DevOps Meets Security

Keith McMillan

CISSP, CCSP, SAFe Program Consultant, Certified Scrum Professional

Technology Strategist – Manager

Private Equity Value Creation

PricewaterhouseCoopers

Agenda

- Meet your Speaker
- What’s the Problem?
- What Won’t Work?
- What Does Work?
- Information Risk Program Structure
- Steps Before Deployment
- After-deployment Activities
- Q&A

Meet your Speaker

Keith McMillan

Technology Strategist - PwC Deals Practice - Private Equity Value Creation

30+ years architecture, development and deployment experience

Designed and deployed more than 100 mission-critical applications across multiple domains

Deep information risk and cybersecurity experience

(ISC)^2 Certified Information System Security Professional

(ISC)^2 Certified Cloud Security Professional

Scaled Agile Framework Program Consultant

Scrum Alliance Certified Professional ScrumMaster

A Quick Word on Terms

0

Defining “DevOps”

Because sometimes we need to

Combination of development and operational responsibility

Focused on the “Three Ways”

- Flow
- Feedback
- Continuous experimentation (Kaizen)

Complementary with agile and lean development

Defining "DevOps"

First Way: Flow

Remove silos and hand-offs

Make work visible

Limit WIP

Reduce batch size

Identify and reduce waste

Defining "DevOps"

Second Way: Feedback

Real-world experience best informs development

Fail-fast, swarm and collectively fix problems

Push quality left

Optimize for downstream workcenters – don't throw over the wall

Defining “DevOps”

Third Way: Learning and Optimizing

Mistakes are okay – learn from them

Institutionalize improvement of work

Transform local discoveries to global improvement

Inject resiliency

Senior leaders must reinforce

Defining "DevOps"

Tools play a part

Flow is enhanced by tools like CI/CD pipelines

Tools are not necessary, but are helpful

Having the tools doesn't mean you are doing DevOps

Defining “Agile”

“Agile project management” any approach that conforms to the Agile Manifesto and Principles

Empirical process

Focused on rapid, lightweight development

Involves business directly in project

Short development cycles

Responsive to change in requirements

Minimal required process and documentation

Frequently, but not necessarily Scrum, Kanban, SAFe

So what’s the problem?

1

The Old Way

Security and Development have had a strained relationship.

Traditional way:

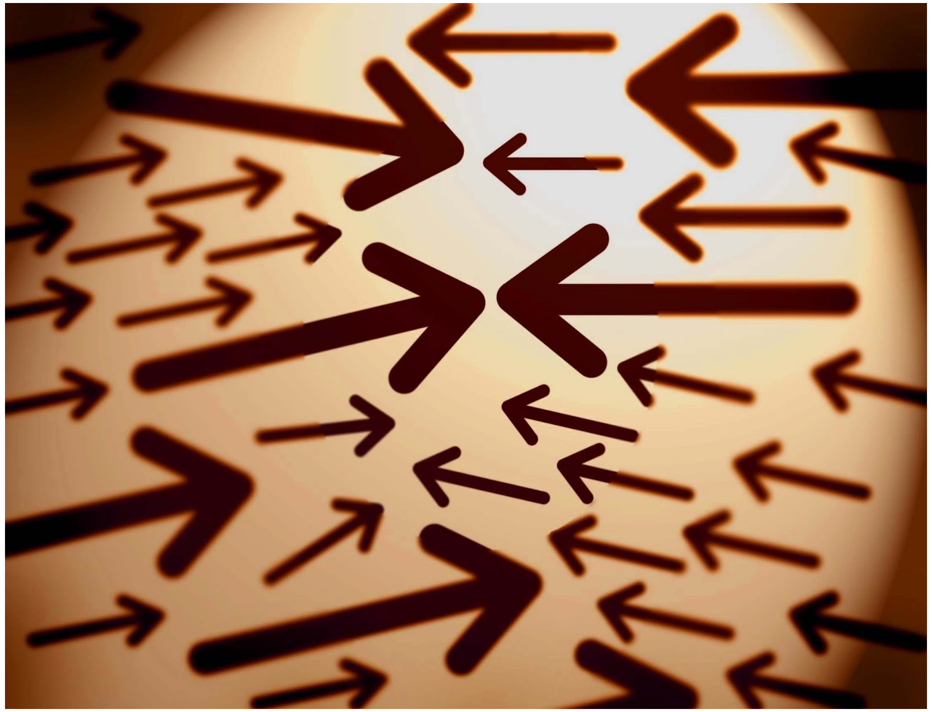
- Define security requirements up front
- Engage at the end to validates requirements, before deployment

BUT

Agile and DevOps requirements change quickly

Deployment to production is frequent and rapid

Both Teams Benefit the Enterprise



Information Risk and Cybersecurity

- Ensure regulatory compliance
- Minimize
  - Fines
  - Operational cost to restore service
  - Loss of business reputation
- Preserving data assets and availability
- Avoidance of jail
- Continuing operation of the business

Development / DevOps

- Rapid development of disruptive functionality
- Respond quickly to business and customer needs
- Pivot quickly to changes in the market and in response to learning
- Reduce development waste (YAGNI, Lean)
- Rapid, smooth and regular deployment to production

Different goals, different styles

Information Risk and Cybersecurity

- Cautious
- Formal
- Prescriptive
- Careful and thorough analysis
- Risk-averse

Development / DevOps

- Lightweight requirements and design
- Frequent deployment
- Quick feedback
- Rapid response to business environment change

We Need Both

What We Need

Security and risk considerations included in development / DevOps work

Development / DevOps needs the ability to quickly respond to change in the market or business needs

The organization needs up-to-date insight into security posture at a system, group and organizational level

What Won’t Work

Hire more security experts, embed them with the development teams

- Global shortfall of 3.4 million qualified workers[1]

Ignore the problem, hope the attackers go away

- 34% of executives polled by Deloitte reported being targets of cyber adversaries[2]
- Global unrest and state actors are more prevalent

Slow down development

Wait until the end to address security in systems

1. 2022 (ISC)² Cybersecurity Workforce Study
2. Forbes Cybersecurity Trends & Statistics For 2023; What You Need To Know

What Does Work

- Security requirements that meet corporate policies and regulatory needs
- Ability for development teams to find the requirements that apply to their project
- A catalog of off-the-shelf solutions that met those requirements
- A way to get approval to not meet requirements
- A formal approval to deploy
- Tracking and reporting

Before Deployment

2

Getting from Regulation to Requirements

Risk and Security Policy Hierarchy

- Policies state the organizations intent to meet legal and regulatory mandates. They define “what.” Regulatory policies map regulations to what the organization intends to do.
- Standards specify “how” the organization will implement the policy. They should be technology-agnostic.
- Guidelines provide guidance in meeting standards, such as when alternatives are available, or guidance on intent when in gray areas.
- Procedures are step-by-step instructions

Legal and Regulatory Influences

- SOX
- PCI-DSS
- CCPA and other state privacy laws
- SEC rules
- US-EU Transatlantic Data Privacy Framework
- GDPR
- NYDFS 500 and revisions

Organizational Policies

- Access Policy
- Data Security Policy
- Password Policy
- Data Retention Policy
- Acceptable Use

Standards

- Encryption standard
- PII access standard
- Configuration Control standard
- Alternate Processing Site standard
- Login ID standard

Guidelines

- Evaluating encryption alternatives for PII
- Code review guidelines

Procedures

- ID provisioning
- Enabling row-level encryption
- Release promotion procedure

Not All Standards Apply All the Time

Standard Baselines and Profiles

- Depending on characteristics and use, standards may not apply to some systems
- Profiles and baselines create overlapping subsets of the standards
- Profiles are mix-and-match, and are finer grained than baselines
- Profiles and baselines should exist independently of any particular system

Baselines

- Application server security baseline
- Cloud deployment security baseline
- Accounting baseline

Profiles

- Publicly accessible
- Supports individual logins
- Handles financial transactions
- Handles PII / PHI
- Security Categorization

Assessing Systems

3

Self-Service! ⇩

What Do We Have to Do?

Applying Standard Baselines and Profiles

- Developers and system owners identify which baselines and profiles apply
- Profiles and baselines “pull in” standards that apply to this system
- System requirements are a union of all standards for all applicable profiles and baselines

Baselines

- Application server security baseline
- Cloud deployment security baseline
- Accounting baseline

Profiles

- Publicly accessible
- Supports individual logins
- Handles financial transactions
- Handles PII / PHI
- Security Categorization

Self-Service! ⇩

“How Do We Do That?”

Catalog of Known Solutions

Once we know what we have to accomplish, how do we do it?

Readily accessible catalog of preferred solutions to meet standards

- Technology-specific
- Common controls
- How-to instructions
- Guides
- Degree of standard support is known

Need to be accessible, linked to standards, and self-service

Self-Service! ⇩

What if We Can't?

Findings, or deviations from standards, are common

- Common control is unavailable
- Preferred technology is not what's being used
- Business demands delay implementation
- Functionality unavailable in vendor-provided solution

Deviations can be temporary or permanent

Full-Service! ⇩

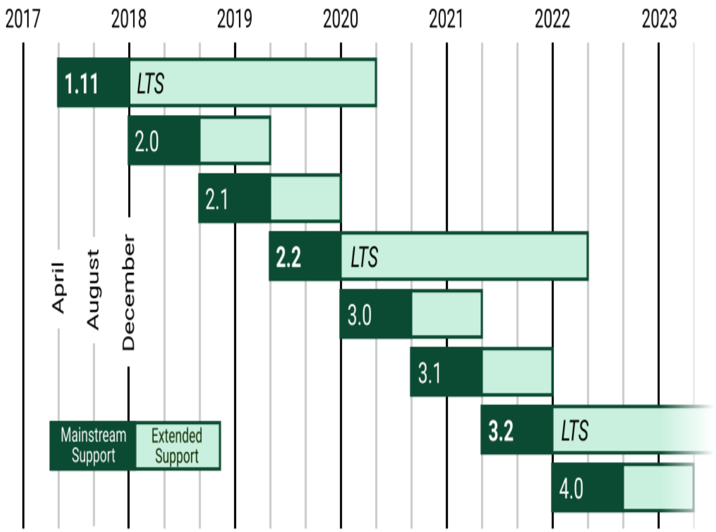
Self-Service! ⇩

We Can't Right Now

<u>Remediation Plans</u> document how systems will (eventually) remedy the deviation

- Request, assessment and grant process should be clear
- Approval should be formal and have a defined SLA
- Should include dates for when remediation will be complete
- Need to be reviewed when due date arrives
- Should be tracked

Mature organizations may be able to automatically grant remediation plan approval



Full-Service! ⇩

We Can't Ever

Exceptions document long-term allowed deviations

- Exception request, assessment and grant process should be clear
- Review and approval authority should be formal
- Exceptions management should track and report
- Exceptions are periodically reviewed

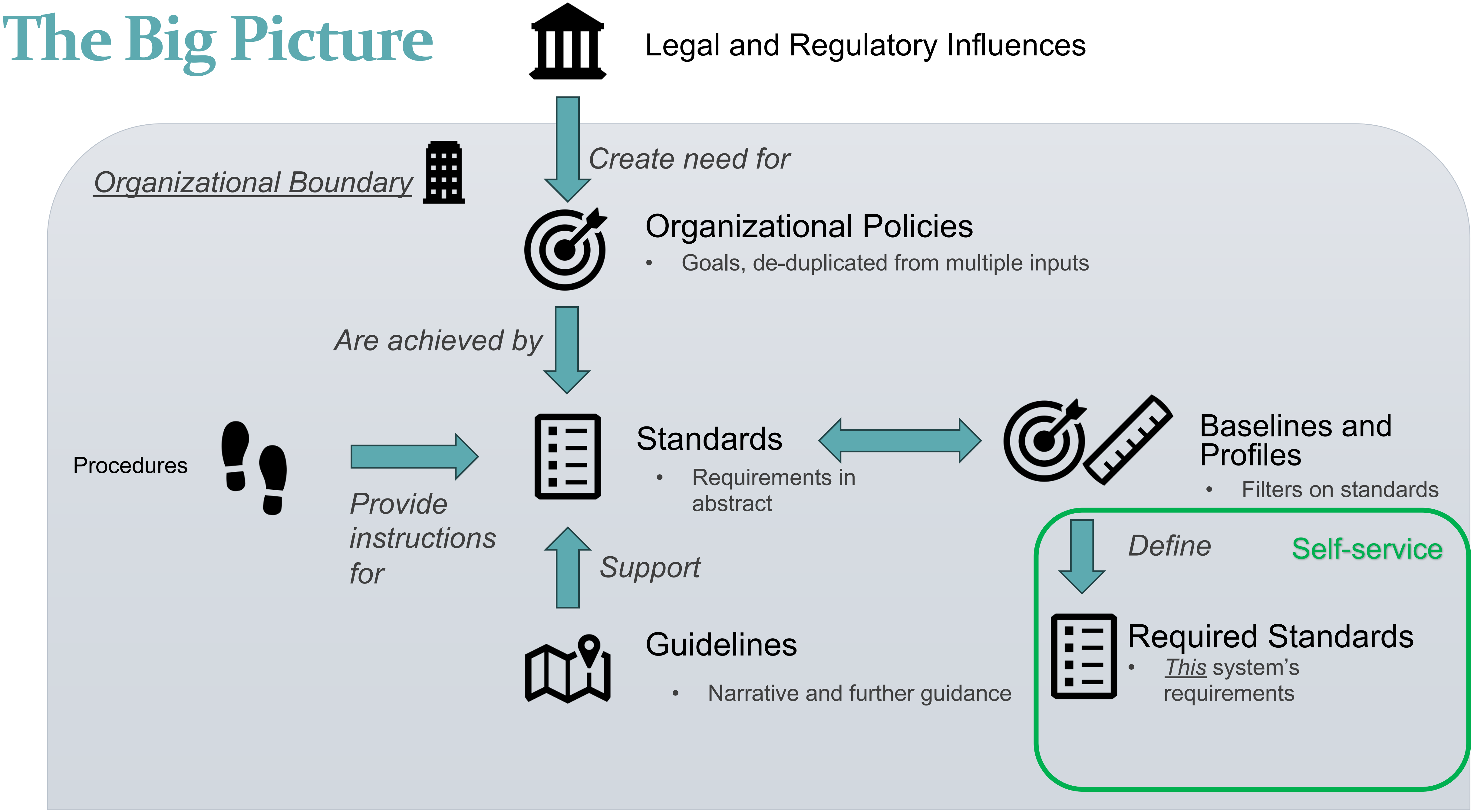
This Photo by Unknown Author is licensed under CC BY-SA

Tracking Findings

Findings management process should be formal

- Track existence
- Report
- Manage review and updates

The Big Picture



Legal and Regulatory Influences

Create need for

Organizational Boundary

Organizational Policies

- Goals, de-duplicated from multiple inputs

Are achieved by

Standards

- Requirements in abstract

Baselines and Profiles

- Filters on standards

Procedures

Provide instructions for

Support

Guidelines

- Narrative and further guidance

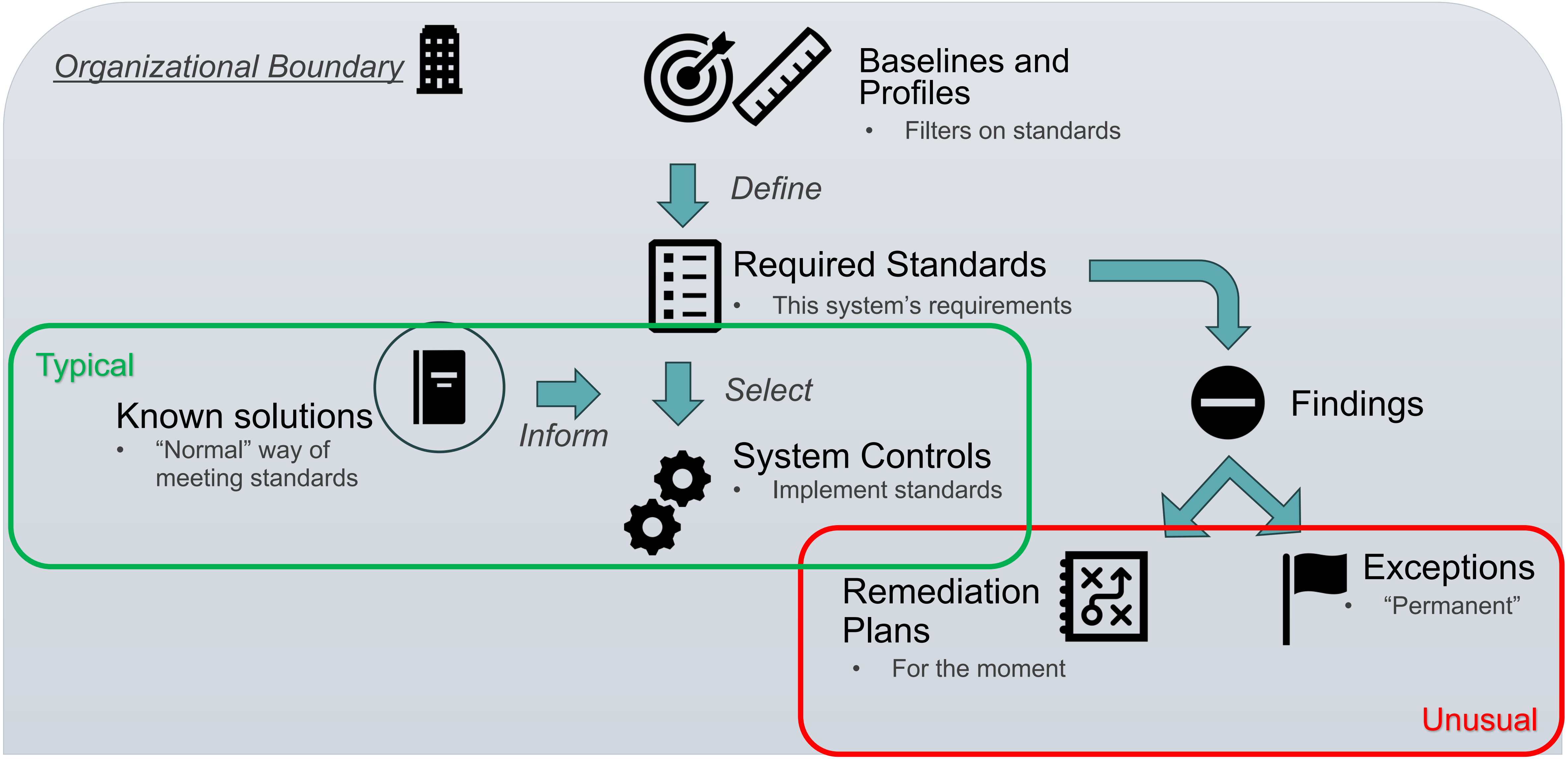
Self-service

Define

Required Standards

- *This* system’s requirements

The Big Picture



Organizational Boundary

Baselines and Profiles

- Filters on standards

Define

Required Standards

- This system's requirements

Typical

Known solutions

- "Normal" way of meeting standards

Inform

Select

System Controls

- Implement standards

Findings

Remediation Plans

- For the moment

Exceptions

- "Permanent"

Unusual

Decision

How Secure is Enough?

Approval to use the system

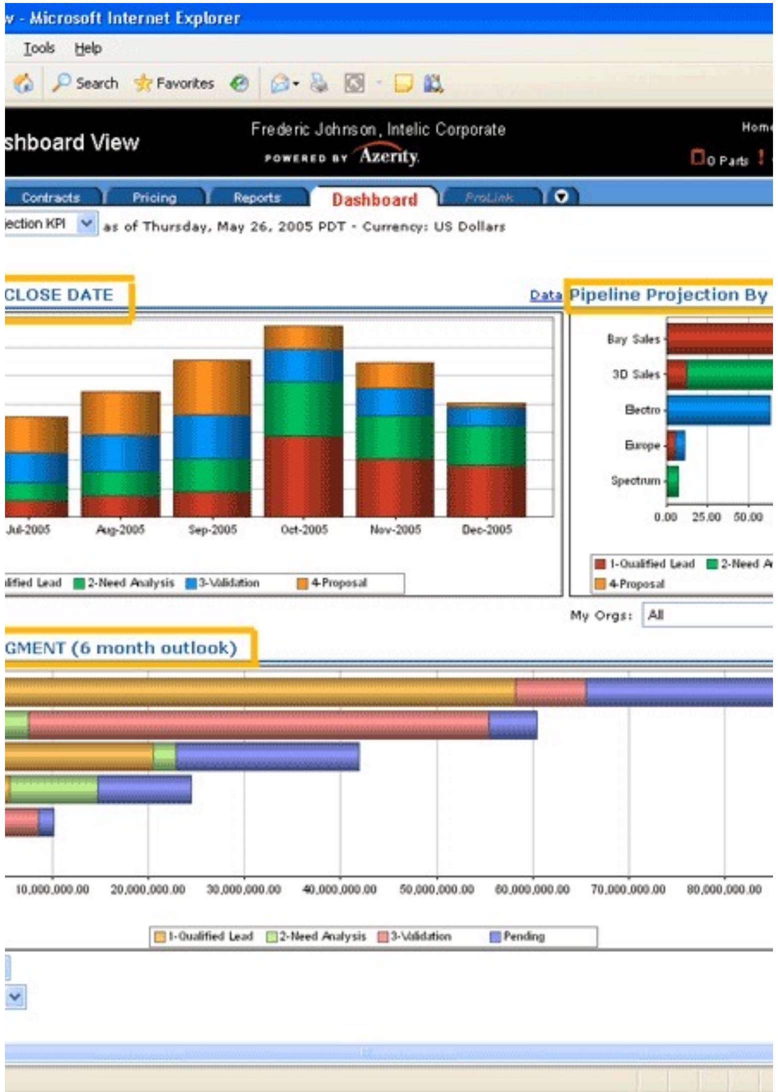
- ATO process allows application deployment and operation in production
- Requires assessing overall security
  - Findings
    - Exceptions
    - Remediation plans
  - Controls
- Step-back, view the big picture
  - Address death by a thousand cuts
  - Findings may be owned by different standard owners

Authorization to Operate

- Formal approval
- Should incorporate security
  - Integrate with findings management
- Security role may be advisory or compulsory
  - Depends on organizational paradigm
- May be conditional
- Should be re-reviewed

After Deployment

4



This Photo by Unknown Author is licensed under CC BY

Tracking

If periodic reassessment is in scope (and it should be) an Authorization to Operate management system is advised

Findings management is required to manage exceptions and remediation plans

- Existence
- Workflow

Findings management reporting informs multiple insights

- Individual system security
- Organizational unit system security
- Organizational compliance overall
- Quality of standards
- Areas for investment

Findings management systems are strongly encouraged

Tips and Guidance

5

Tips and Guidance

Making it work more smoothly

- ✓ Focus on as much self-service as you can enable
- ✓ Findings management tools are highly encouraged
- ✓ Deprioritize evaluation run-of-the-mill control implementations
- ✓ Develop a security categorization scheme, it informs both standards and processes in the risk program

Tips and Guidance

Making it work more smoothly

- ✓ Embed security into your build/deploy process through SAST tools
- ✓ Build your solutions catalog
- ✓ Establish points of contact for standards (owners or their delegates) to clarify and explain standards
- ✓ When first setting up ATO, focus on highest security category systems

Thank You!