Compliance is Regulatory

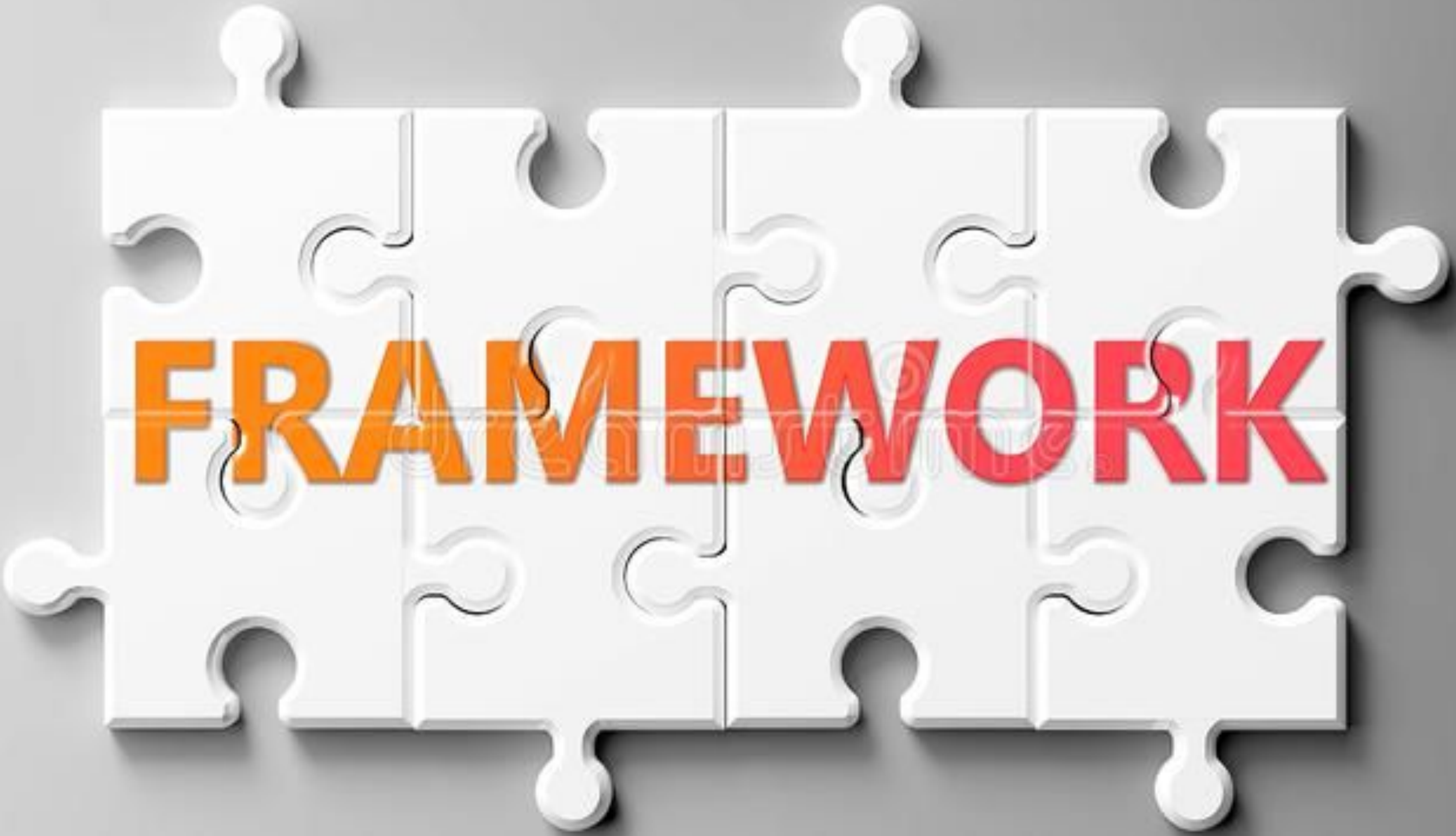
Protecting The Business And Helping Yourself

About

apporima.com

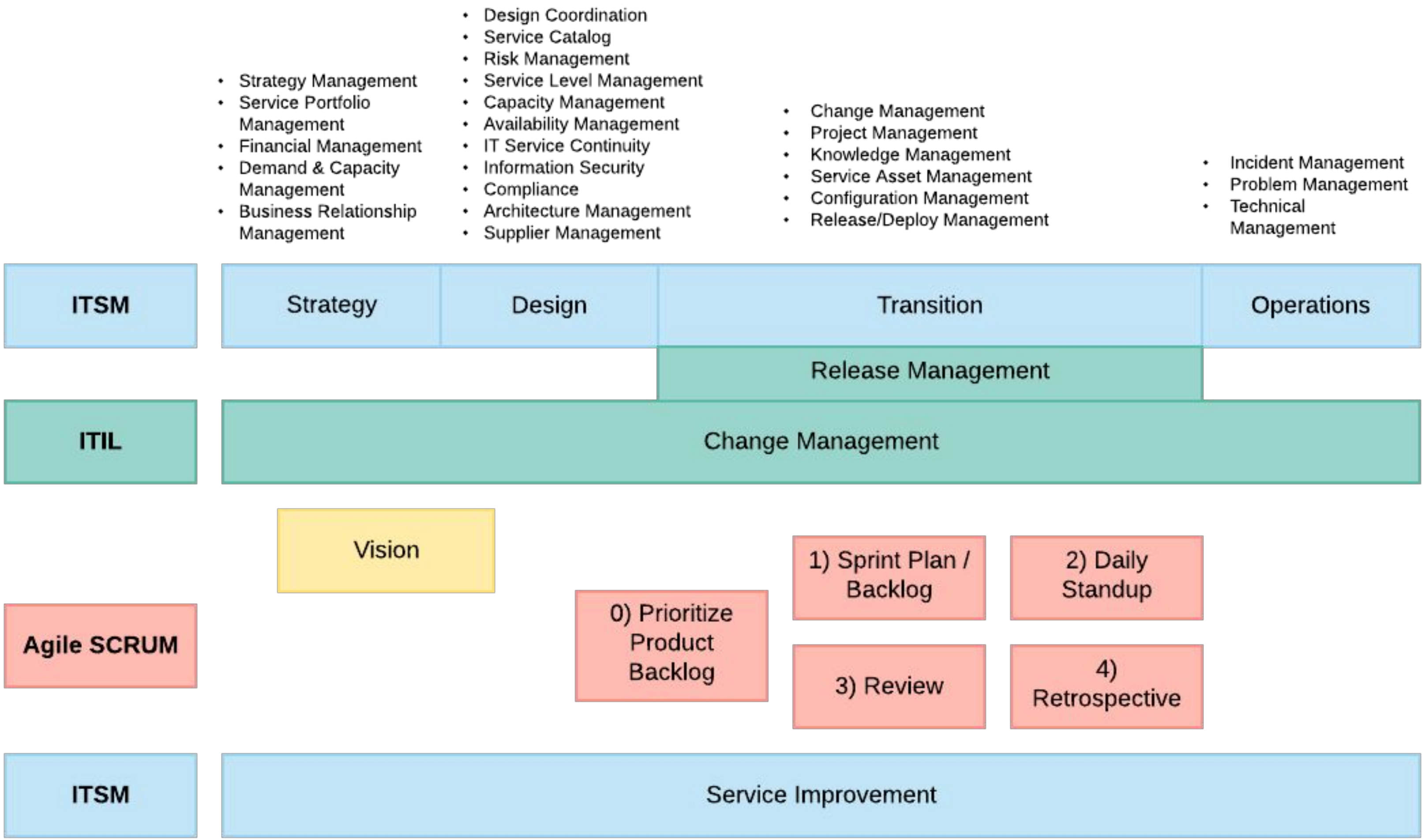
- Solution Architect @ Red Hat
- Conference organizer, lead
- Security & Compliance Weekly
- *97 Things Every Information Security Professional Should Know: Collective Wisdom from the Experts*

@apporima


FRAMEWORK

Frameworks

- Information Technology Service Management (ITSM)
- Information Technology Infrastructure Library (ITIL)
- Agile Methodology (13 frameworks)
- Scaled Agile Framework (SAFe)
- Risk Management Framework (RMF)
- Cybersecurity Framework (CSF)
- Privacy Framework
- Workforce Framework for Cybersecurity (NICE Framework)



- Strategy Management
- Service Portfolio Management
- Financial Management
- Demand & Capacity Management
- Business Relationship Management

- Design Coordination
- Service Catalog
- Risk Management
- Service Level Management
- Capacity Management
- Availability Management
- IT Service Continuity
- Information Security
- Compliance
- Architecture Management
- Supplier Management

- Change Management
- Project Management
- Knowledge Management
- Service Asset Management
- Configuration Management
- Release/Deploy Management

- Incident Management
- Problem Management
- Technical Management

ITSM Strategy | Design | Transition | Operations

Release Management

ITIL Change Management

Vision

Agile SCRUM

0) Prioritize Product Backlog

1) Sprint Plan / Backlog

2) Daily Standup

3) Review

4) Retrospective

ITSM Service Improvement

Why does this matter?

Sleeping Positions
CEO
CFO
COO
CISO

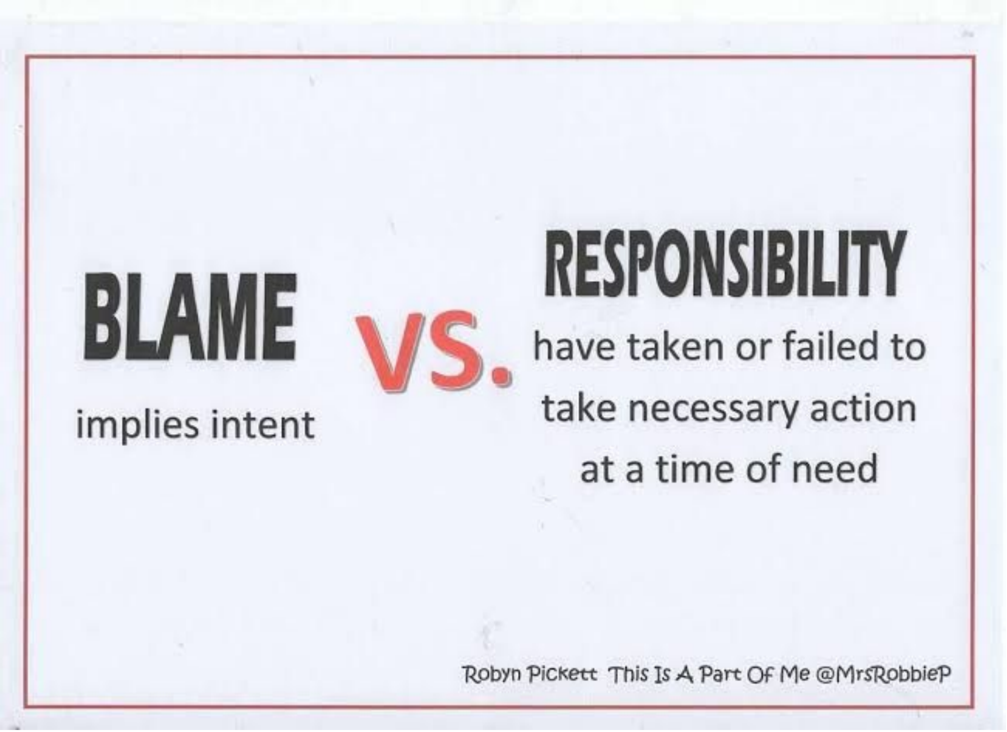
@apporima

What is the problem?

- Fiefdoms in business
- Not working together, or withholding support
- Startup: fill responsibility gaps with many hats
- Services aren’t delivered quickly enough
- Services delivered too quickly – with bugs
- Many more...

Responsibility Shift

- Asset Management
- Patch Management
- Education & Awareness
- Development testing



BLAME

implies intent

VS.

RESPONSIBILITY

have taken or failed to take necessary action at a time of need

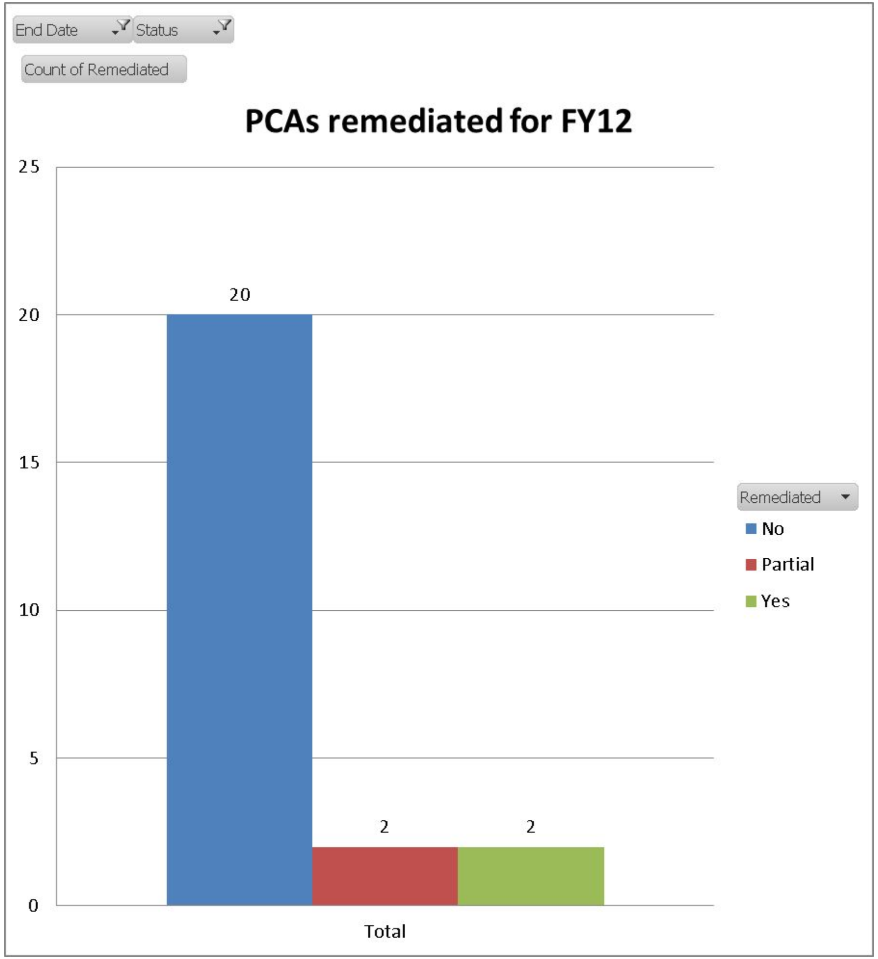
Robyn Pickett This Is A Part Of Me @MrsRobbieP

Audits versus Assessments

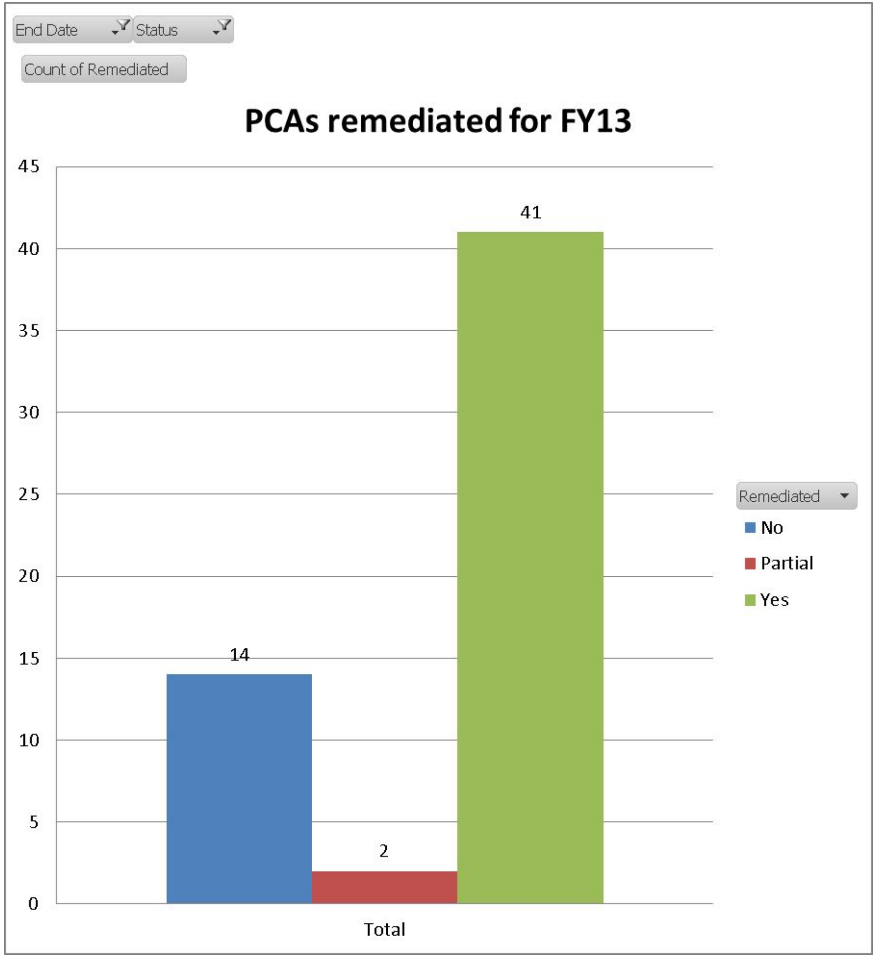
Audit – *Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures.*

Assessment – *The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact.*

csrc.nist.gov/glossary



PCAs remediated for FY12



PCAs remediated for FY13

Conclusion

- Understand how the organization functions
- Understand how the business makes money!
- Break down fiefdoms by proposing resolutions
- Seize the opportunities to help one another
- Voice concerns or changes that you need help raising to management
- Metrics, metrics, metrics. Collect metrics.

apporima.com

@apporima