Total Enterprise Assurance: A Practical Guide

By: Benjamin Tomhave, MS, CISSP

CIScon 2009 Post-Session

A Few Requests

- Phones: silent/vibrate + calls outside
- Breaks (yes, please!)
- Please ask lots of questions!!

Instructor Background

- ~15 years security experience
- A mile wide, a mile deep
- MS InfoSec Mgmt (GWU in DC)
- Risk, Architecture, Compliance, Solutions, Policies, Etc.

ARE YOU READY?

Introduction

- Course Objectives
- Agenda
- Key Definitions

Course Objectives

- Baseline Key Concepts
- Challenge Conventional Thinking
- Provide an Actionable Roadmap
- Motivate You to Adapt to Succeed

Agenda

Morning

- Introduction
- Survivability
- Risk Mgmt. Fail
- TEAM for Success
- Policy Framework

Afternoon

- Info. Risk Mgmt.
- Info. Sec. Mgmt.
- Q&P Mgmt.
- Putting it Together
- Advanced Topics

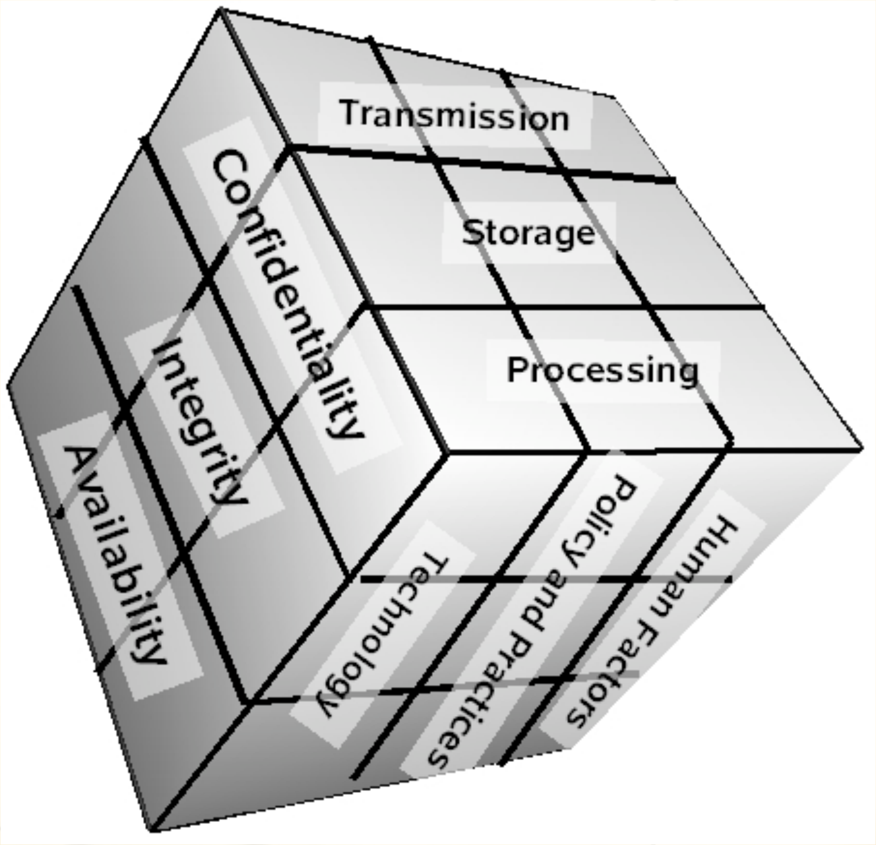
Key Definitions

- Why “Assurance Management”?
- Risk = loss or probability of loss
- Threats, Vulnerabilities, Countermeasures, Controls, Safeguards

Key Definitions

- Confidentiality, Integrity, Availability
- People (Human Factors), Processes (Policies and Practices), Technology
- Information States (S, T, P)

The McCumber Cube



Survivability

- What is it?
- What does it mean in practical terms?
- How does it apply to assurance mgmt?
- Defensibility & Recoverability

What Is Survivability?

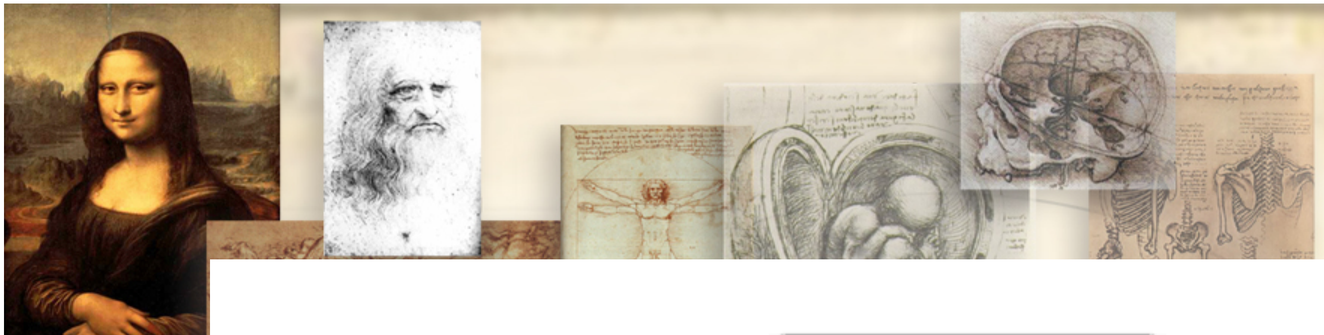
- Fault tolerance
- Performing Despite Degradation
- Not Just Availability or Reliability
- Defensibility & Recoverability

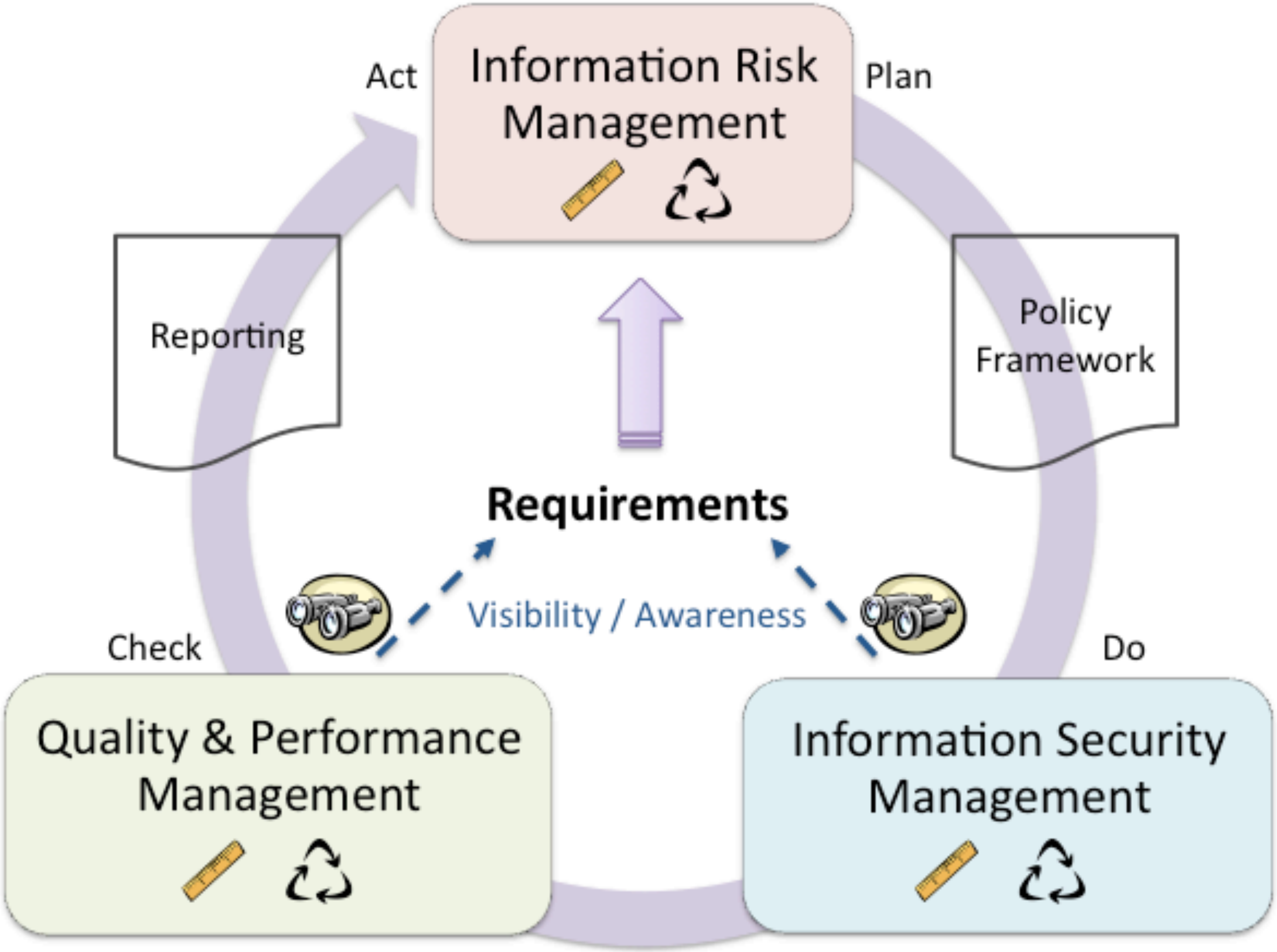
Meaning What, Practically?

- Not *if*, but *when* bad things happen…
- We cannot win the current war
- Changing the rules
- Ties into compliance and law

Survivability + Assurance = ?

- Wait, hold up – assurance mgmt wha?
- We’ll talk about TEAM in a bit, but…





Information Risk Management

Act

Plan

Reporting

Policy Framework

Requirements

Visibility / Awareness

Check

Do

Quality & Performance Management

Information Security Management

Survivability + Assurance = ?

- Ok, so… how do they work together?
- It’s about building-in fault tolerance…
- It’s about a defensible position…
- It’s about recoverability…

Defensibility

- The Defense-in-Depth myth…
  - Pete Herzog's Möbius Defense
- Legal Angle
  - Due diligence & reasonable care
- Beyond “best practices”

Source: http://www.dilbert.com/strips/comic/2008-09-03/

BEST PRACTICES ARE MEDIOCRITY!

Defensibility

- Plan for failure…
- Accept operating with degradation…
- Ties into risk tolerance – elasticity!

Recoverability

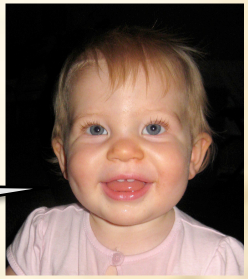
- What good is elasticity without recovery?
- Who ya gonna call?
- Incident Response = Biz Continuity!

Recoverability

- Compartmentalization?
- Data encryption & key management?
- Remote wipe for mobile devices?
- Logging & monitoring

Defensibility & Recoverability

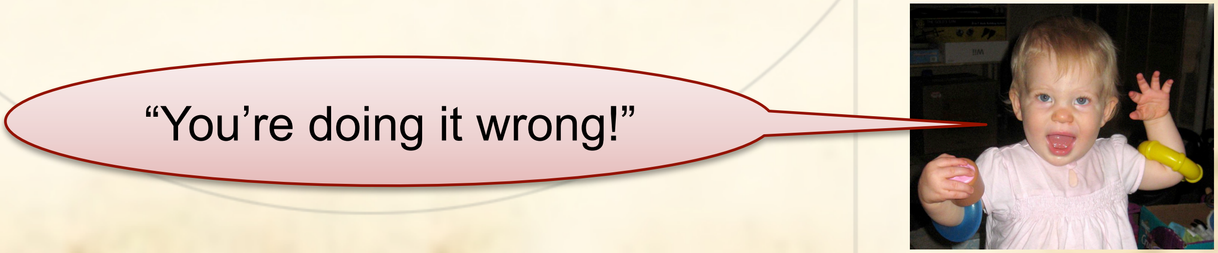
“The objective is clear:
Identify what’s important and then model threats against those things to build contingency plans.”



SHORT BREAK!

Risk Management Fail

- Need for visibility, transparency, & honesty
- Focus on survivability



What about…?

- Do you have visibility?
- What about transparency?
- How about honesty?
  - Can you trust what you’re told?
  - How do you know?

Surviving Risk

- As we already discussed… elasticity!
- But, here’s the thing…
  - Is your risk data good?
  - Beware GIGO!

You’re Doing it Wrong

- You assessed, you remediated, what?
- Did you model?
  - Huh?
- Did you analyze?
  - Metrics? What are those?

We’ll Come Back to Risk…

- For now, chew on this…
  - You’re probably being lied to today.
    - ((No, not by me.))
  - You’re probably not truly “managing” risk.

So, Now What?

- Survivability is cool, but…
- I thought I was doing RM, but…
- Surely there must be a another way…
  - ((Please don’t call me Shirley.))
    - ((Shirley is my mother-in-law… TMI!))

TEAM for Success!

- Total Enterprise Assurance Management Model v2
- Using Business Requirements to drive Assurance Management

A Brief History of TEAM

- Published in 2006
- Masters’ Thesis at GWU
- v2 Released in 2009
- Why should you care / adopt?

Quick Selling Points

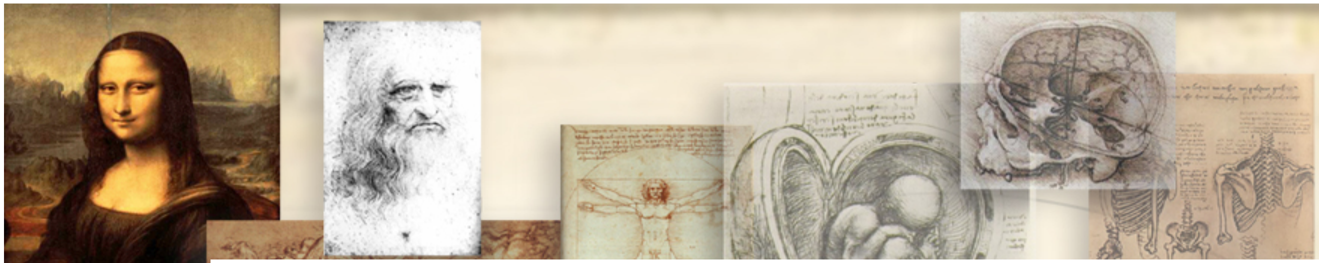
- Mostly just common sense…
- De-conflicts silos
  - A seat for everyone at the table
- Allows embedding best-fit methods

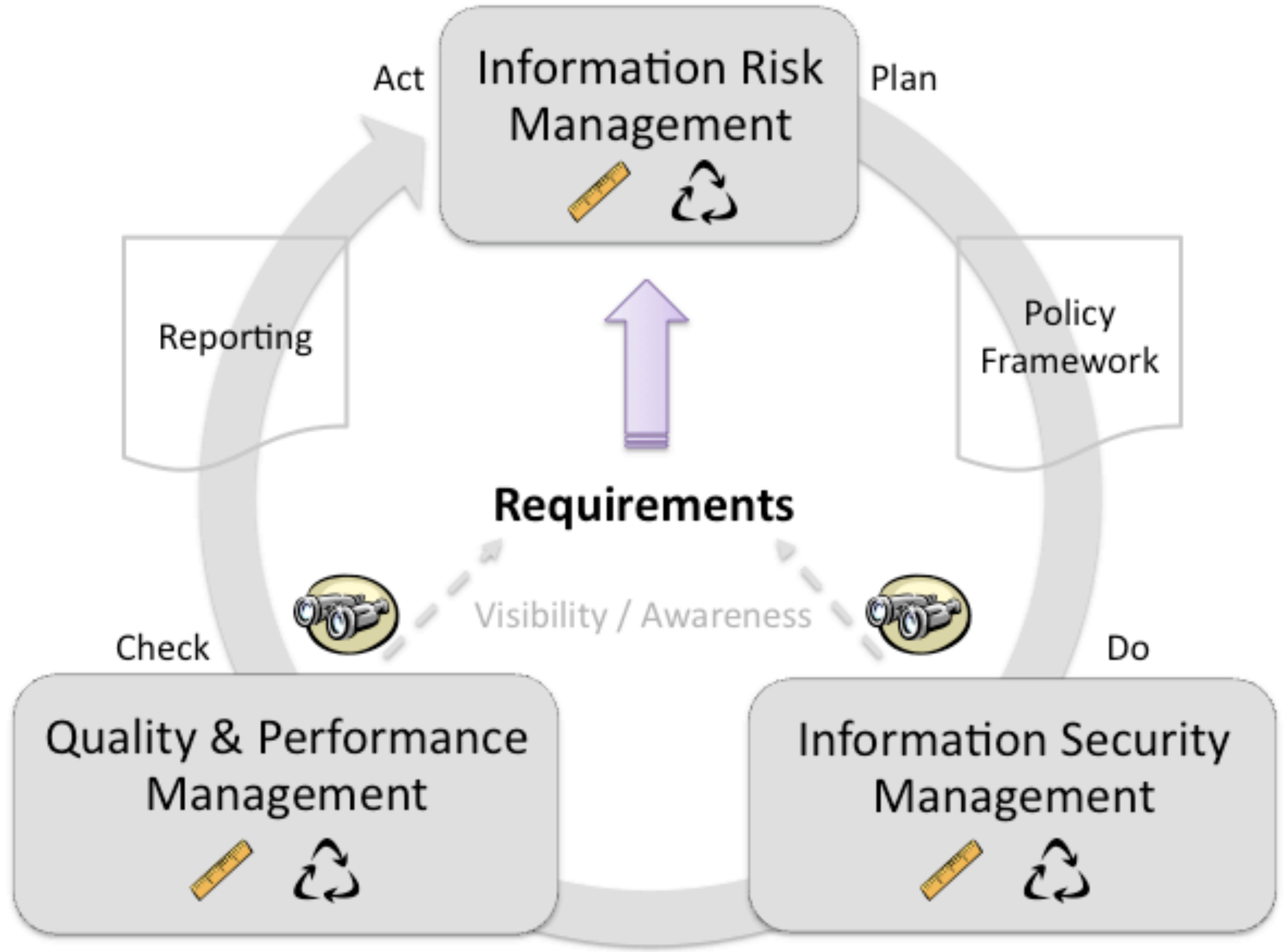
TEAM Model v2

- Information Risk Management
- Security Policies
- Information Security Management
- Quality & Performance Management
- Thin Grey Line of Auditor Independence

So, Let’s Talk About…

- Business Requirements…
- Then, TEAM Model from 50k feet…
- Then, A Short Break…
- Then, the Policy Framework…
- Then, Lunch…



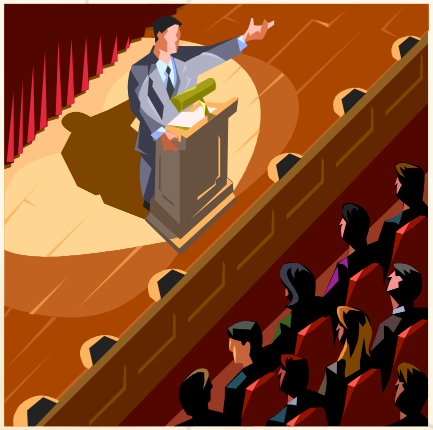

Act
Information Risk Management
Plan
Reporting
Policy Framework
Requirements
Visibility / Awareness
Check
Do
Quality & Performance Management
Information Security Management

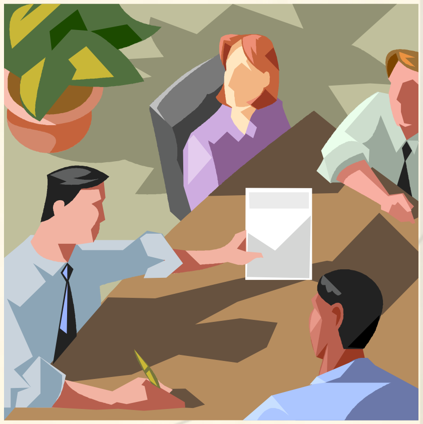
Business Requirements

- What's important to the business?
  - How do you know?
- What metrics do you use for success?
  - Have you defined "success"?
  - Is it achievable?

Collaboration = Leadership

- Which is your organization?





Who Knows What?

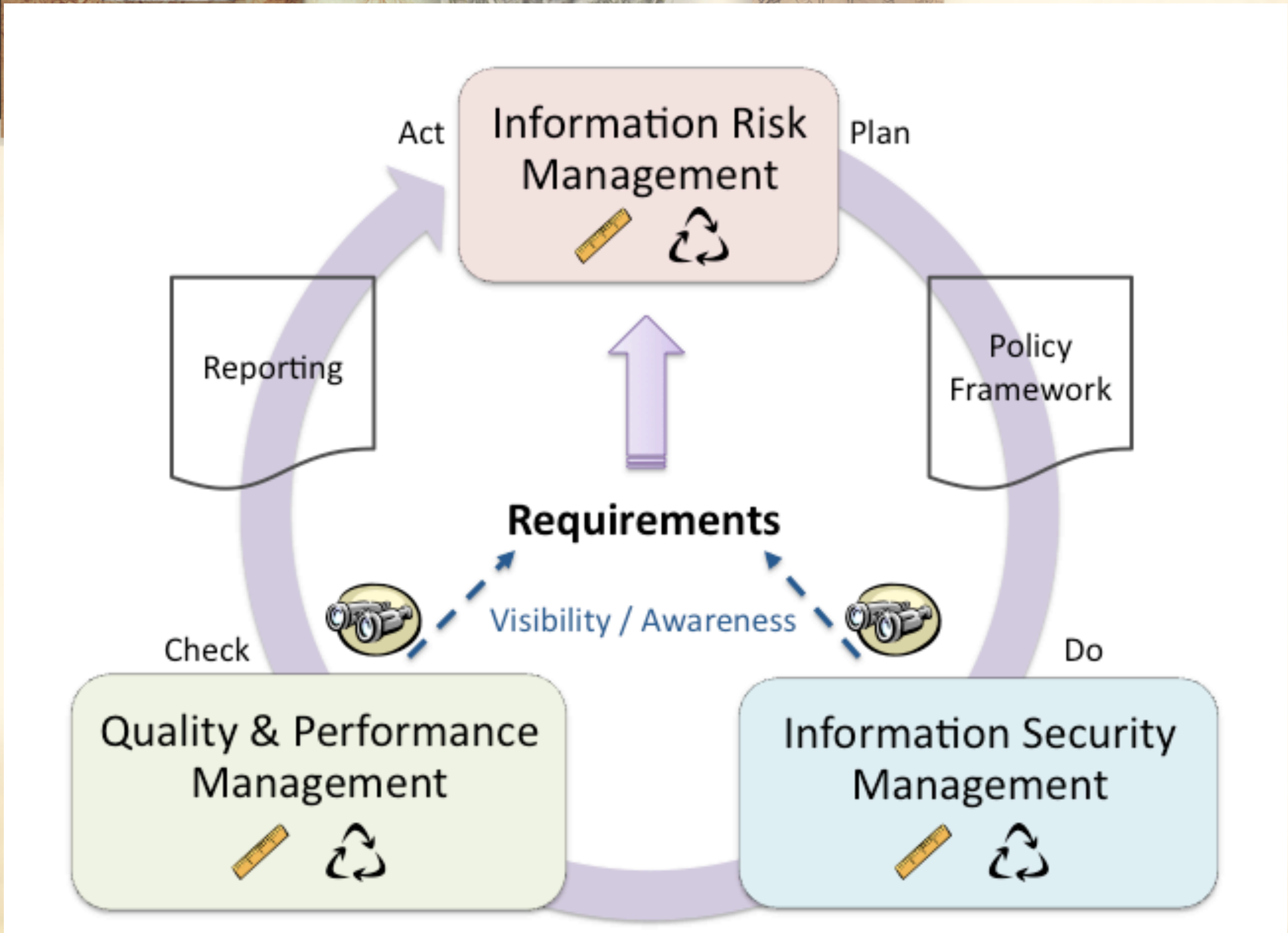
- Does your business have well-defined objectives or mission?
- Is everybody on-board?
- Requirements *should* drive much…

Back to the TEAM Model…

- What was it again?
  - Total Enterprise Assurance Management
  - Masters’ Thesis circa 2006
  - Revised Summer 2009

TEAM Model v2

- Information Risk Management
- Security Policies
- Information Security Management
- Quality & Performance Management
- Thin Grey Line of Auditor Independence


Act
Information Risk Management
Plan
Reporting
Policy Framework
Requirements
Visibility / Awareness
Check
Do
Quality & Performance Management
Information Security Management

Plan-Do-Check-Act

- AKA “The Deming Cycle”
  - Google “W. Edwards Deming”
- http://en.wikipedia.org/wiki/PDCA
- Basis of many ISO Standards

Plan

- Establish objectives and processes
- Targeted toward expected results
- Key: Completeness & Accuracy
- Spend time on thorough designs

Do

- Implement the process(es)
- Limit scale (if possible)
- It’s just that simple…

Check (or Study)

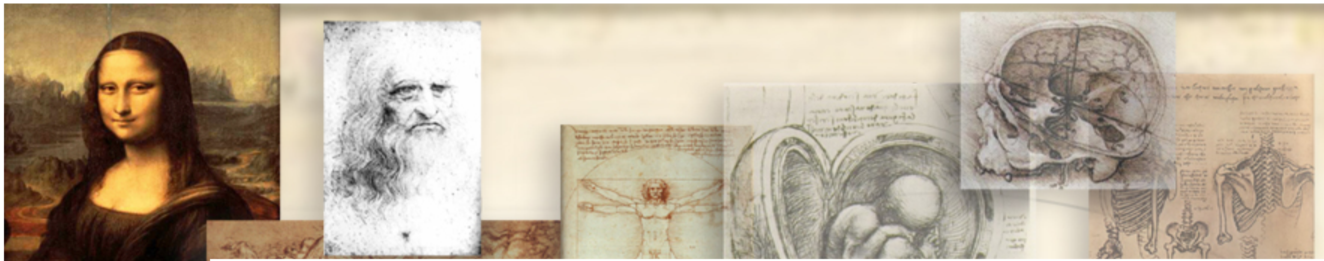
- Measure processes against expected results
- Document differences for further analysis

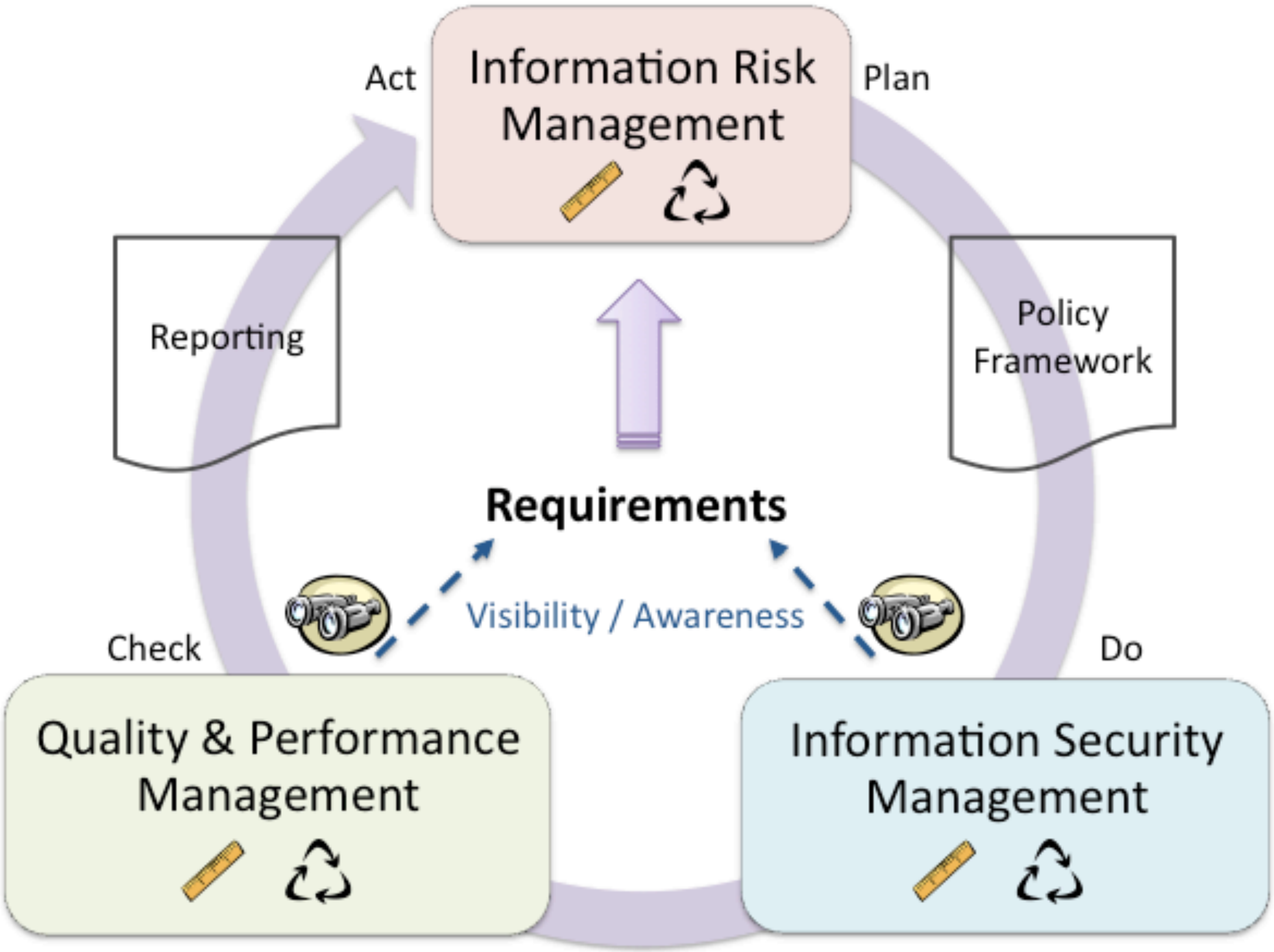
Act

- Analyze differences (cause analysis)
- Determine where changes should be made
- Document recommendations
- No differences? Reinvent…

PDCA and the TEAM Model

- Learning, lifecycle approach
- Always room for improvement
- It doesn’t map cleanly, per se…
- It provides a reference model…




Act
Information Risk Management
Plan
Reporting
Policy Framework
Requirements
Visibility / Awareness
Check
Do
Quality & Performance Management
Information Security Management

Key Attributes

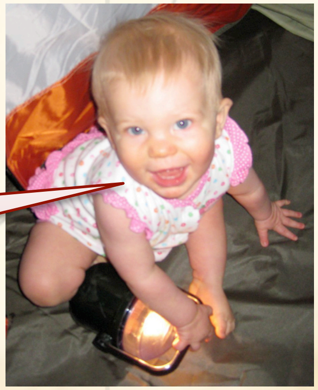
- Requirements-driven
- Nested lifecycles
- Allows best-fit methods in key areas
- De-conflicts / Cross-functional silos
- Promotes visibility & awareness

Information Risk Mgmt

- “Risk is loss or the probability of loss.”
- A lifecycle approach…
- Based on business requirements
- Sets the strategy…

Policy Framework

- A communication vehicle
- The path from strategy to operations
- More to come…



“Rules without consequences are just suggestions.”

Information Security Mgmt

- Operations management
- Includes processes
- Could be ITIL, could be ISO 27002
- Must cover ALL operations

Quality & Performance Mgmt

- Metrics & Measurements
- Security Testing
- Audit & Compliance
- Lots and Lots and Lots of Analysis

Auditor Independence

- The thin grey line…
- This is very important!
- Scope, roles, control…

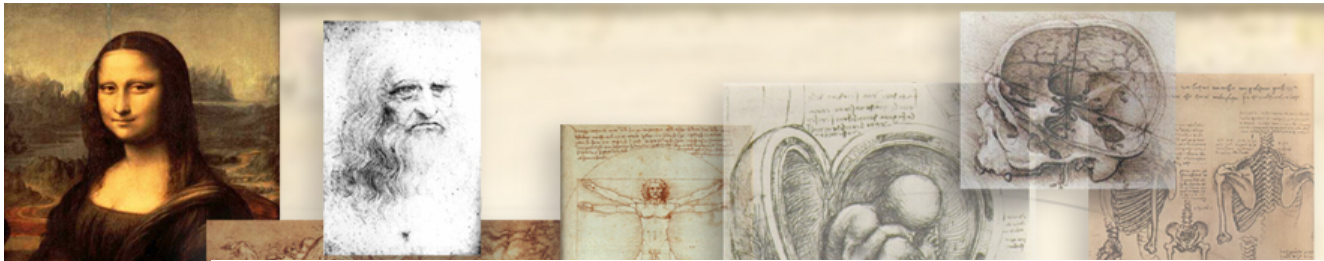
Reporting

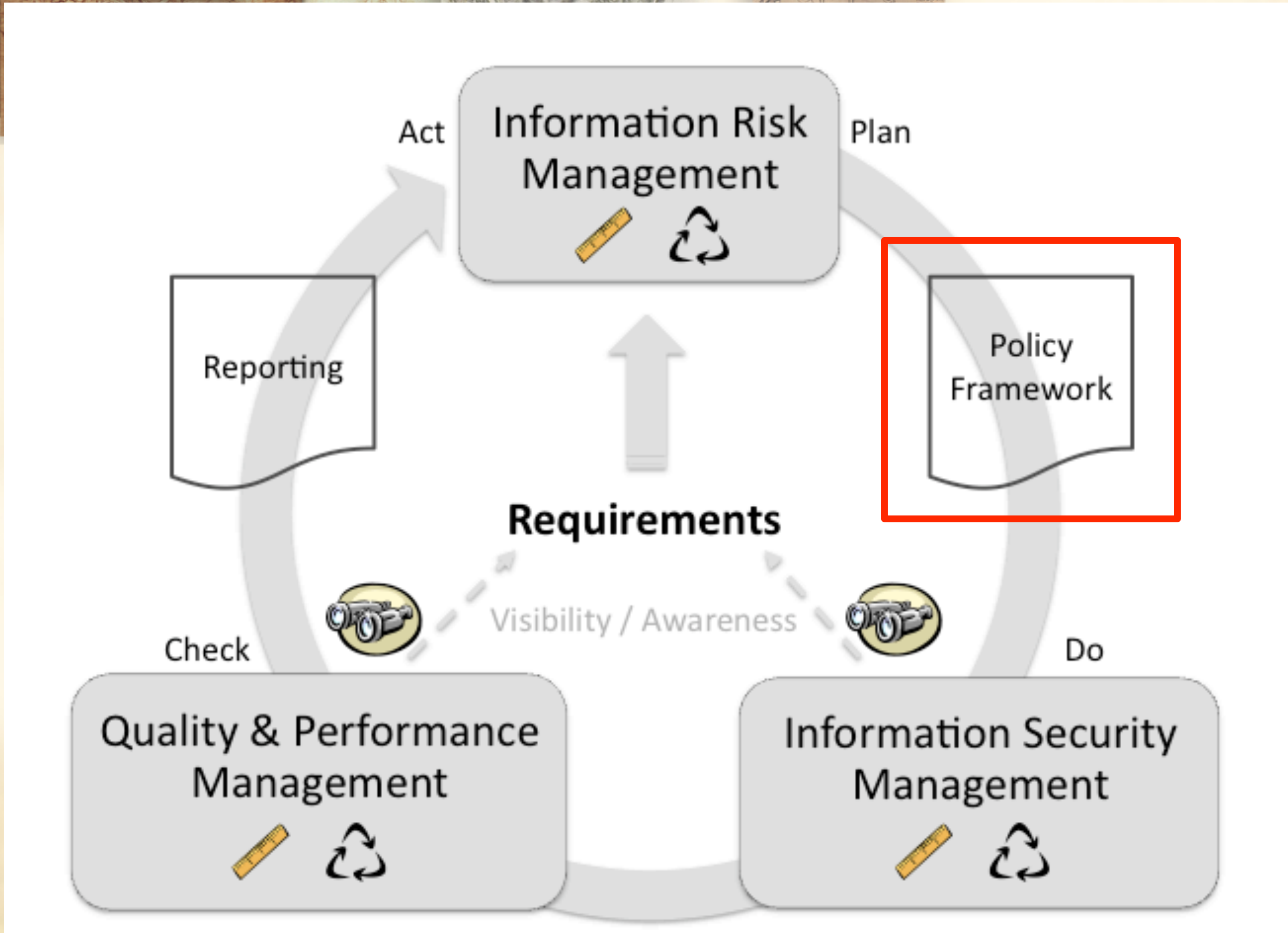
- Could be compliance reports…
- Could be audit reports…
- Could be weather reports…
  - ((think dashboard))
- Drives accountability + improvement!

Reporting

- Inform management and executives
- Inform the board
- Helps ensure due diligence
- KISS Principle

SHORT BREAK!





Information Risk Management

Act

Plan

Reporting

Policy Framework

Requirements

Visibility / Awareness

Check

Do

Quality & Performance Management

Information Security Management

The Policy Framework

- Queue dramatic music…
- Picture a world…
- Queue Oompaloompas…
- Ok, now stop it. ☺

The Policy Framework

- Communication vehicle
- Policies, Standards, Procedures
  - Maybe Guidelines, Processes
- How to…
- Some practical guidance

A Communication Vehicle

- Why do you need this?
- What are you trying to say?
- Translating strategy into operations
- Setting expectations

A Communication Vehicle

- Support with training and awareness
- The vehicle should keep moving
  - Revise regularly
  - Adapt, evolve, survive
- Officially sanctioned

Comprised of…

- Policy: high-level requirements statements
- Standard: detailed requirements
- Procedures: step-by-step guidance
- Guidelines? Processes?

Lineage

- All standards derive from policies
- All procedures derive from standards
- Lineage communicates authority
- Authority must be clear and absolute

How to... Author

Do	Don't
Build a team	Work alone
Define a process	Allow time leaks
Meet regularly	Expect perfection
Set deadlines	Accept excuses
Report to board	Work in a vacuum

How to... Approve

Do

- Include executives
- Include the board
- Use stakeholders
- Promote positives
- Be flexible
- Acknowledge

Don't

- Ignore stakeholders
- Forget legal dept.
- Allow time leaks
- Give up
- Be combative
- Expect an easy road

How to... Promulgate

Do	Don’t
• Over-communicate	• Send and forget
• Use diff. methods	• Be jack-booted
• Make it easy	• Overcomplicate
• Provide training	• Forget training
• Integrate with HR	• Forget HR
• Publish clearly	• Be rude

How to... Revise

Do

- Have a process
- Build a team
- Advise the execs
- Advise the board
- Notify everyone
- Update training

Don't

- Have surprises
- Ignore input
- Forget feedback
- Rush controversy
- Forget to publish
- Exclude people

How to... Enforce

Do

- Be positive
- Be encouraging
- Set consequences
- Follow through
- Work with HR
- Work with Legal

Don't

- Abuse people
- Make an example
- Give a pass
- Be unbalanced
- Forget management
- Promote fear

Practical Guidance

- KISS Principle
- Publish in a couple formats
- Indexed & Searchable!
- Map to compliance requirements
- Leverage standards (e.g. ISO 27002)

LUNCH BREAK!!!

WELCOME BACK! ☺

Agenda

Morning

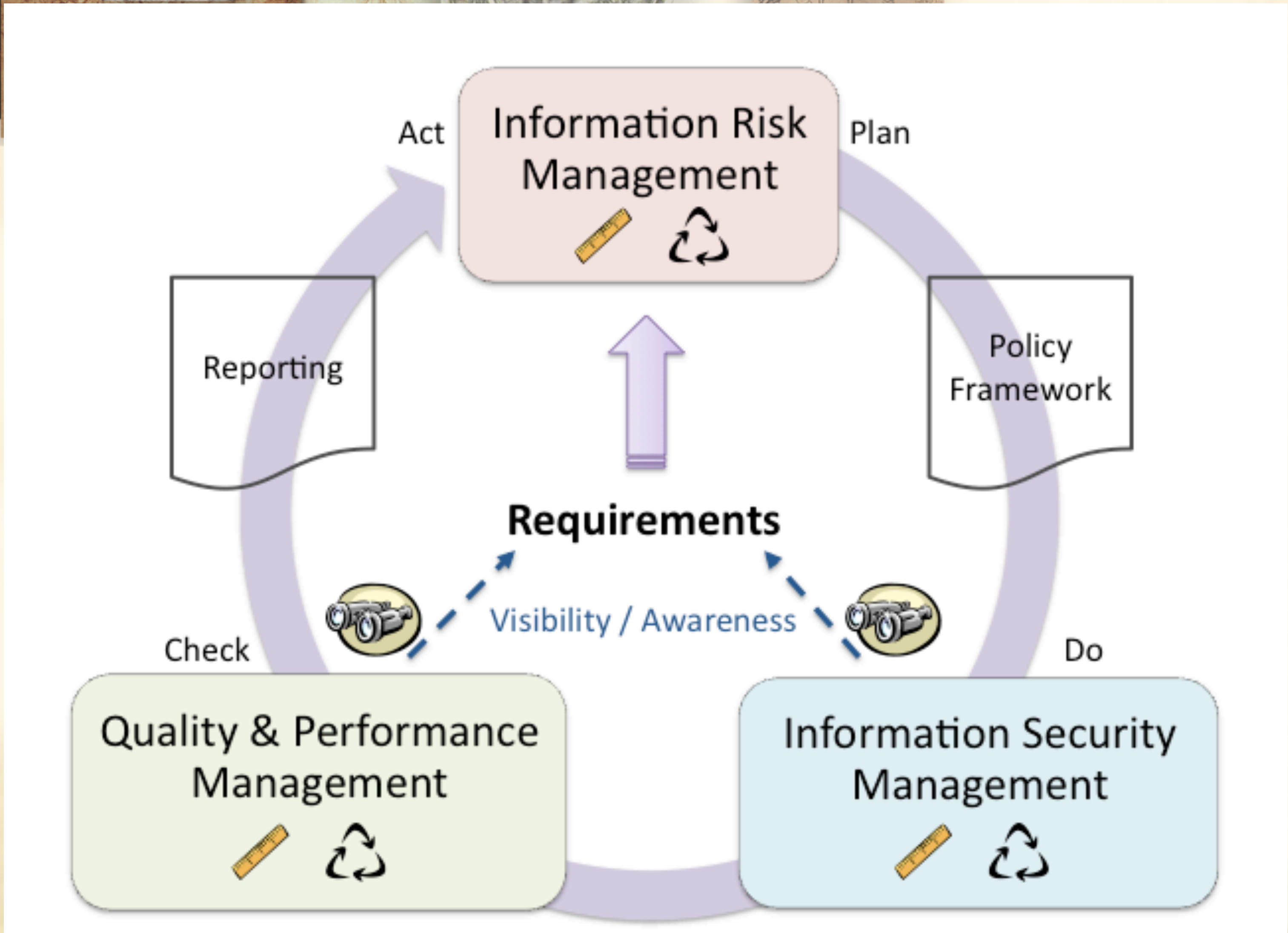
- Introduction
- Survivability
- Risk Mgmt. Fail
- TEAM for Success
- Policy Framework

Afternoon

- Info. Risk Mgmt.
- Info. Sec. Mgmt.
- Q&P Mgmt.
- Putting it Together
- Advanced Topics

First, a Recap…

- Any lingering questions?
- Any lingering doubts?
- Let’s refresh on the TEM Model…



Information Risk Management

Act

Plan

Reporting

Policy Framework

Requirements

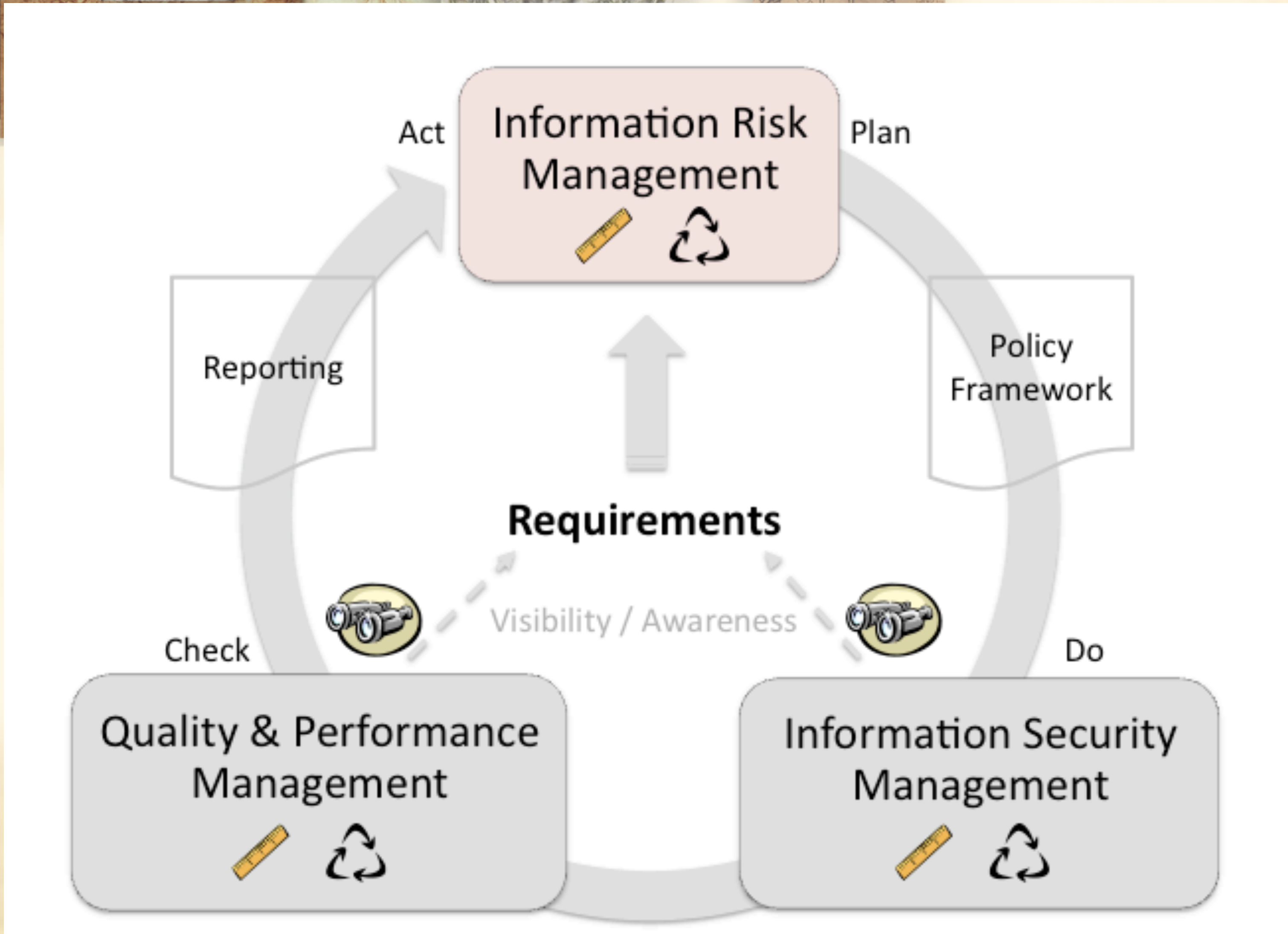
Visibility / Awareness

Check

Do

Quality & Performance Management

Information Security Management



Act

Information Risk Management

Plan

Reporting

Policy Framework

Requirements

Visibility / Awareness

Check

Quality & Performance Management

Do

Information Security Management

Information Risk Management

- Risk Tolerance
- RM Lifecycle
- Formal RM Frameworks
- Maturity
- Assessments
- Risk Treatment (Remediation)
- The Importance of Metrics and Measurement

Risk Tolerance

- Model & Define For Success
- Defense in Depth (or not?)
- Beware Biases
- Acceptable Level of Compromise
- Temporal Tolerance

Model & Define For Success

- Define, baseline risk levels/ratings
- Goes toward data quality…
- Good data facilitates good decisions
- Bad data, false sense of security, etc.

Defense in Depth (or not?)

- The Möbius Defense
- DiD by any other name…
- The Jericho Forum approach
- Survivability!

Beware Biases

- GIGO
- Visibility ➔ Transparency ➔ Quality!
- Cognitive Bias
- Bayesian statistics

Acceptable Level of Comp

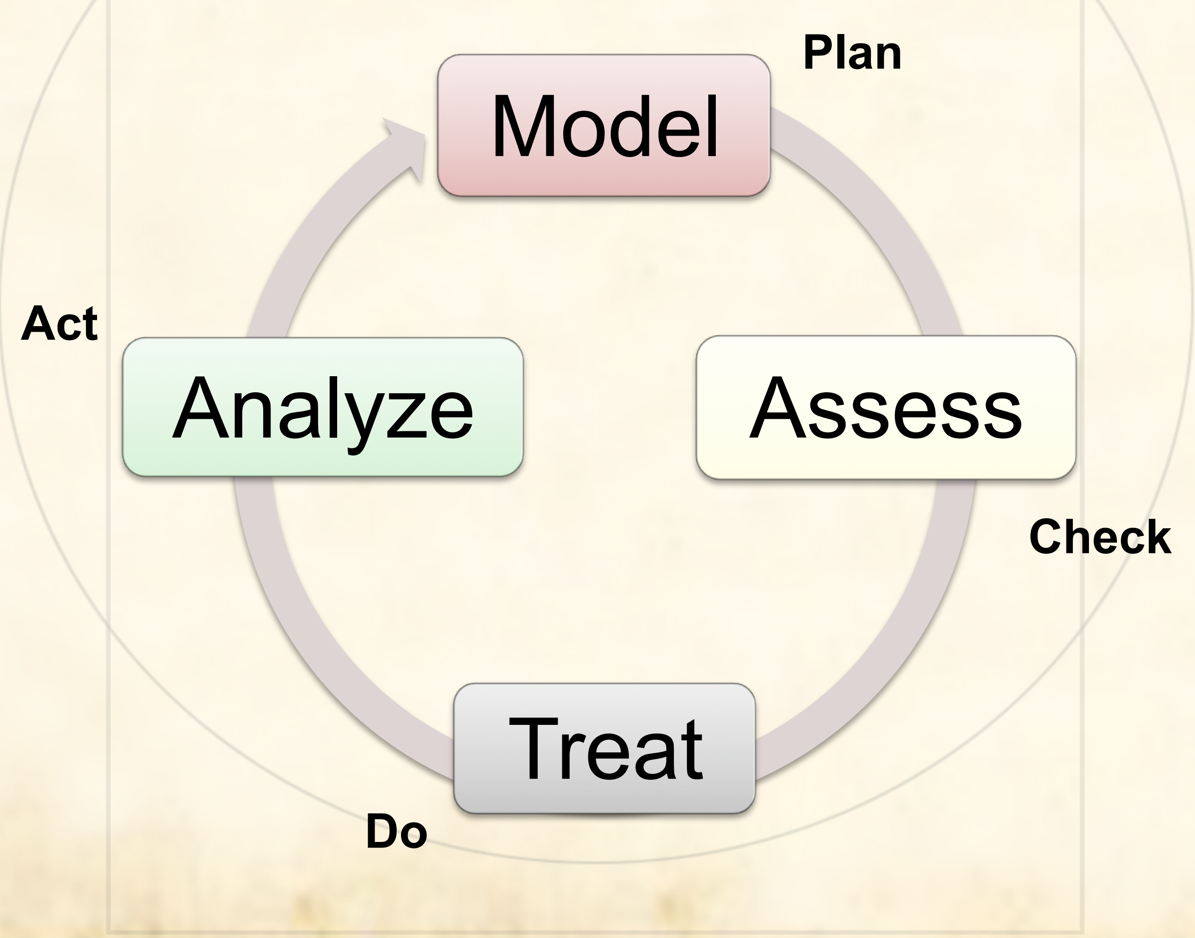
- "The level of system compromise people and enterprises are willing to live with."
- No pain, no motivation for change.

Temporal Tolerance

- What takes years to build can be leveled in hours or days.
- Change cannot be implemented overnight.
- Recoverability vs Defensibility

Info Risk Mgmt Lifecycle

- A lifecycle approach is important
- Risk is never fully eliminated
- Adaptability is imperative
- May not match PDCA?



Plan

Model

Check

Assess

Do

Treat

Act

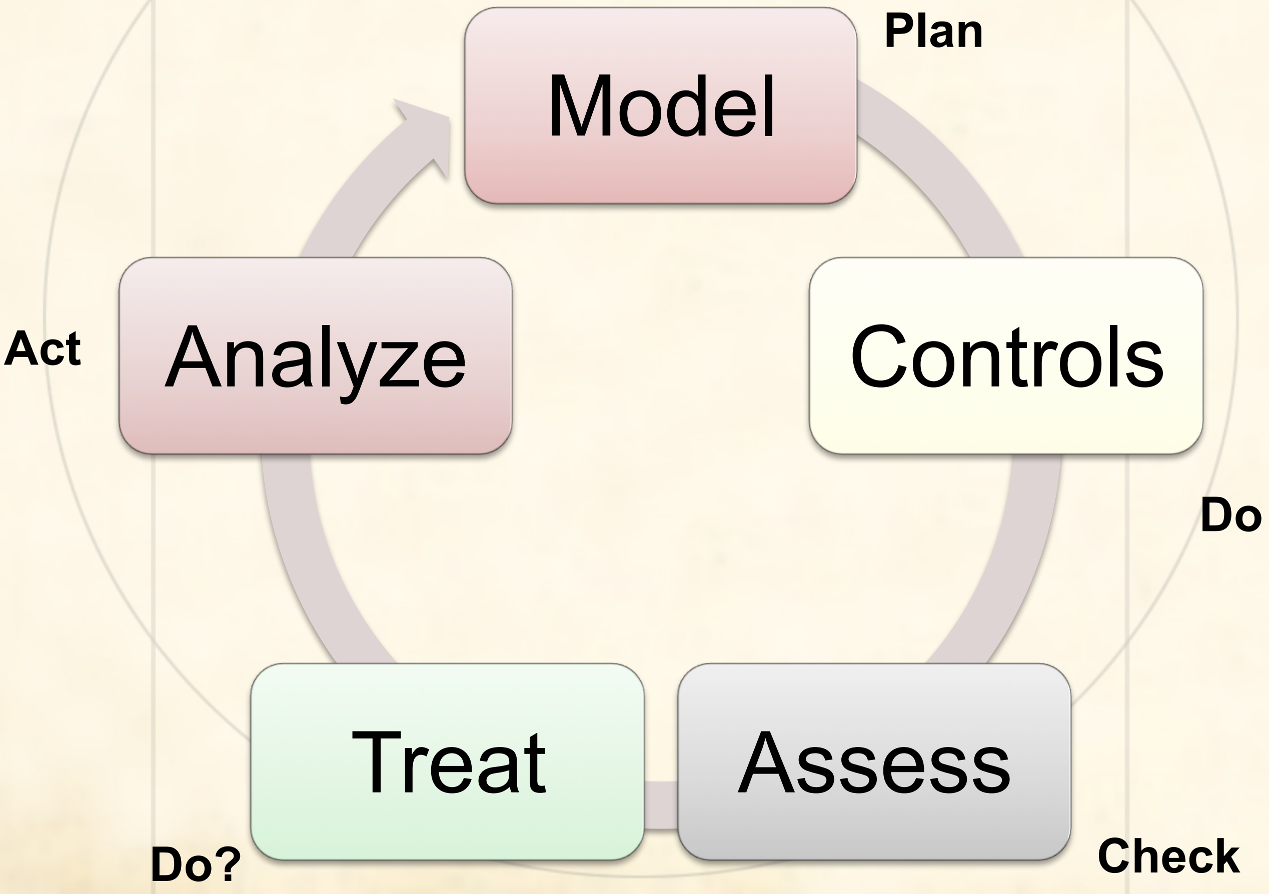
Analyze

Info Risk Mgmt Lifecycle

- Model: Define levels, tolerance
- Assess: Risk assessment
- Treat: Remediation
- Analyze: Actual vs expected results

Info. Risk Mgmt Lifecycle

- Assessing what?
  - Assumes controls implemented
- Remediation
  - Assumes implementing controls


Model
Plan
Controls
Do
Assess
Check
Treat
Do?
Analyze
Act

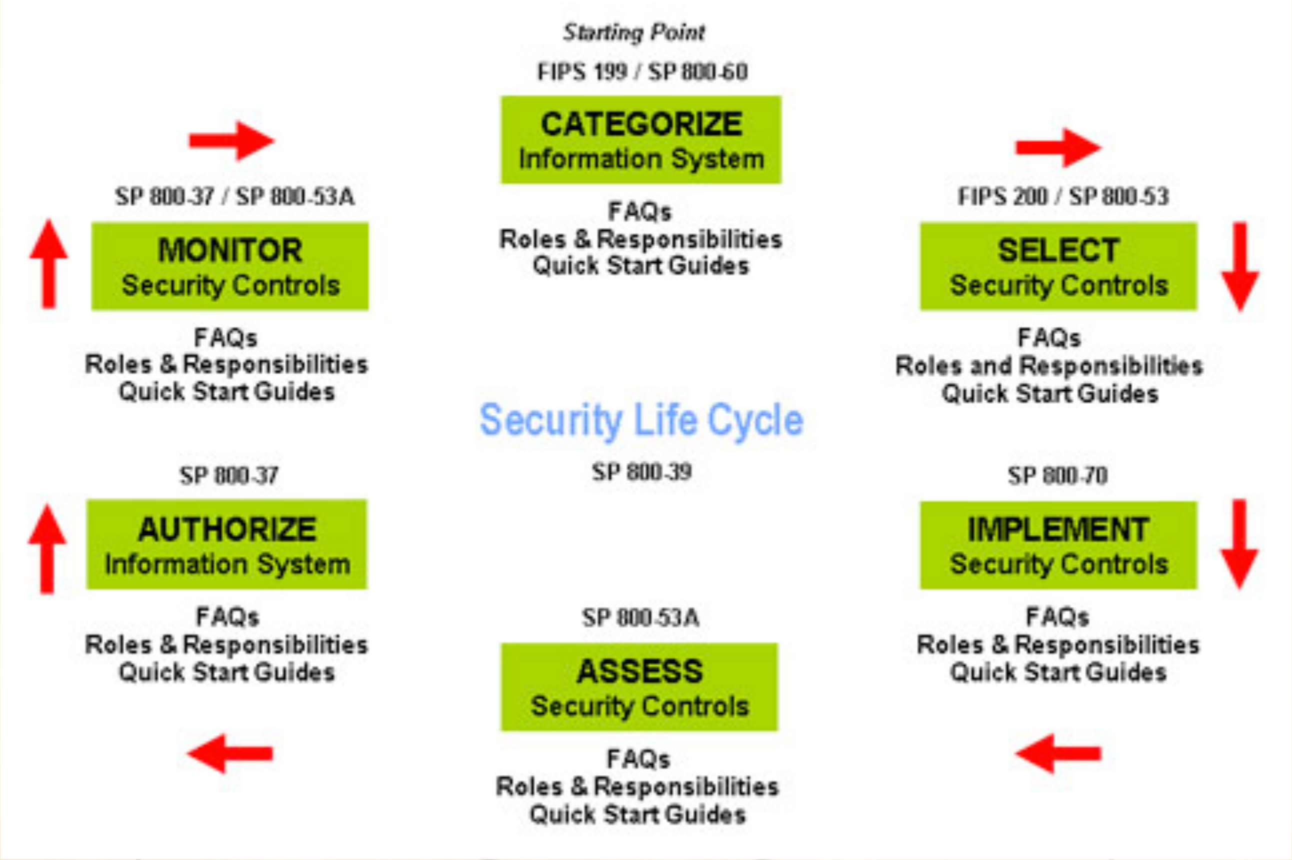
HOW DO OTHERS DO IT?

Formal Frameworks

- NIST RMF
- COSO ERM Framework
- EDUCAUSE/Internet2 RMF
- ISO Standards(27005, 31000, 31010)

NIST Risk Mgmt Framework

- Part of FISMA and CNSS efforts
- Generally required for Federal sector
- Based on series of documents



Starting Point

FIPS 199 / SP 800-60

CATEGORIZE
Information System

FAQs
Roles & Responsibilities
Quick Start Guides

FIPS 200 / SP 800-53

SELECT
Security Controls

FAQs
Roles and Responsibilities
Quick Start Guides

SP 800-70

IMPLEMENT
Security Controls

FAQs
Roles & Responsibilities
Quick Start Guides

SP 800-53A

ASSESS
Security Controls

FAQs
Roles & Responsibilities
Quick Start Guides

SP 800-37

AUTHORIZE
Information System

FAQs
Roles & Responsibilities
Quick Start Guides

SP 800-37 / SP 800-53A

MONITOR
Security Controls

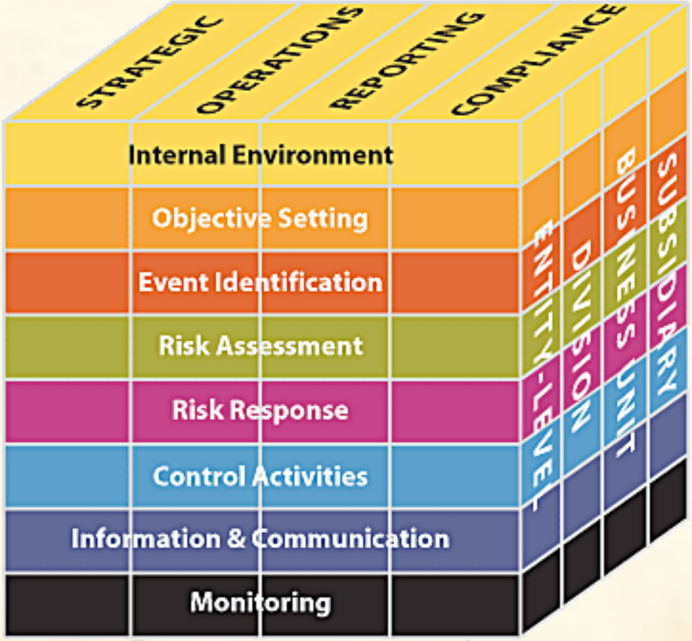
FAQs
Roles & Responsibilities
Quick Start Guides

Security Life Cycle

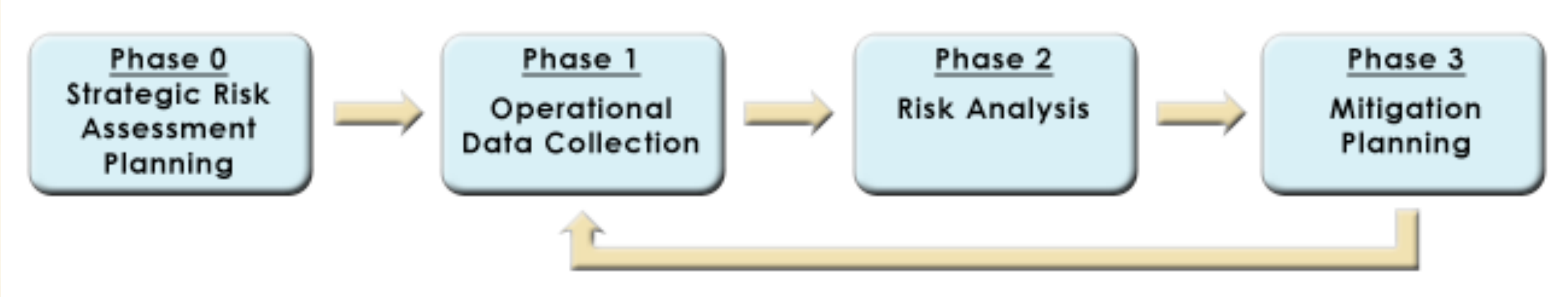
SP 800-39

COSO ERM Framework

- 8 objectives
- 4 categories
  - Strategic
  - Operations
  - Reporting
  - Compliance



EDUCAUSE/Internet2 RMF



Phase 0
Strategic Risk Assessment Planning

Phase 1
Operational Data Collection

Phase 2
Risk Analysis

Phase 3
Mitigation Planning

Model **Assess** **Analyze** **Treat**

EDUCAUSE/Internet2 RMF

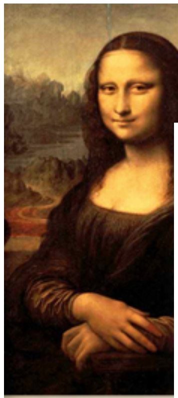
- Ignored PDCA, which is fine
- Lightweight, simple, logical
- Model is never updated?

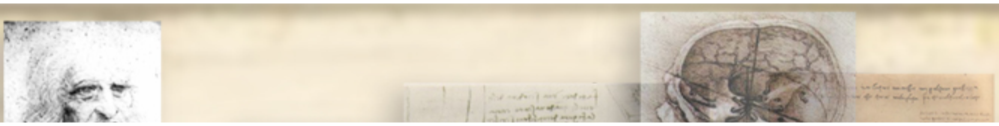
ISO Standards

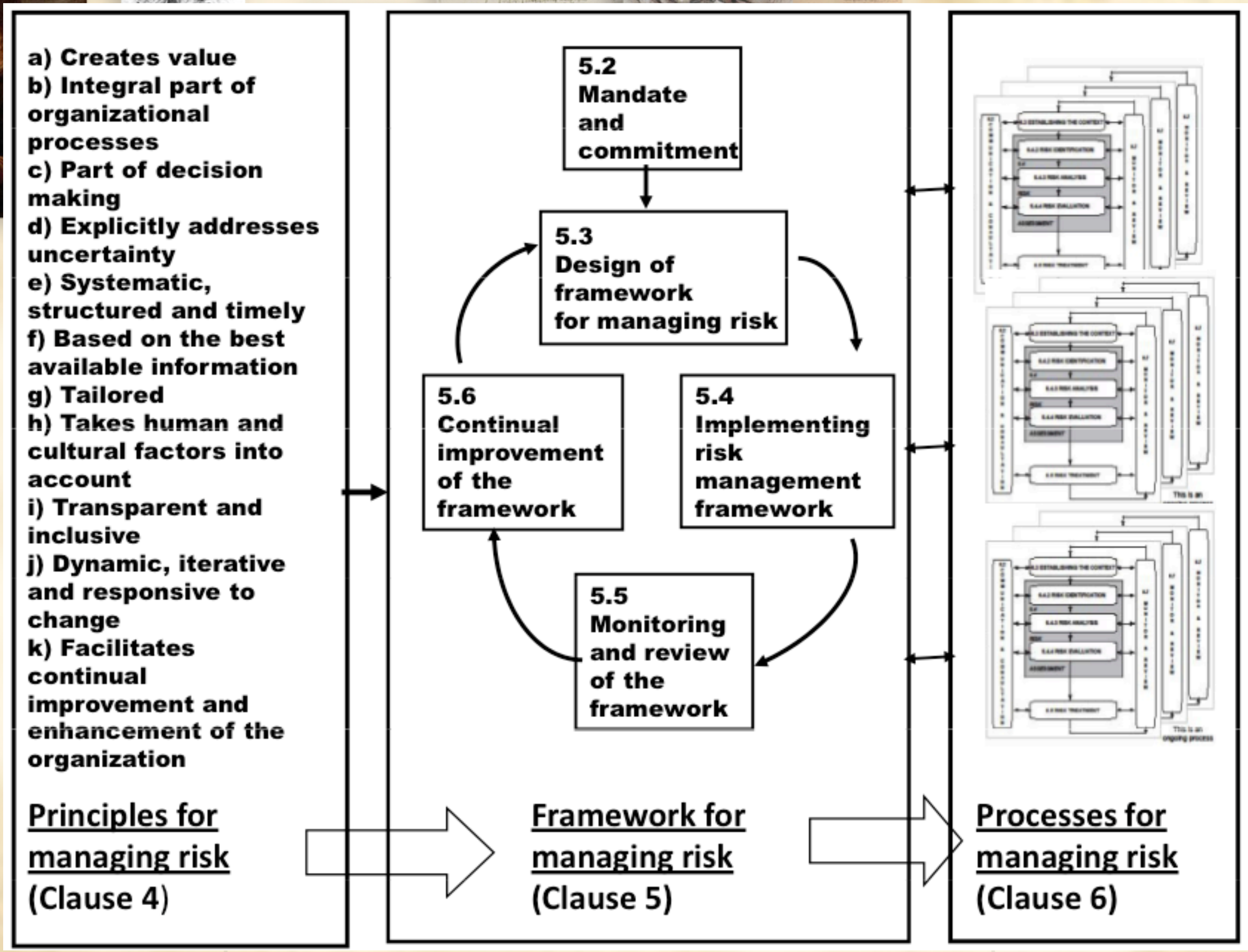
- 27005:2008 – InfoSec Risk Mgmt
  - Part of 27000 Series
  - Expected to re-align to 31000
- 31000 – Risk Management Principles
- 31010 – Risk Assessment Techniques

ISO/IEC 31000:2009

- New standard, due out 2009
- Will be THE ISO risk mgmt approach
- Generic, extensible
- Maps to PDCA







a) Creates value
b) Integral part of organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured and timely
f) Based on the best available information
g) Tailored
h) Takes human and cultural factors into account
i) Transparent and inclusive
j) Dynamic, iterative and responsive to change
k) Facilitates continual improvement and enhancement of the organization

Principles for managing risk
(Clause 4)

5.2 Mandate and commitment

5.3 Design of framework for managing risk

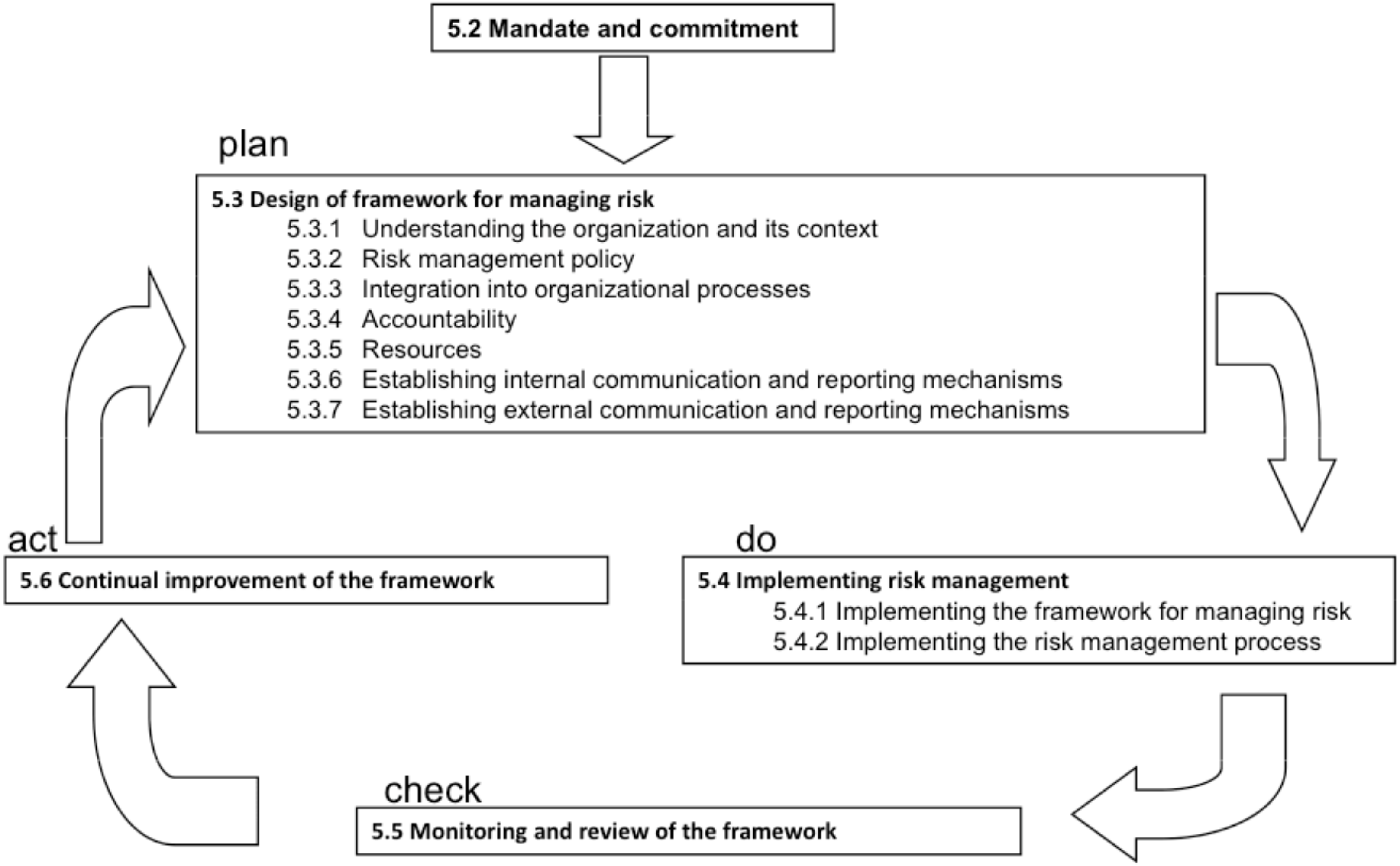
5.4 Implementing risk management framework

5.5 Monitoring and review of the framework

5.6 Continual improvement of the framework

Framework for managing risk
(Clause 5)

Processes for managing risk
(Clause 6)



5.2 Mandate and commitment

plan

5.3 Design of framework for managing risk

5.3.1 Understanding the organization and its context
5.3.2 Risk management policy
5.3.3 Integration into organizational processes
5.3.4 Accountability
5.3.5 Resources
5.3.6 Establishing internal communication and reporting mechanisms
5.3.7 Establishing external communication and reporting mechanisms

do

5.4 Implementing risk management

5.4.1 Implementing the framework for managing risk
5.4.2 Implementing the risk management process

check

5.5 Monitoring and review of the framework

act

5.6 Continual improvement of the framework

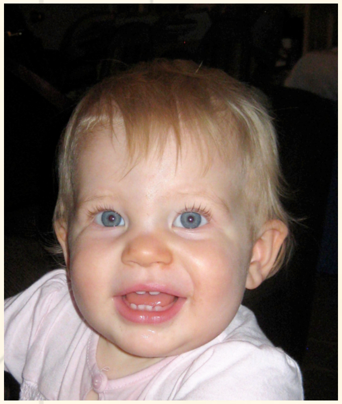
Continuous Improvement of the ISO 31000 Framework for risk management

ISO/IEC 31000:2009

- Overall, a good model
- Heavyweight standard (as usual)
- Could resolve many questions
  - IF adopted…

Risk Mgmt Maturity

- Intro to CMM approach…
  - Why is this useful?
- Currently, no CMM for RM
- What would it look like?
  - Good question… TBD!



Assessment Techniques

- Everybody has one…
  - Very few publish them…
- RMI FAIR recommended
- IA-CMM (was) recommended
  - ISATRP coming soon…

Assessment Techniques

- Watch out for:
  - Lack of in-context modeling
  - Blind “value” assignments
  - Lack of in-context analysis
- Is it really High / Medium / Low?

Assessment Techniques

- More in the Q&PM section…
- Beware absolutist statements
- 3rd party vs 1st party

Risk Treatment

- Various names:
  - Control
  - Countermeasure
  - Safeguard
  - Firewall ☺

Risk Treatment

- Beware Biases!
- Prioritize assessment results
- Look at cost + ease + effectiveness
- For example…

Risk Treatment: Example 1

- Whiz-bang UTM…
  - Expensive, SPOF
  - May “solve” lots of problems
- What about open-source?
- Do you need everything?

Risk Treatment: Example 2

- Anti-virus…
  - Regs require
  - Not overly effective
  - Better than nothing?
  - Needed? (Mac vs Windows vs Linux)

Risk Treatment: Example 3

- Scans & penetration testing…
  - Do you know your environment?
  - Are you sure?
  - ACL drops can be deadly
  - Also consider red teams…

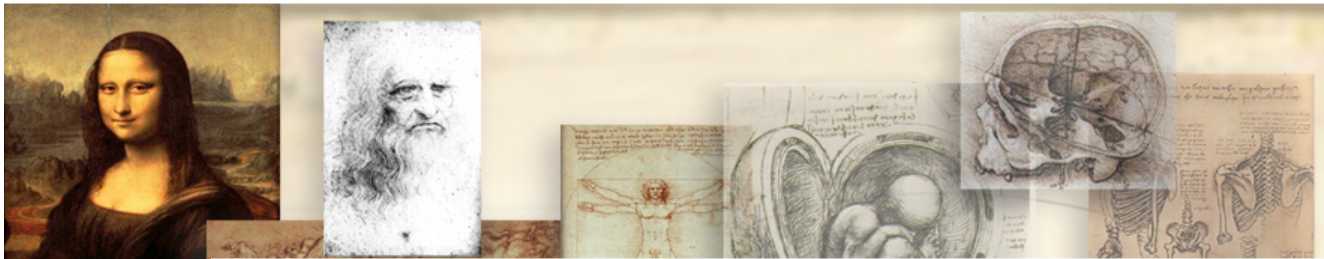
Risk Treatment: Example 4

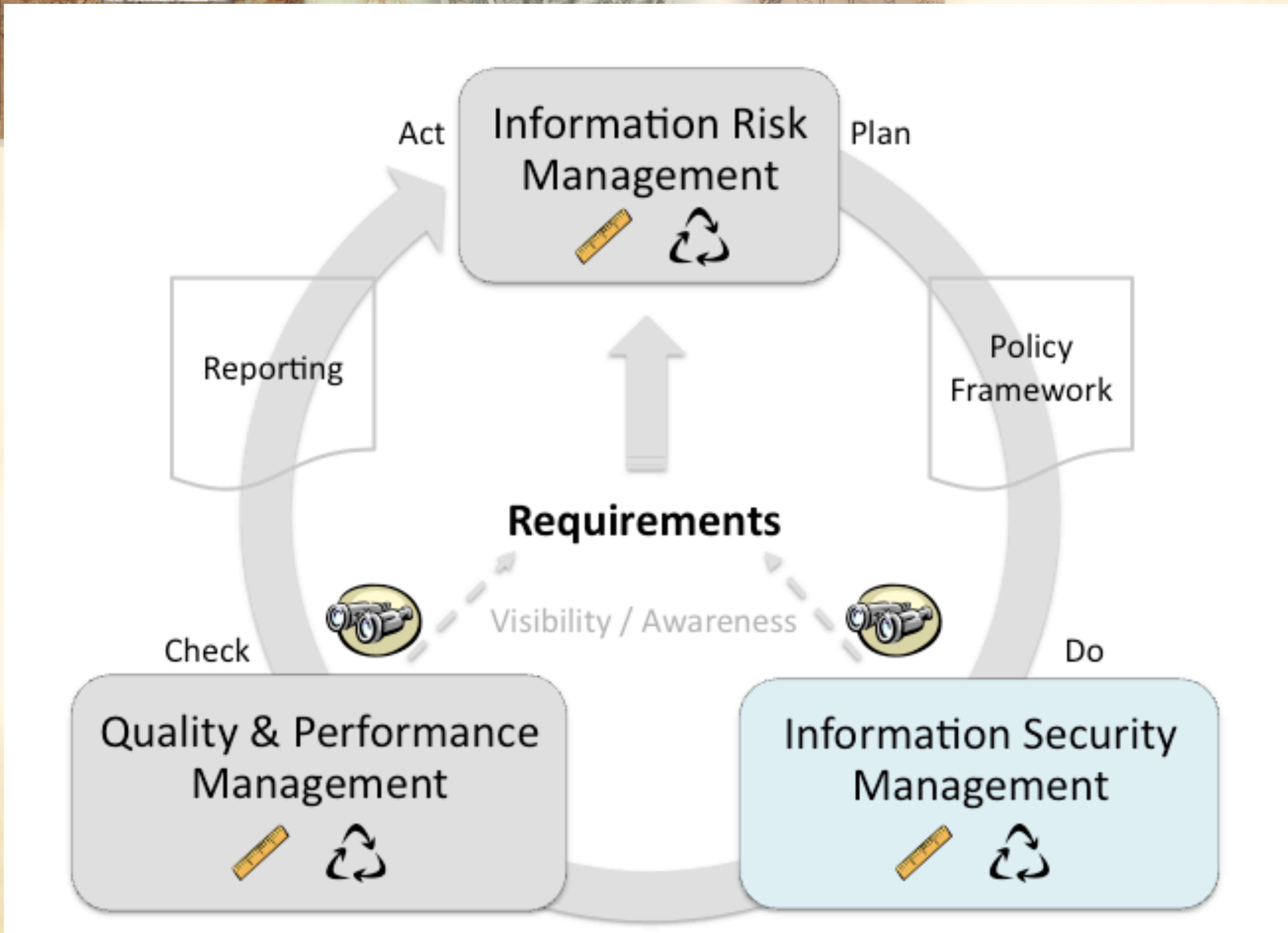
- Log management…
  - Commercial vs open-source
  - Major PITA oftentimes
  - Regs require
  - Potentially huge upside

Metrics and Measurement

- Will discuss more later, but…
- Good data & GIGO (as discussed)
- RM value directly correlates to data
- Goal: measuring progress/maturity

SHORT BREAK!





Information Risk Management

Act

Plan

Policy Framework

Reporting

Requirements

Visibility / Awareness

Check

Do

Quality & Performance Management

Information Security Management

Information Security Mgmt

- Approaches
- Building In Risk Tolerance
- Where the Rubber Meets the Road

Approaches to InfoSec Mgmt

- ISO/IEC 27001/27002
- ITIL v3
- Is it InfoSec or IT Mgmt?
  - Should there be a difference?
  - Does org. size matter?

Building In Risk Tolerance

- Defense in Depth
- Incident Response Management
- Not If, But When

Defense in Depth

- Defensibility!
- Möbius Defense
- Jericho Forum
- Best-fit methods *for your organization*!

Defense in Depth

- Really, compartmentalization
- And, logging & monitoring
- And, processes
- And, accountability for processes

Incident Response Mgmt

- Recoverability!
- Minimally:
  - Know who to call
  - Know what to do
  - Have BCP/DRP

Incident Response Mgmt

- Processes
- Documentation
- Classification
  - Type
  - Severity

- Contacts:
  - IRM Team
  - Mgmt / Execs
  - Law Enforcement
  - Card Brands
  - Etc.

Not If, But When

- You are being attacked already
- You will have an incident
  - You probably already have!
  - Incident != Compromise (necessarily)
- Track, adapt, win

Training & Awareness

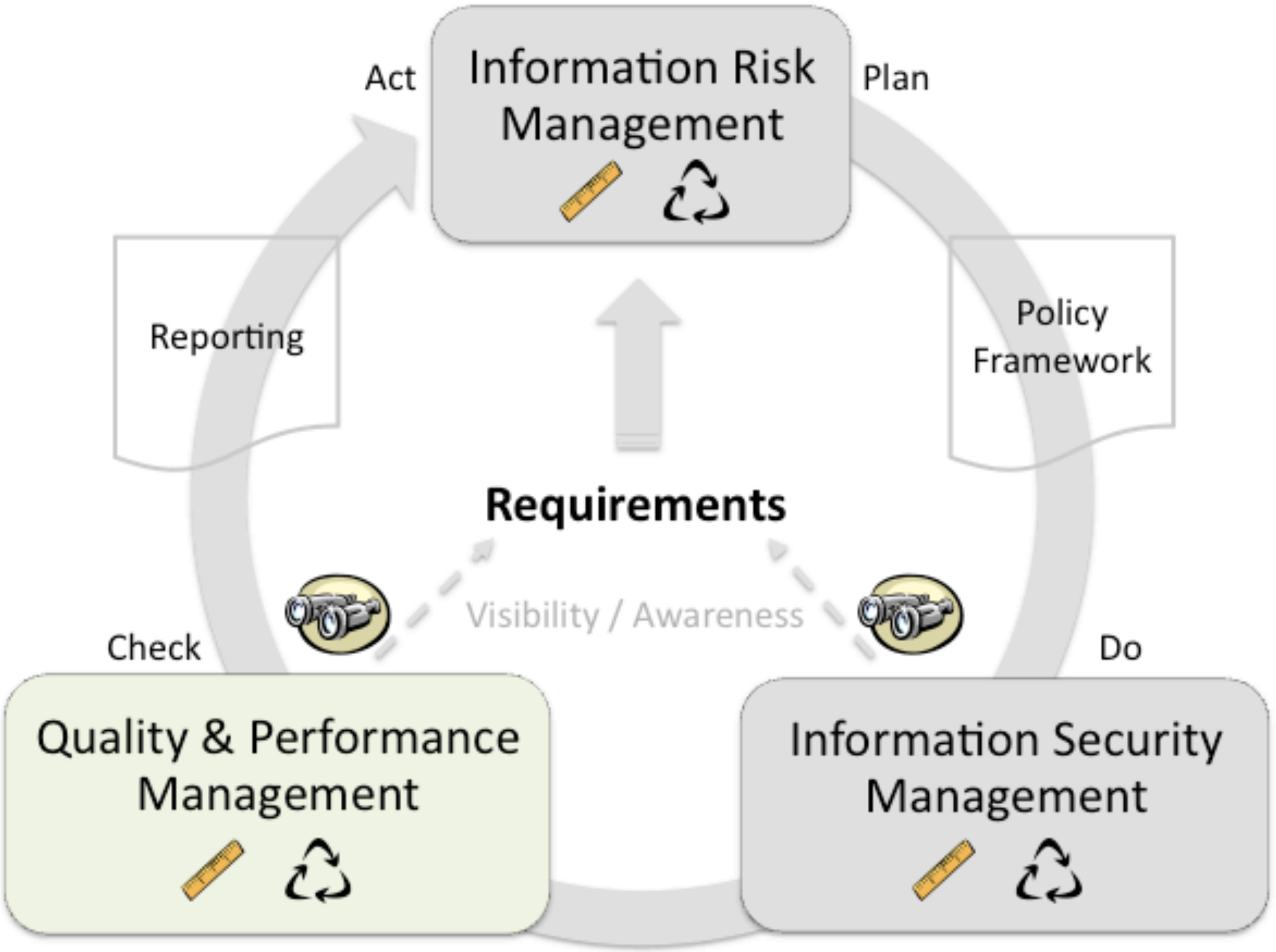
- Cheap!
- Effective!
- Responsibility!
- Accountability!

- Possible topics:
  - General
  - Processes
  - Suspicious behavior/activity
  - Notifications

Rubber Meets the Road

- Practical Advice:
  - You can’t do everything at once
  - Need security at multiple levels
  - Don’t underestimate the value of data
  - Scans, tests, logs = Visibility

SHORT BREAK!



Act
Information Risk Management
Plan
Reporting
Policy Framework
Requirements
Visibility / Awareness
Check
Do
Quality & Performance Management
Information Security Management

SO, YOU DID STUFF, BUT…

WAS IT USEFUL STUFF?

Quality & Performance Mgmt

- ROI/ROSI
- Audit & Compliance
- Security Testing
- Metrics & Measurement
- The Importance of Time

ROI/ROSI

- Return on (Security) Investment
- Cost-Benefit vs Cost-Effectiveness
- Is any of this even valid?
- How do you prove a negative?

Audit & Compliance

- Is audit important?
- Can you use CObIT?
- Which came first, the audit or auditor?
- Scoping, Checklists, and Other Myths

Is Audit Important?

- Audit is important, within it’s role…
- 3rd party attestation is here to stay…
- Don’t settle for checklists…
- ***You*** make the experience valuable

Can You Use CObIT?

- Yes, of course…
- Is there value?
- Does it help your org.?
  - Or, does it just help your auditor?
    - …with profitability?

Which Came First…

- …the audit or the auditor?
- Make sure your auditor knows who’s in charge.
- Make sure you own the audit scope.
- Be flexible.

Scoping, Checklists, Myths

- Audits live and die by scope.
- Audits often use checklists.
- Insist on experienced auditors.
  - Not just “lead” auditors – all/most of them!

Scoping, Checklists, Myths

- Myths:
  - auditor sets the scope
  - auditor can tell you what to do
  - auditor knows best
  - auditor knows your business

Bonus: Marketing Hype

- GRC: Governance, Risk, Compliance
  - Doesn’t even make sense…
  - Used to sell products you may not need!
- FUD: Fear, Uncertainty, Doubt
  - Common sales technique (in politics, too)

Security Testing

- Penetration Testing
- Code Review/Assessment
- Application Security Testing
- Red Teams
- High-Level Reviews

Penetration Testing

- Networks and/or systems
- Some regs. require
- Given time, there will be findings
- Anything can be hacked OR broken

Penetration Testing

- NOT a Nessus scan
- NOT an audit (no checklists)
- NOT a policy review
- NOT a risk assessment
- NOT an ASV scan

Code Review/Assessment

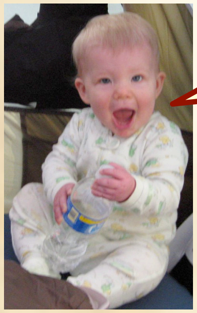
- Dynamic vs Static
- Static:
  - Tools-oriented
  - Time-consuming
  - Often expensive

Application Security Testing

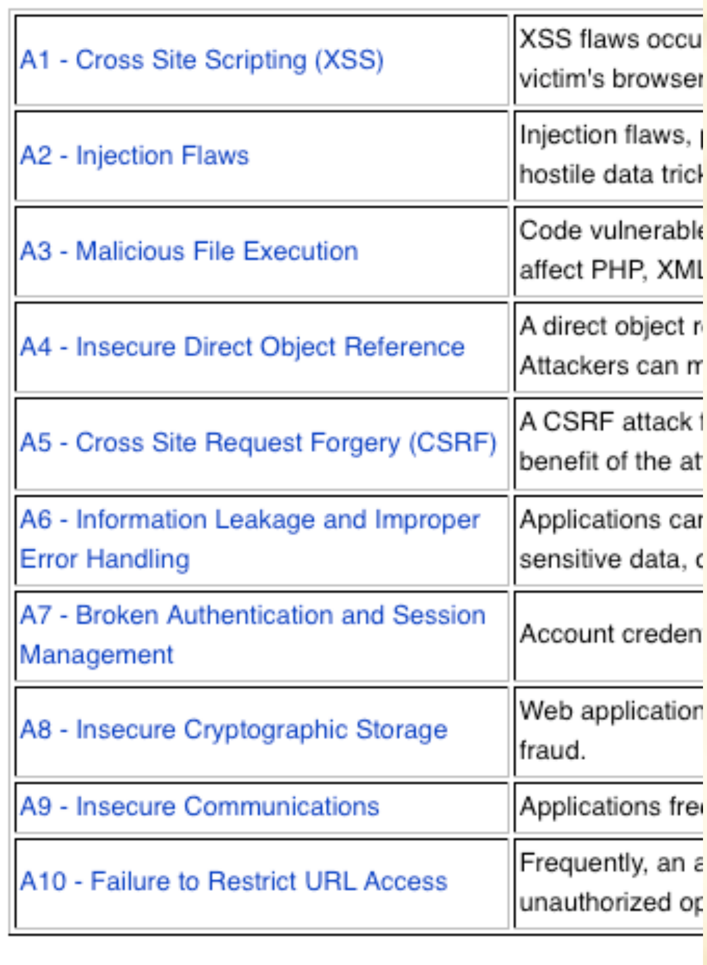
- A type of pen-testing & code review
- Focuses on apps, is dynamic
- XSS, CSRF, SQLi
- OWASP!!!

Open
Web
Application
Security
Project

Top
10
List
2007



"No OWASP
in Montana?!"



A1 - Cross Site Scripting (XSS)	XSS flaws occu victim's browser
A2 - Injection Flaws	Injection flaws, p hostile data trick
A3 - Malicious File Execution	Code vulnerable affect PHP, XML
A4 - Insecure Direct Object Reference	A direct object r Attackers can m
A5 - Cross Site Request Forgery (CSRF)	A CSRF attack f benefit of the at
A6 - Information Leakage and Improper Error Handling	Applications car sensitive data, c
A7 - Broken Authentication and Session Management	Account creden
A8 - Insecure Cryptographic Storage	Web application fraud.
A9 - Insecure Communications	Applications fre
A10 - Failure to Restrict URL Access	Frequently, an a unauthorized op

Source: http://www.owasp.org/index.php/Top_10_2007

Red Teams

- Threat modeling
- Social engineering most common
- ISATRP methodology next year

High-Level Reviews

- Risk assessments
- Design reviews
- Generally not technical hands-on
- More “builder” than “breaker”

The Importance of Context

- Not all findings are equal
- Hard to network “root” an offline box
- Findings *must* be put into biz terms
- “Tell me why this is important *to me*.”

Metrics & Measurements

- The holy grail of assurance mgmt!
- How do you know if you’re improving?
- Bayesian vs. frequentist statistics
- Trending and analysis
- GIGO (again)

Metrics & Measurements

- Resources:
  - CIS Security Metrics
  - SecurityMetrics.org / MetriCon
  - NIST SP 800-55

The Importance of Time

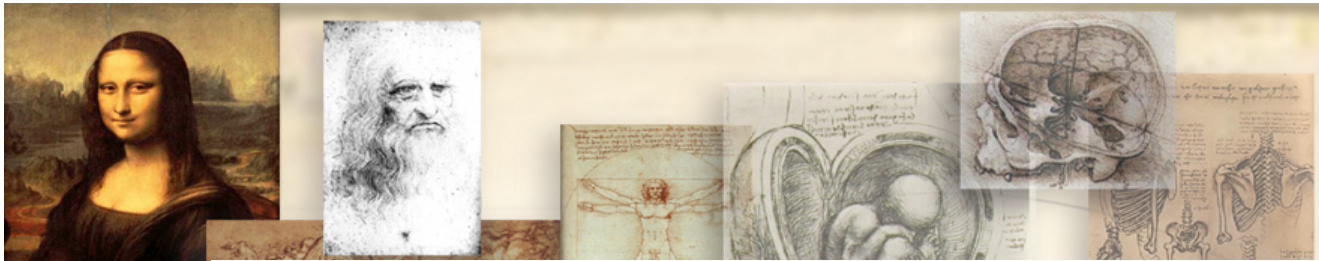
- Necessary for incident response
- Necessary for litigation support
- Required by some regs.
- How reliable is your time source?

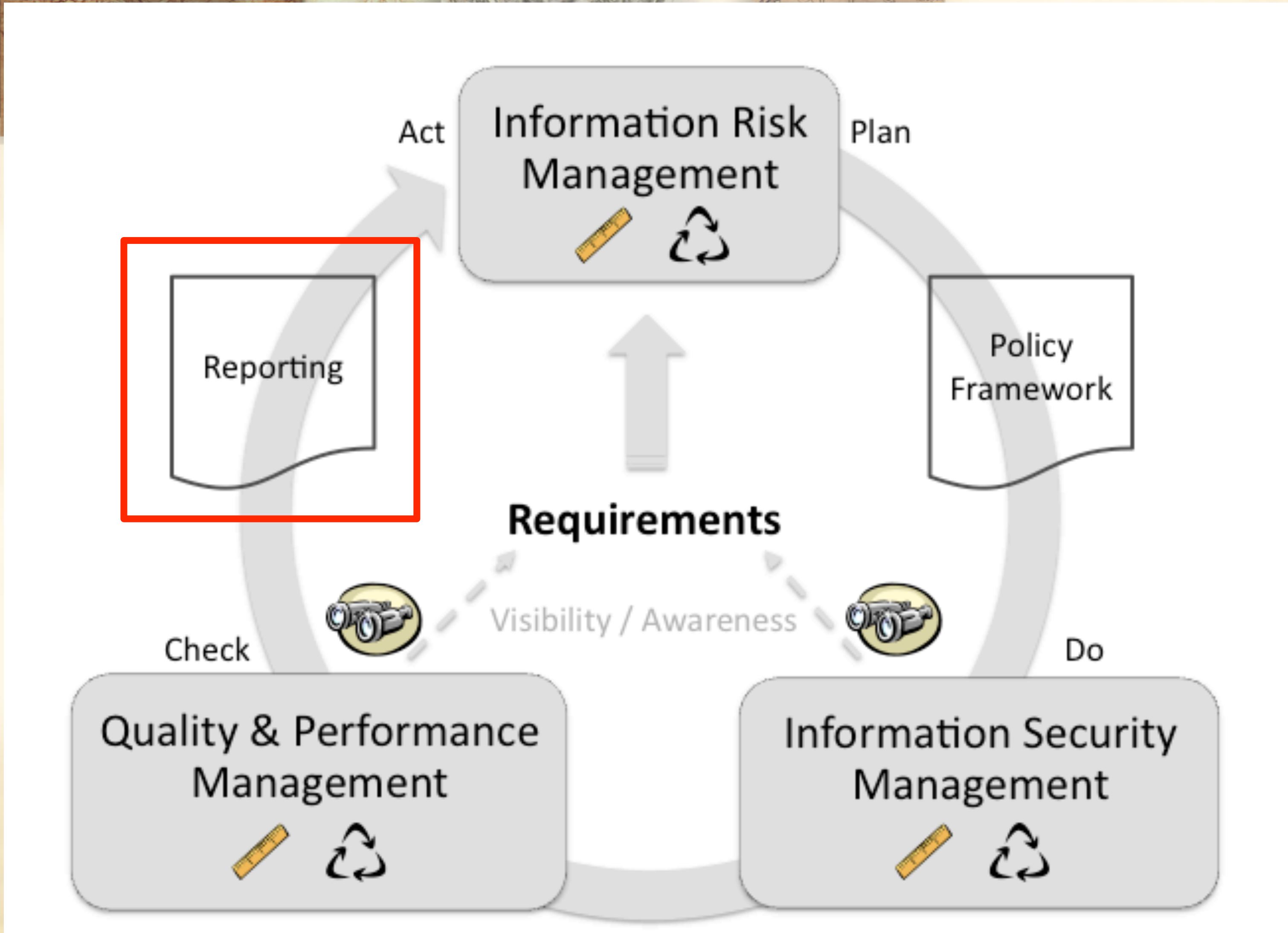
The Importance of Time

- Best Practice:
  - 2-3 time servers within your org.
  - Servers sync off known good source
  - Everything else syncs of your servers
- See Certichron (certichron.com)…

Reporting!

- If you’ll recall…





Information Risk Management

Act

Plan

Reporting

Policy Framework

Requirements

Visibility / Awareness

Check

Do

Quality & Performance Management

Information Security Management

Reporting

- Continuous Improvement
- Maturity and Adaptation
- Ties to Defensibility & Recoverability

SHORT BREAK!

IN THE HOME STRETCH…

Putting It All Together

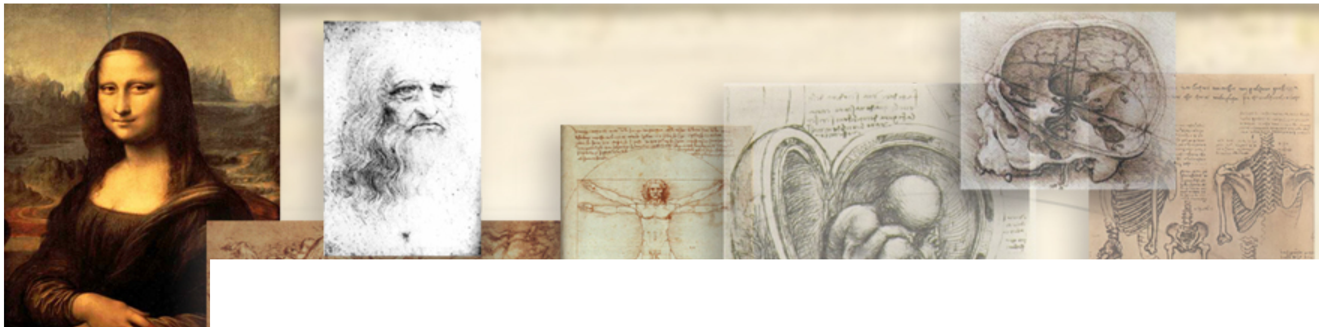
- The Big Picture
- How TEAM Leads to Survivability
- Next Steps

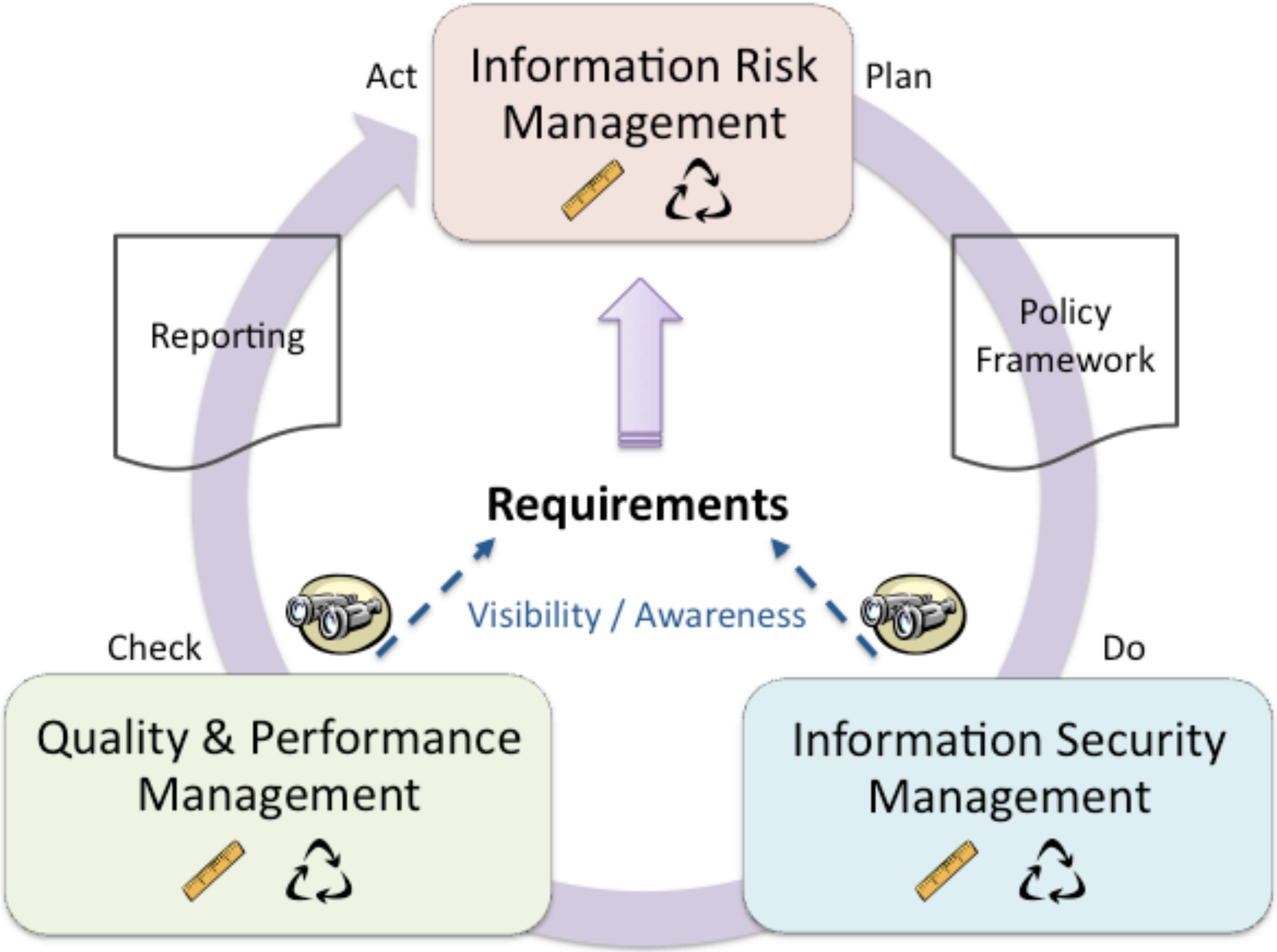
The Big Picture

- We've covered:
  - Survivability
    - Defensibility & Recoverability
  - Policy Framework
  - The TEAM Model

The Big Picture

- Goals:
  - Visibility & Transparency
  - Defensibility & Recoverability
  - Quality Data for Quality Decisions
  - Proper Risk Management





Act

Information Risk Management

Plan

Reporting

Policy Framework

Requirements

Visibility / Awareness

Check

Do

Quality & Performance Management

Information Security Management

TEAM → Survivability

- TEAM is a reference model
- It allows for orgs to harmonize "best-fit" approaches
- TEAM provides the framework for due diligence and reasonable care

TEAM → Survivability

- Survivability is the goal of TEAM
- Objective is a/an (oftentimes legally) defensible position
- Recoverability means operating despite degradation

TEAM → Survivability

- Do you have to use this approach?
  - Obviously, no.
- Are there alternative models today?
  - None I'm aware of.
- Mainstream vs Emerging Theory

Next Steps…

- Your org. likely already exists…
- Where to start?
  - What do you have?
  - Leverage your strengths!
  - Gap analysis?

Next Steps…

- De-conflict silos
- Clarify roles/responsibilities
- Seek good data
- Collaboration, *not* competition

Next Steps…

- Make an overall plan
- Prioritize efforts
- Evaluate cost-effectiveness
- One size does not fit all in solutions
  - TEAM Model fits most!

Advanced Topics

- Planning & Design
- Needed Tech?
- Standards
- Cloud Computing & Virtualization
- Encryption
- Key Management
- Security of Psychology

Planning and Design

- Very important!
- Measure twice, cut once!
- ***Huge*** cost savings potential
- Helps achieve survivability

Needed Technology?

- What Technology is Really Needed?
  - Beware the hype cycle
  - Shiny Object Syndrome
  - What’s the business case?

Standards

- Role and Importance
- IEEE, IETF, OASIS, ANSI, ISO, ISECOM, TCG, NIST, PCI, CIS, etc.

Cloud Computing & Virtualization

- Cloud Security Alliance http://www.cloudsecurityalliance.org/
- Cloud Computing @ Wikipedia http://en.wikipedia.org/wiki/Cloud_computing

Cloud Computing & Virtualization

- IaaS, PaaS, SaaS…
- Public vs. Private
- Jurisdictional issues
- Control issues
- SLAs, responsibilities

Encryption & Key Mgmt

- Encryption: Easy
- Key management: Very Hard
- Costs to doing it wrong: Very High
- Don’t roll your own code, please!

The Psychology of Security

- Cognitive Dissonance
- Enablement
- Social Engineering

OPEN Q&A / DISCUSSION

Benjamin Tomhave, MS, CISSP
http://www.secureconsulting.net/
tomhave@secureconsulting.net
http://twitter.com/falconsview

THANK YOU!