# DevSecOps Assessment and Maturity Model

*Presented by ASMGi*

October 26, 2020

# Today's Presenters – *DevSecOps Assessment and Maturity Model*

**John Meyer**

*Solutions Architect, ASMGi*

*jmeyer@asmgi.com*





**Frank Yako**

*CIO, Director of Strategic Initiatives*

*fyako@asmgi.com*

# Agenda

◆ What does it mean to "Move to the Left"?

◆ Introduction and Objectives

◆ Overview of SDLC

◆ What is DevOps why DevOps was Adopted?

◆ DevOps to DevSecOps

◆ Methods to determine DevSecOps maturity

◆ How Does an Organization Assess DevSecOps Maturity and Apply It?

# What does it mean to "Move to the Left"?

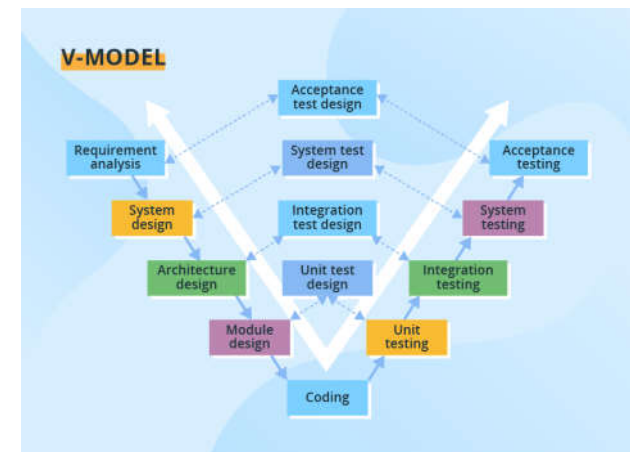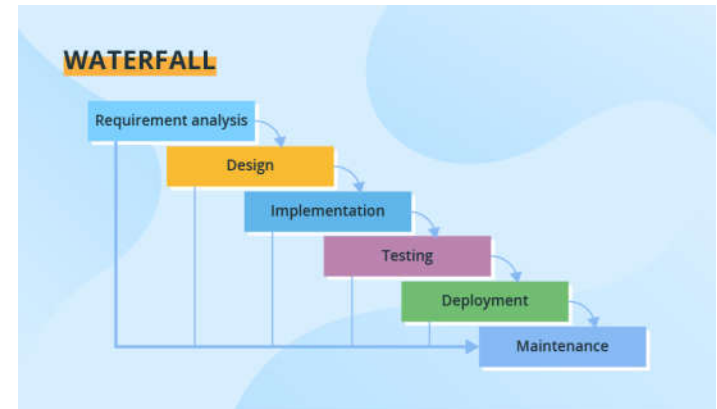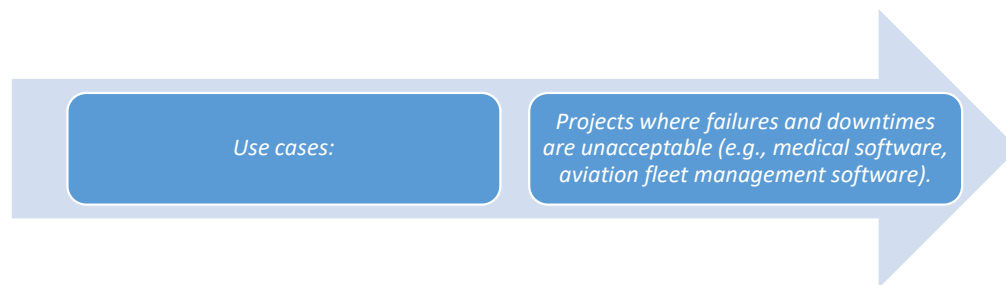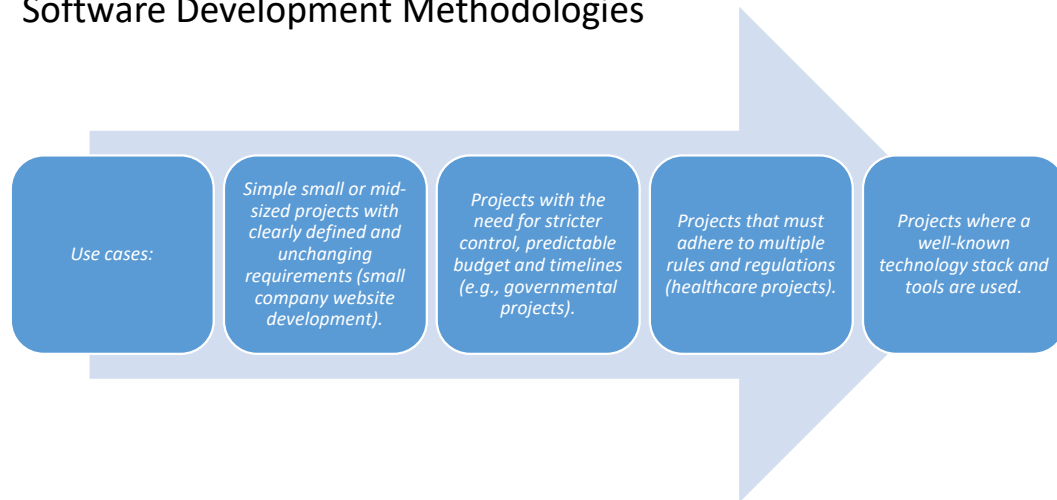*Security moves from an afterthought to the forefront (e.g. "To the Left") thus*

# *DevSecOps*

# Introduction and Objectives

◆ Provide an Overview and Introduction to DevOps and DevSecOps

◆ Discuss the Reasons why an Organization would Consider adopting DevSecOps

◆ Compare the Differences between DevOps and DevSecOps

◆ Explore How to begin the "Move to the Left"

◆ How an Organization integrates DevSecOps and Matures

# The Legacy Software Development Lifecycle

## Software Development Methodologies

**Use cases:** Simple small or mid-sized projects with clearly defined and unchanging requirements (small company website development). | Projects with the need for stricter control, predictable budget and timelines (e.g., governmental projects). | Projects that must adhere to multiple rules and regulations (healthcare projects). | Projects where a well-known technology stack and tools are used.

**Use cases:** Projects where failures and downtimes are unacceptable (e.g., medical software, aviation fleet management software).

### WATERFALL

- Requirement analysis
- Design
- Implementation
- Testing
- Deployment
- Maintenance

### V-MODEL

- Requirement analysis
- System design
- Architecture design
- Module design
- Coding
- Unit test design
- Integration test design
- System test design
- Acceptance test design
- Unit testing
- Integration testing
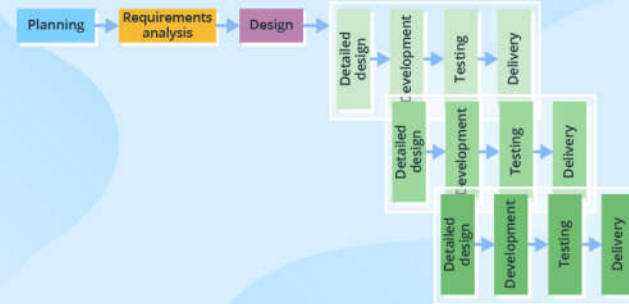- System testing
- Acceptance testing

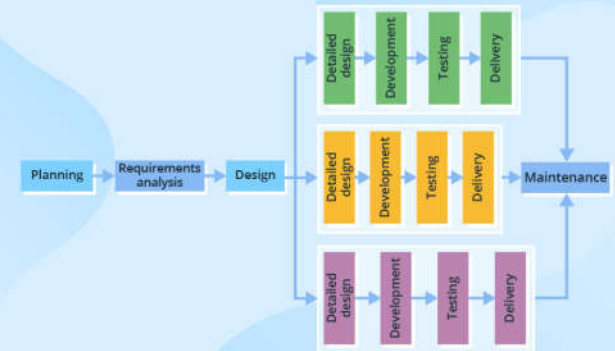# Alternative Software Development Methodologies



**Use cases:** Large, mission-critical enterprise applications that preferably consist of loosely coupled parts, such as microservices or web services.
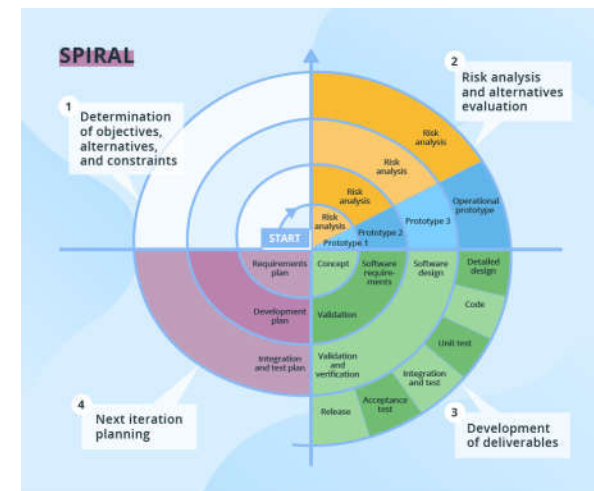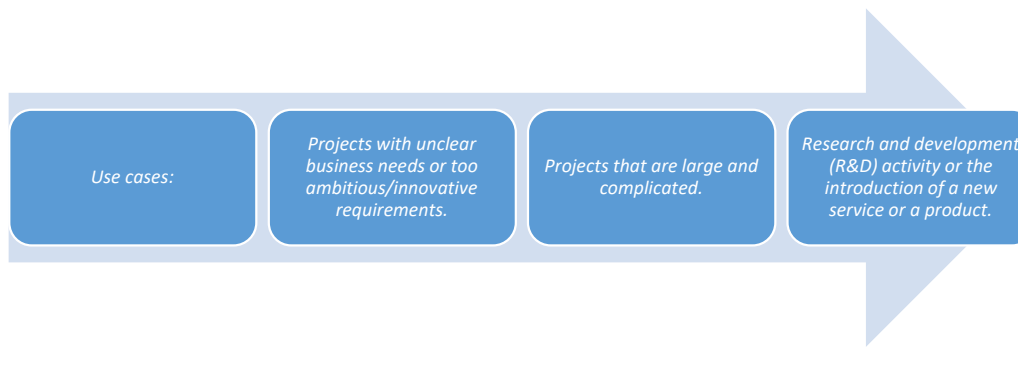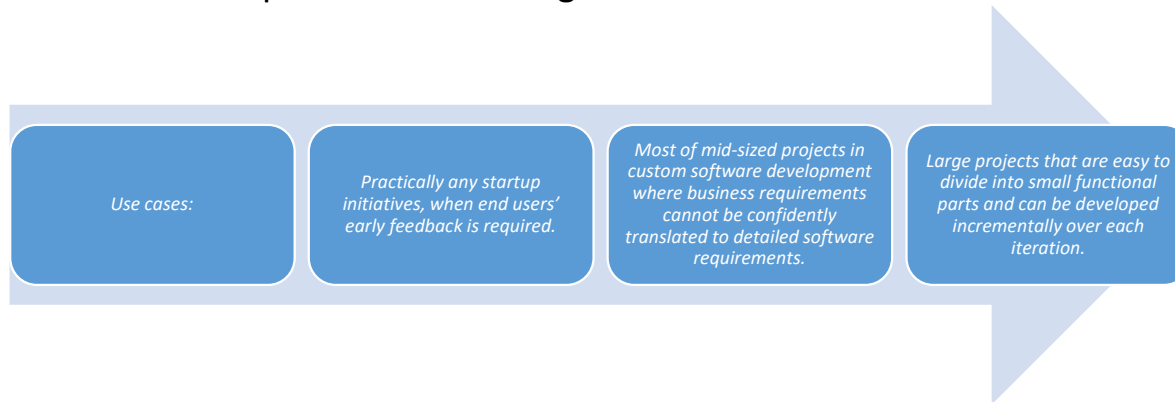
ITERATIVE MODEL

Planning → Requirements analysis → Design → Detailed design → Development → Testing → Delivery

INCREMENTAL MODEL

Planning → Requirements analysis → Design → Detailed design → Development → Testing → Delivery → Maintenance

# The Modern Software Development Lifecycle

## Software Development Methodologies

| | | | |
|---|---|---|---|
| *Use cases:* | *Practically any startup initiatives, when end users' early feedback is required.* | *Most of mid-sized projects in custom software development where business requirements cannot be confidently translated to detailed software requirements.* | *Large projects that are easy to divide into small functional parts and can be developed incrementally over each iteration.* |



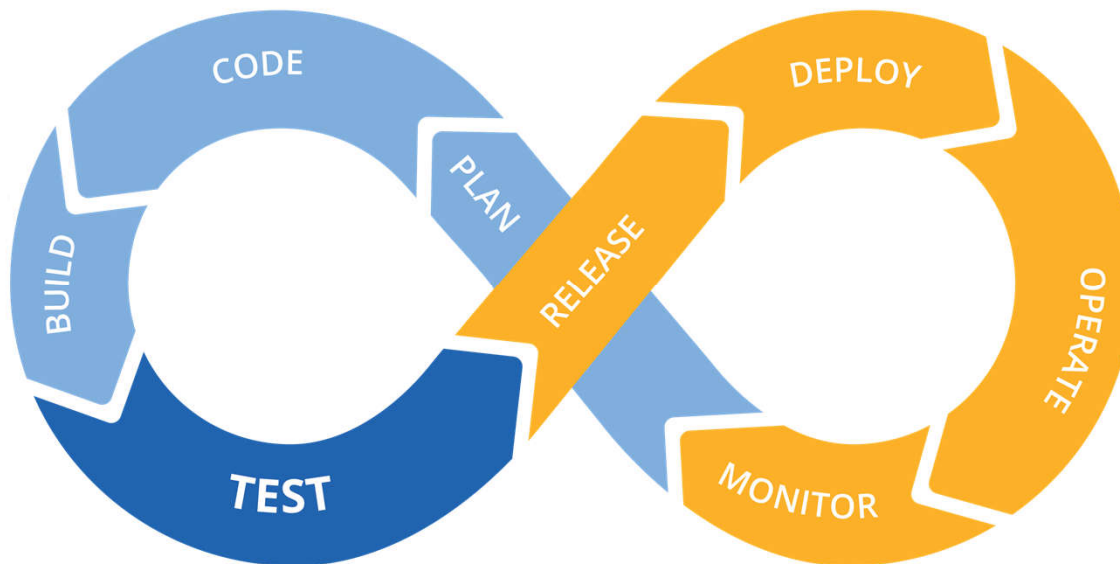| | | | |
|---|---|---|---|
| *Use cases:* | *Projects with unclear business needs or too ambitious/innovative requirements.* | *Projects that are large and complicated.* | *Research and development (R&D) activity or the introduction of a new service or a product.* |

# Developers and Operations were first to the Scene…

## DevOps



Developer

Operations

# Why was DevOps adopted?

**Top Objectives for Organization's DevOps Efforts at the Beginning**
Percentage of Respondents

| Objective | 1st Choice | 2nd | 3rd | 4th | 5th | Sum | Customer Very Satisfied (6,7) n = 139 | Customer Less Satisfied (1-5) n = 105 | Very Successful at Scaling DevOps (6,7) n = 136 | Less Successful at Scaling DevOps (1-5) n = 107 |
|---|---|---|---|---|---|---|---|---|---|---|
| Improving Agility | 15% | 12% | 14% | 10% | 8% | 59% | 63% | 54% | 62% | 55% |
| Improving Release/ Fewer Defects | 10% | 10% | 12% | 11% | 9% | 53% | 49% | 60% | 51% | 57% |
| Improving System Reliability | 12% | 11% | 10% | 8% | 11% | 52% | 51% | 56% | 50% | 56% |
| Reduction in Overall Waste | 11% | 9% | 10% | 10% | 10% | 51% | 54% | 46% | 58% | 40% |
| Cost Reduction | 10% | 12% | 12% | 9% | 7% | 49% | 42% | 56% | 40% | 57% |
| Fast Delivery of Customer Value | 9% | 14% | 11% | 7% | 7% | 48% | 47% | 47% | 43% | 45% |
| Improving User Experience | 8% | 7% | 10% | 11% | 12% | 47% | 50% | 46% | 51% | 47% |
| Maintaining Market Competitiveness | 5% | 10% | 7% | 8% | 10% | 41% | 45% | 37% | 42% | 42% |
| More Predicable Delivery of Customer Value | 9% | 8% | 7% | 7% | 7% | 38% | 40% | 37% | 38% | 40% |
| Improving IT Employee Job Satisfaction | 10% | 6% | 4% | 7% | 6% | 33% | 40% | 27% | 39% | 32% |
| No Definitive Goals Were Set | 0.37% | | | | | | 1% | - | 1% | 1% |

■ Statistical significant difference: 95%

n = 273
Q: What were the top objectives for your organization's DevOps efforts at the beginning? Summary of Top 5 Ranks (1-5)
Source: Gartner 2019 DevOps Survey
ID: 377293

# …and then Security appeared on the Scene
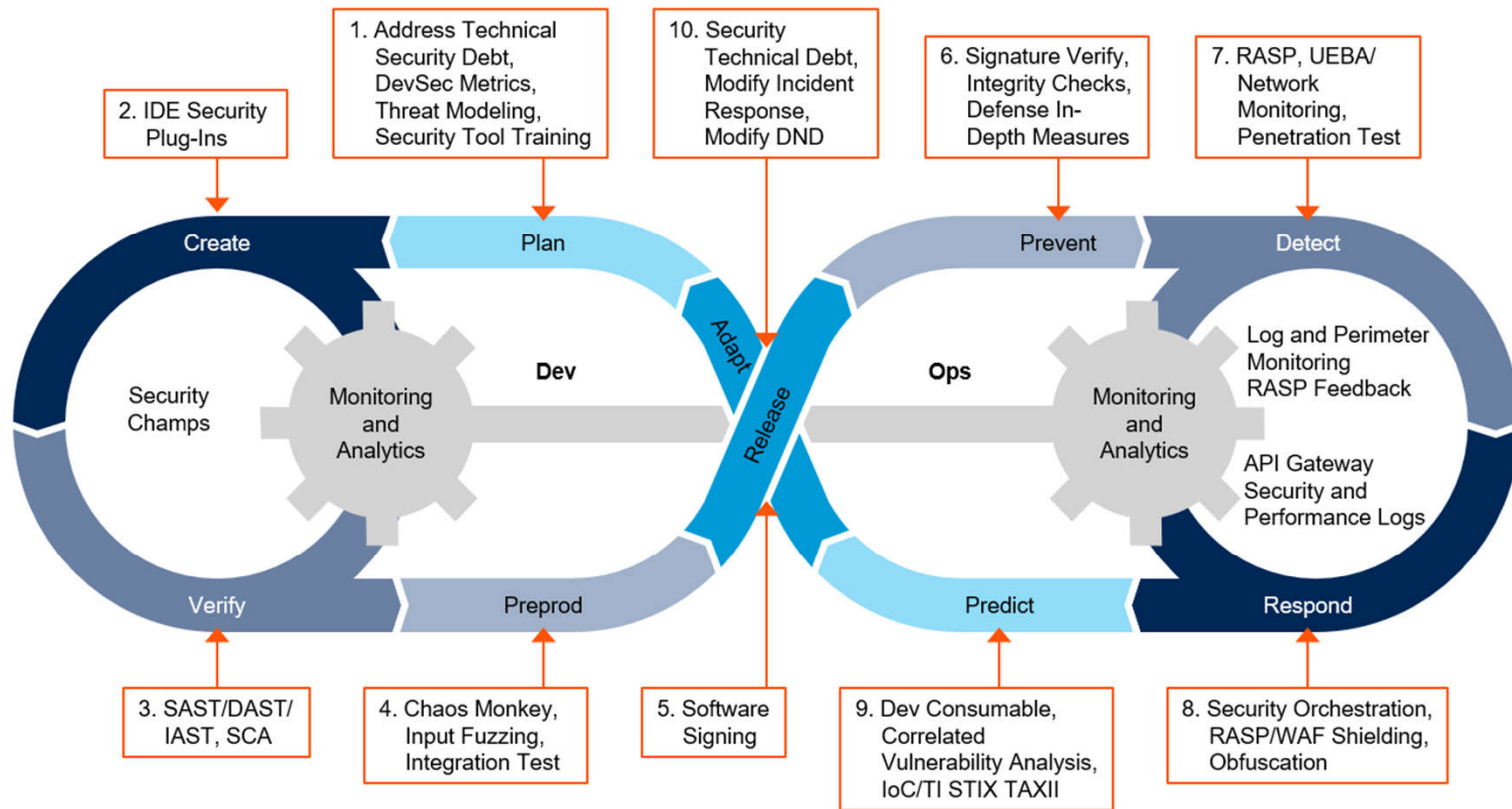
## DevSecOps

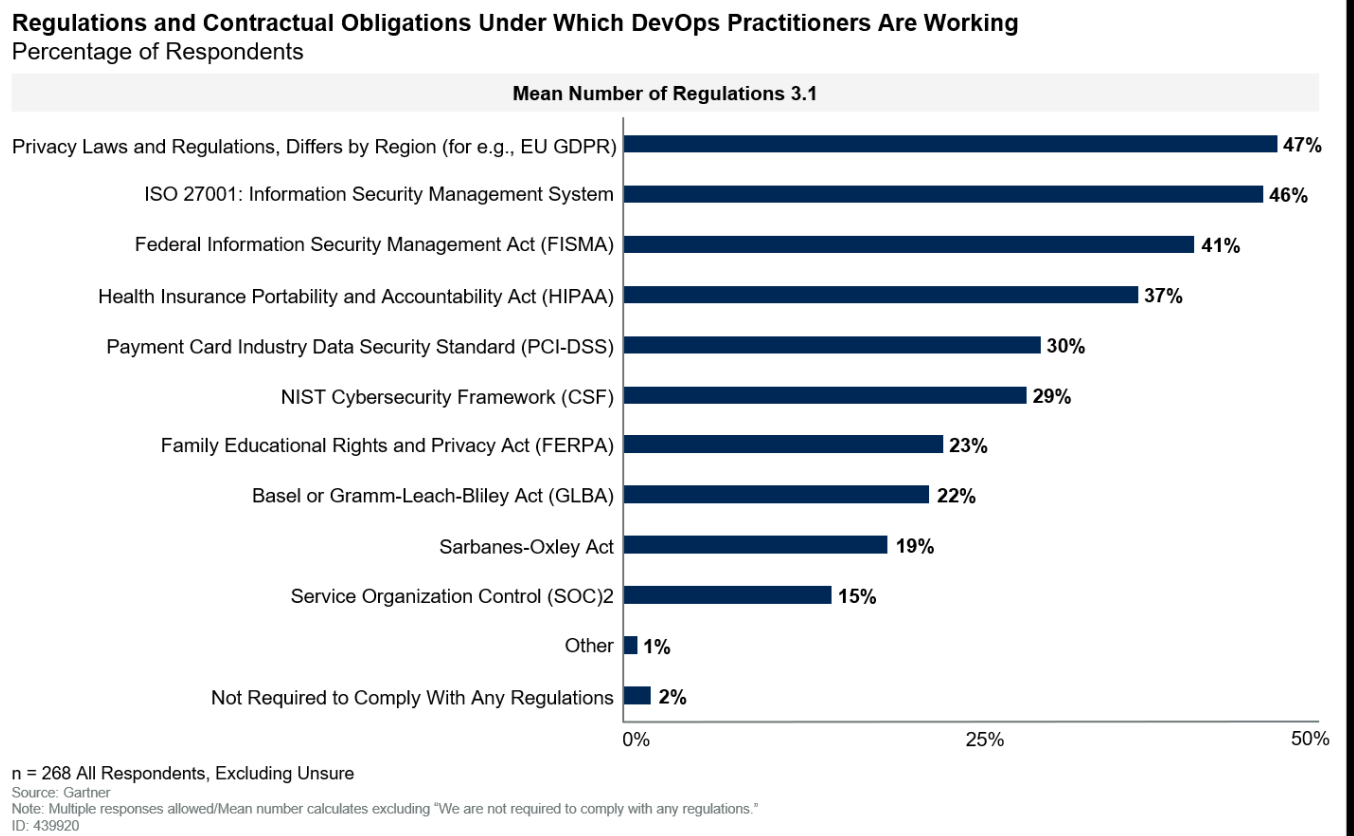Developer

Security

Operations

# DevSecOps Software Development Lifecycle



The DevSecOps Toolchain

Source: Gartner
ID: 377293

# Regulations and Contractual Obligations Under Which DevOps Practitioners Are Working



**Regulations and Contractual Obligations Under Which DevOps Practitioners Are Working**
Percentage of Respondents

**Mean Number of Regulations 3.1**

| Regulation | Percentage |
|---|---|
| Privacy Laws and Regulations, Differs by Region (for e.g., EU GDPR) | 47% |
| ISO 27001: Information Security Management System | 46% |
| Federal Information Security Management Act (FISMA) | 41% |
| Health Insurance Portability and Accountability Act (HIPAA) | 37% |
| Payment Card Industry Data Security Standard (PCI-DSS) | 30% |
| NIST Cybersecurity Framework (CSF) | 29% |
| Family Educational Rights and Privacy Act (FERPA) | 23% |
| Basel or Gramm-Leach-Bliley Act (GLBA) | 22% |
| Sarbanes-Oxley Act | 19% |
| Service Organization Control (SOC)2 | 15% |
| Other | 1% |
| Not Required to Comply With Any Regulations | 2% |

n = 268 All Respondents, Excluding Unsure
Source: Gartner
Note: Multiple responses allowed/Mean number calculates excluding "We are not required to comply with any regulations."
ID: 439920

# What Does it Mean to Mature in DevSecOps

◆ Finding the right balance and distribution of roles

◆ Successful integration of security controls and tools throughout the DevSecOps toolchain

◆ Use DevSecOps practices and automation to substitute traditional controls

◆ Validate and measure success of DevSecOps compliance efforts by continually monitoring status of compliance

◆ Scale compliance practices across the organization by leveraging compliance-specific software

Governance

People

Technology

Process
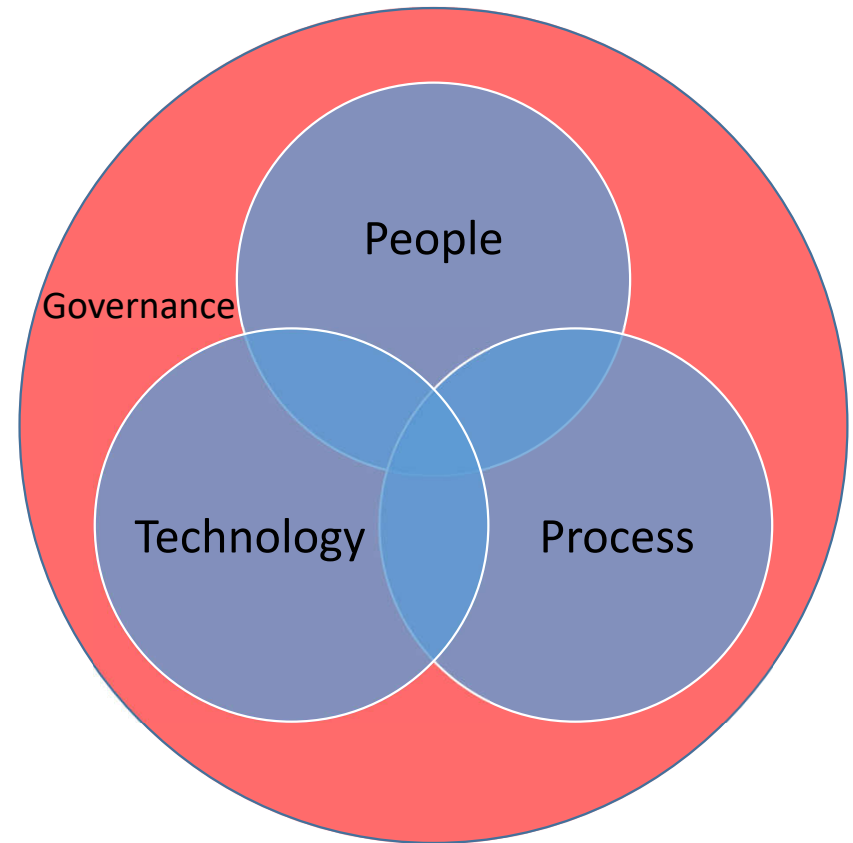
# How to Begin the Journey

◆ Understand "Why".  Make the Business justification!

◆ Assessment = Current State vs. Desired Future State

◆ Identify Gaps and Propose Solutions

◆ Build a Roadmap = Can't Do "IT" all at Once!

◆ Incremental Change over Time

◆ Start Now

– It will take 2 years whether you "Start Now" or start 2 years from now, so Start Now!
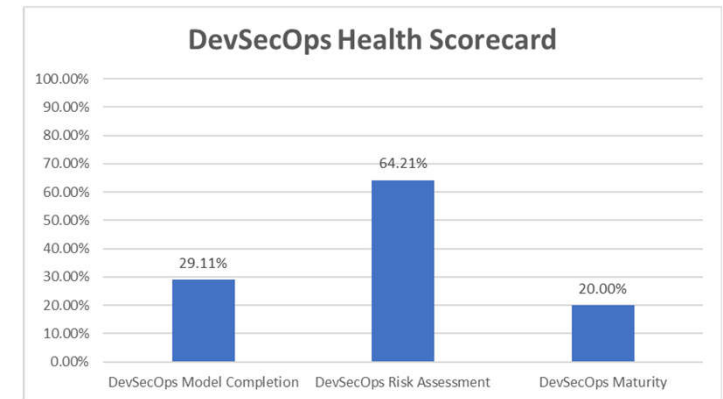
# What Does an Assessment Look Like
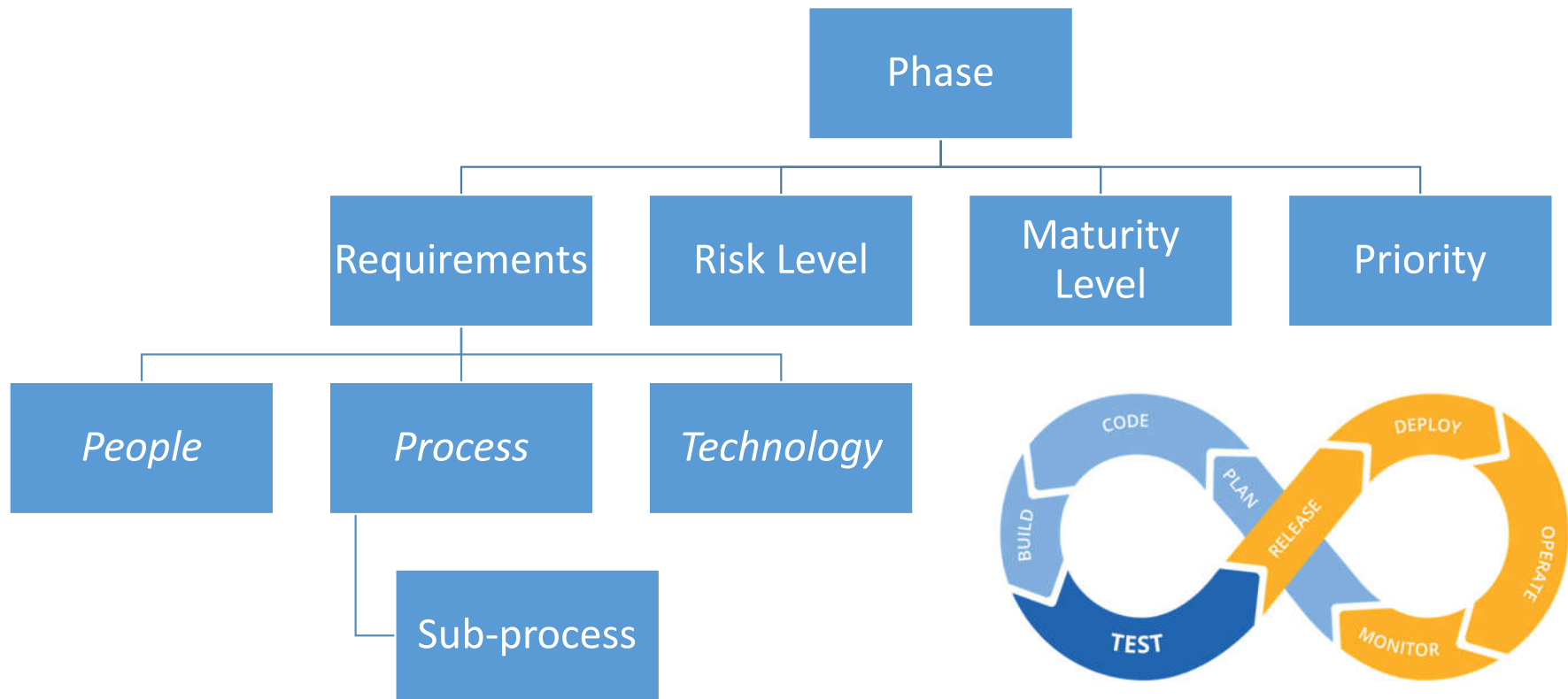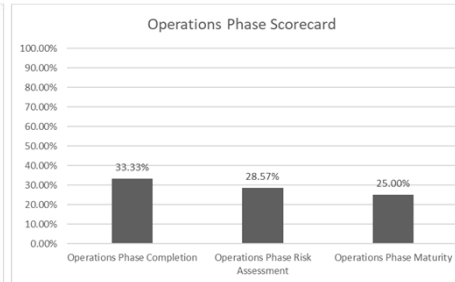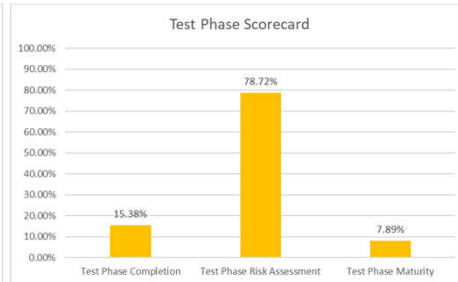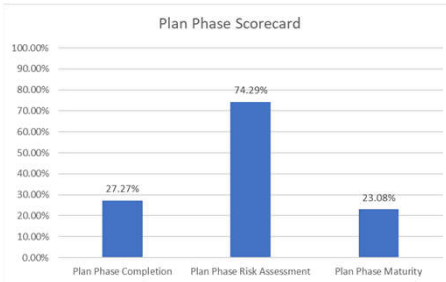
# Systematically Assess DevSecOps Maturity

| | | | DevSecOps Ecosystem Design | | | Type of Requiremnt (or Dependencies) | | | | | | | | | |
| ID | Phase | Requirements by Phase | Process | Sub Process | Process Yes(1)/No(0 | People | People Yes(1)/No(0 | Technology | Tech Yes(1)/No(0 | Cumulativ | Risk | Current Risk Factor | Maturity Level | Current Maturity | Priority |
|----|-------|----------------------|---------|-------------|---------------------|--------|--------------------|-----------|------------------|-----------|------|--------------------|----------------|------------------|----------|
| ID - 01 - 01 | Plan | Design DevSecOps process & workflows | DevSecOps Ecosystem Design | DevSecOps process flow chart; DevSecOps ecosystem tool selection; Deployment platform selection | 0 | Release Manager; Project Manager; DevOps Architect; DevOps Engineer; Software Architect; Automation Architect; Systems Engineer | 0 | Team collaboration tools | 0 | 0 | 3 | 3 | 1 | 0 | High |

◆ List phases

◆ List requirements for each phase

◆ List processes & sub-processes to satisfy the requirement

◆ List organization roles needed to satisfy the requirement

◆ List the technology needs to carry out the processes

◆ Assess strengths, weaknesses, and risks, then prioritize!

**DevSecOps Grading & Health Report**

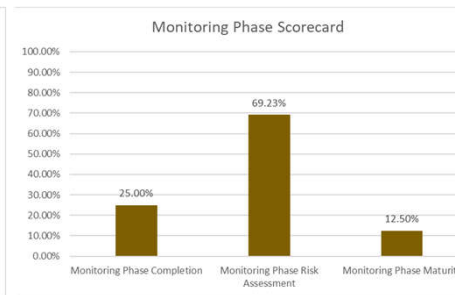| Category | Score Value | Score Completion |
|----------|-------------|------------------|
| DevSecOps Model Completion | 23/79 | 29.11% |
| DevSecOps Risk Assessment | 171/268 | 64.21% |
| DevSecOps Maturity | 39/192 | 20.00% |
| | | |

**DevSecOps Health Scorecard**

# Organization Self-Assessment



**Plan Phase Scorecard**
- Plan Phase Completion: 27.27%
- Plan Phase Risk Assessment: 74.29%
- Plan Phase Maturity: 23.08%

**Test Phase Scorecard**
- Test Phase Completion: 15.38%
- Test Phase Risk Assessment: 78.72%
- Test Phase Maturity: 7.89%

**Operations Phase Scorecard**
- Operations Phase Completion: 33.33%
- Operations Phase Risk Assessment: 28.57%
- Operations Phase Maturity: 25.00%

**Development Phase Scorecard**
- Development Phase Completion: 18.18%
- Development Phase Risk Assessment: 72.97%
- Development Phase Maturity: 7.41%

**Release Phase Scorecard**
- Release Phase Completion: 50.00%
- Release Phase Risk Management: 50.00%
- Release Phase Maturity: 37.50%

**Monitoring Phase Scorecard**
- Monitoring Phase Completion: 25.00%
- Monitoring Phase Risk Assessment: 69.23%
- Monitoring Phase Maturity: 12.50%

**Build Phase Scorecard**
- Build Phase Completion: 33.33%
- Build Phase Risk Assessment: 60.00%
- Build Phase Maturity: 30.00%

**Deployment Phase Scorecard**
- Deployment Phase Completion: 42.86%
- Deployment Phase Risk Management: 52.17%
- Deployment Phase Maturity: 19.05%

**Security Phase Scorecard**
- Security Phase Completion: 42.86%
- Security Phase Risk Assessment: 53.13%
- Security Phase Maturity: 31.82%

## DevSecOps Grading & Health Report

| Category | Score Value | Score Completion |
|---|---|---|
| DevSecOps Model Completion | 23/79 | 29.11% |
| DevSecOps Risk Assessment | 171/268 | 64.21% |
| DevSecOps Maturity | 39/192 | 20.00% |
| | | |

**DevSecOps Health Scorecard**
- DevSecOps Model Completion: 29.11%
- DevSecOps Risk Assessment: 64.21%
- DevSecOps Maturity: 20.00%

# What is Achieved Through a Mature DevSecOps Model

Improving team dynamics and cross-functionality

Compliance through automation

Effectively following business processes

Meaningfully implementing effective tools

Iterative reassessment and improvement

# Thank You!

800 Superior Ave E, Ste 1050
Cleveland, OH 44114

Phone: 216.255.3040
Fax: 216.274.9647

Email: info@asmgi.com

www.asmgi.com