Policy Definition

Assets Inventory

Establish Program Goals

Complete Maturity Assessment

Commitment from Executive Level

🟩 Phase 1
🟨 Phase 2
🟥 Phase 3

Phased Activities

PROGRAM FOUNDATIONAL DOCUMENTS

- Program Guide
  - Defines the level of investment that the enterprise is providing, and what they can expect from V eracode
  - Describes roles and responsibilities in the 3rd Party program
  - Umbrella document to be shared internally to gain team alignment and support
- Executive Notification Letter
  - Introduces the Program and Expectations to the Supplier, confirming the importance of compliance by the Enterprise
- Vendor FAQ
  - Ready made resource to address many V endor questions/concerns
- Tailoring Plan
  - Defines scope of complex application projects, captures project milestones, and documents roles and responsibilities
- Communications Plan
  - Executive and tactical levels communications templates that ensure consistency, scalability, ad repeatability in communications

THE POLICY

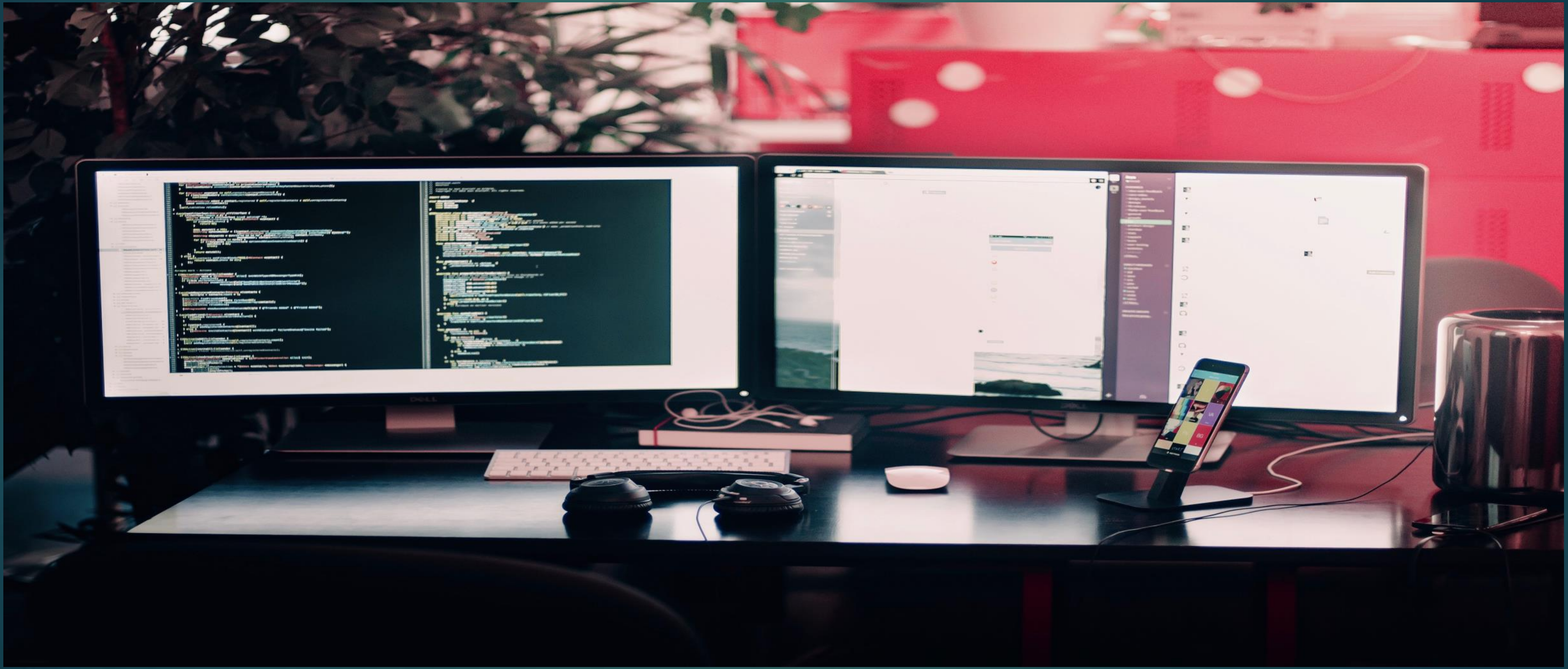
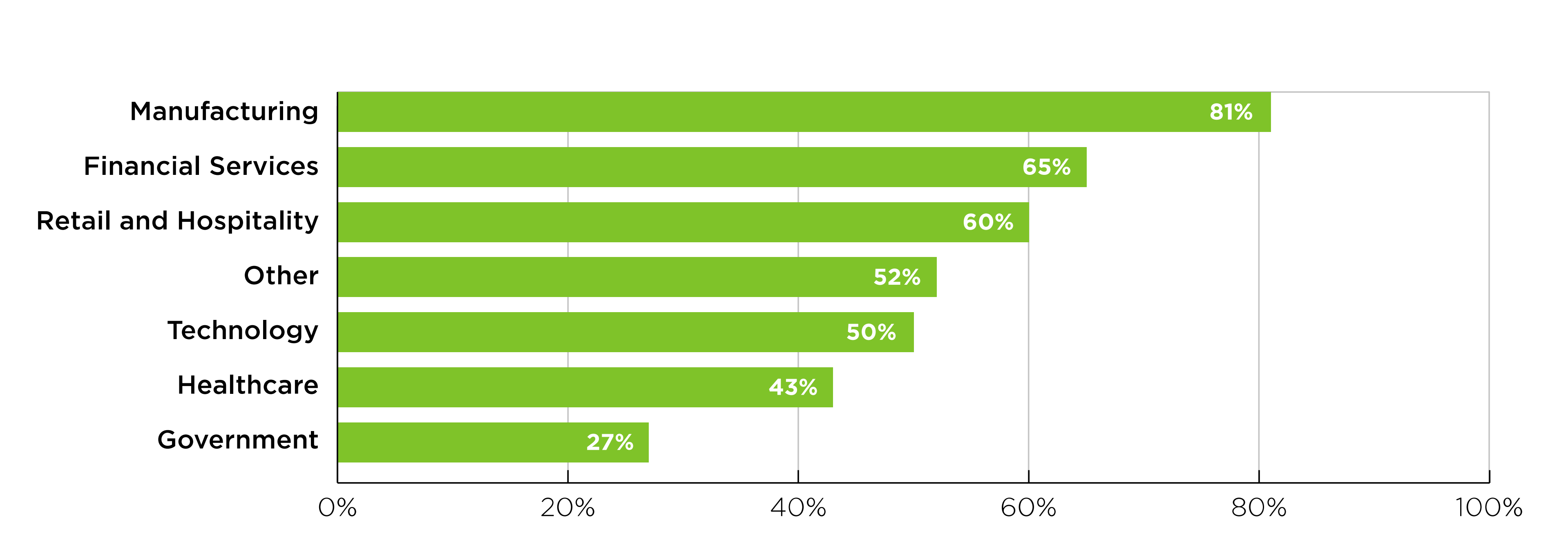


Photo by **Farzad Nazifi** – url: https://unsplash.com/photos/p-xSl33Wxyc

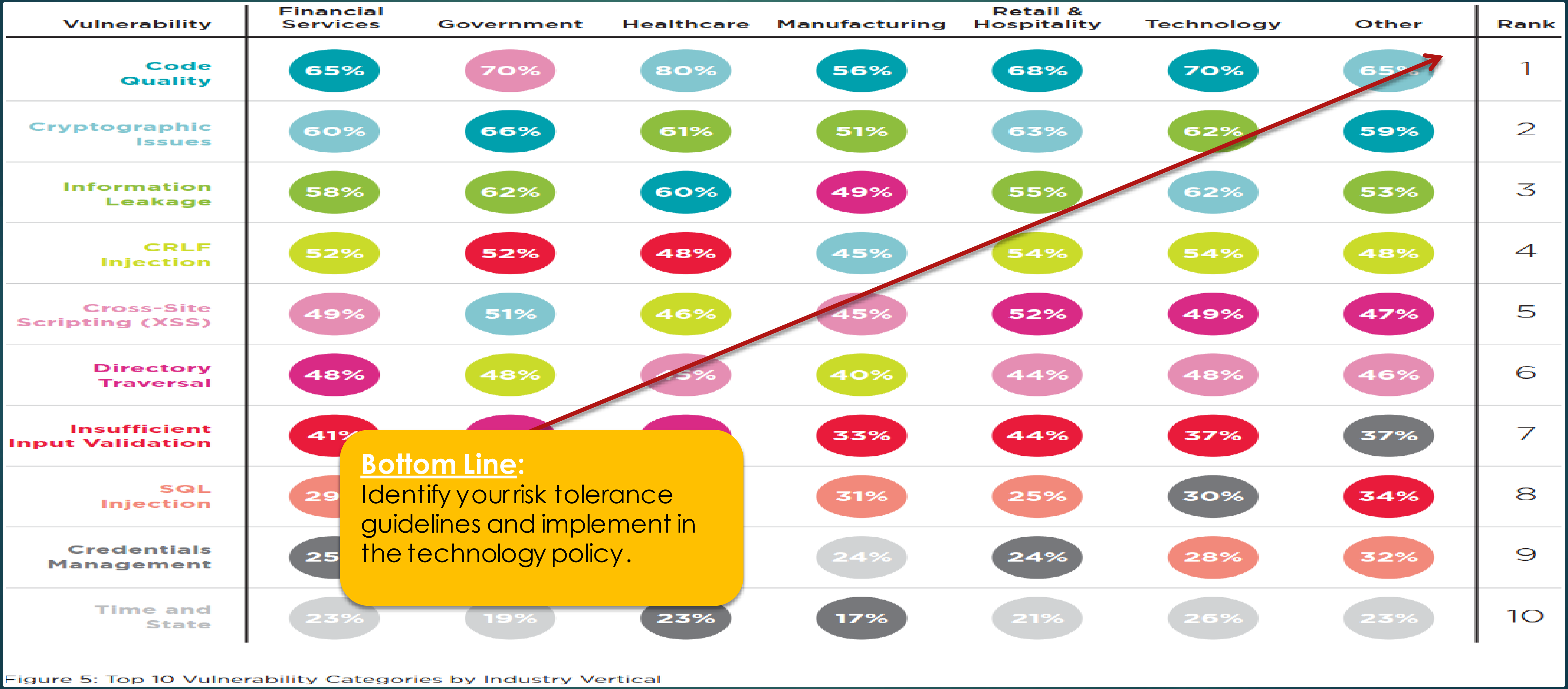
REMEDIATION BY INDUSTRY VERTICAL

- Financial Services and Manufacturing are most secure
- Remediate most of their vulnerabilities, 65% and 81% respectively
- Higher enforcement of enterprise wide policies and continuous improvement



Source: SoSS Volume 6 Report

USE POLICY TO DETERMINE COMPLIANCE AND BASELINE RISK PROFILE



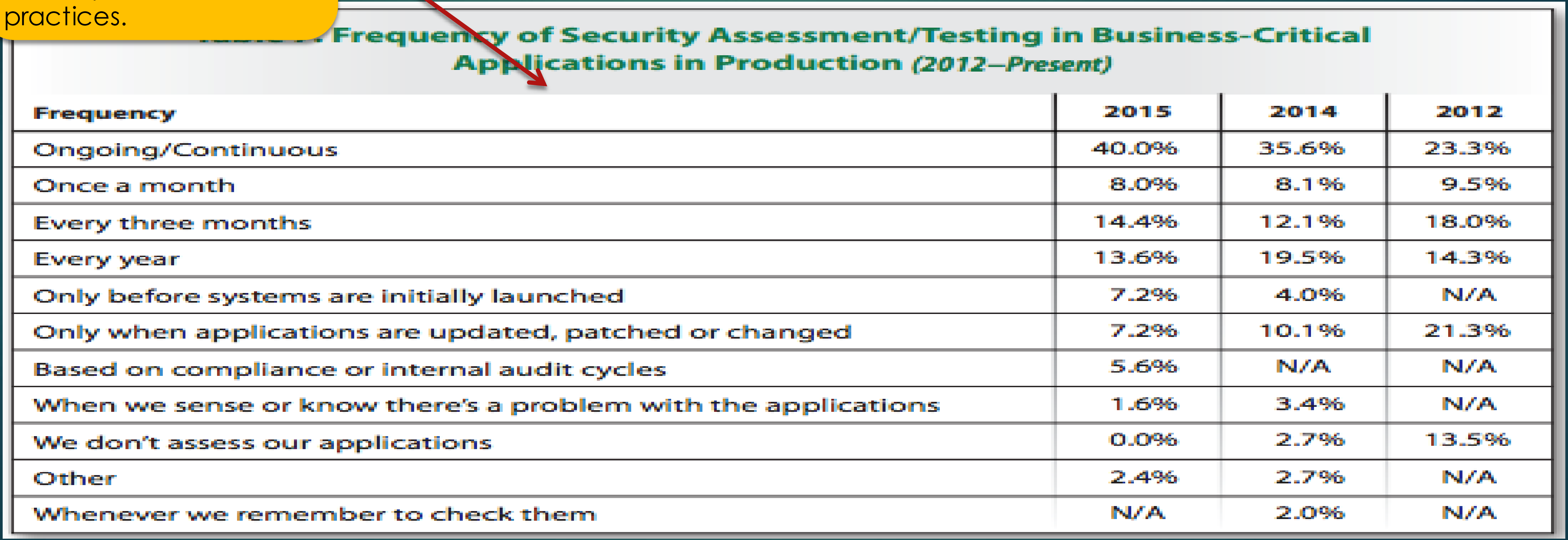
Vulnerability	Financial Services	Government	Healthcare	Manufacturing	Retail & Hospitality	Technology	Other	Rank
Code Quality	65%	70%	80%	56%	68%	70%	65%	1
Cryptographic Issues	60%	66%	61%	51%	63%	62%	59%	2
Information Leakage	58%	62%	60%	49%	55%	62%	53%	3
CRLF Injection	52%	52%	48%	45%	54%	54%	48%	4
Cross-Site Scripting (XSS)	49%	51%	46%	45%	52%	49%	47%	5
Directory Traversal	48%	48%	45%	40%	44%	48%	46%	6
Insufficient Input Validation	41%			33%	44%	37%	37%	7
SQL Injection	29			31%	25%	30%	34%	8
Credentials Management	25			24%	24%	28%	32%	9
Time and State	23%	19%	23%	17%	21%	26%	23%	10

Figure 5: Top 10 Vulnerability Categories by Industry Vertical

Bottom Line:
Identify your risk tolerance guidelines and implement in the technology policy.

USE REMEDIATION TIMETABLES TO DRIVE RISK REDUCTION

Bottom Line:
Codifying remediation timetables into policy enforces secure development best practices.



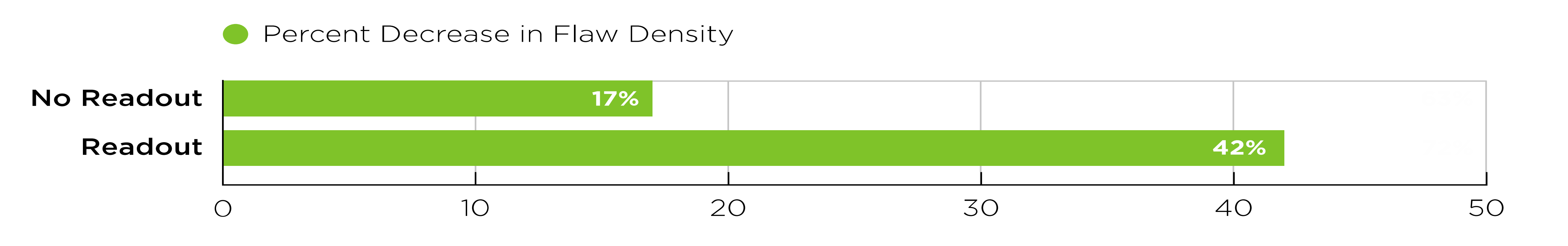
Frequency of Security Assessment/Testing in Business-Critical Applications in Production *(2012—Present)*

Frequency	2015	2014	2012
Ongoing/Continuous	40.0%	35.6%	23.3%
Once a month	8.0%	8.1%	9.5%
Every three months	14.4%	12.1%	18.0%
Every year	13.6%	19.5%	14.3%
Only before systems are initially launched	7.2%	4.0%	N/A
Only when applications are updated, patched or changed	7.2%	10.1%	21.3%
Based on compliance or internal audit cycles	5.6%	N/A	N/A
When we sense or know there's a problem with the applications	1.6%	3.4%	N/A
We don't assess our applications	0.0%	2.7%	13.5%
Other	2.4%	2.7%	N/A
Whenever we remember to check them	N/A	2.0%	N/A

Source: SANS Application Security Survey

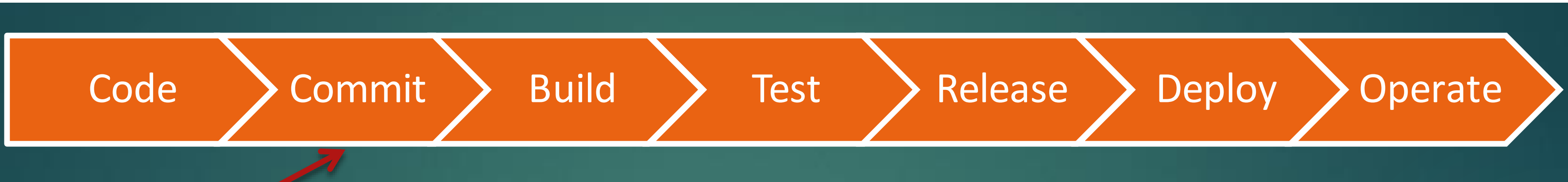
REDUCTION IN FLAW DENSITY

- Flaw density is represented as number of vulnerabilities per MB of code.
- Remediation coaching has a big impact on reducing application risk
- Development teams that use Veracode's experts to help them remediate fix 2.5 times as many flaws as those who go it on their own.



Source: SoSS Volume 6 Report

APPLICATION SECURITY BEST PRACTICES



Bottom Line:
Mature AppSec programs that utilize scanning and remediation early in the SDLC have less flaws introduced in implementation.

Design and Build: Consider compliance and privacy requirements; design security features; develop use cases and abuse cases; complete attack surface analysis; conduct threat modeling; follow secure coding standards; use secure libraries and use the security features of application frameworks and languages.

Test: Use dynamic analysis (DAST), static analysis (SAST), interactive application security testing (IAST), fuzzing, code reviews, pen testing, bug bounty programs and secure component lifecycle management.

Fix: Conduct vulnerability remediation, root cause analysis, web application firewalls (WAF) and virtual patching and runtime application self-protection (RASP).

Govern: Insist on oversight and risk management; secure SDLC practices, metrics and reporting; vulnerability management; secure coding training; and managing third-party software risk.

BALANCING PEOPLE, PROCESS, AND TECHNOLOGY

Thank You