County of Sacramento California

1 2 3 4 5

Case Study: Five ways to energize your information security program

By Jim Reiner, ISO, HIPAA Security Manager

reinerj@saccounty.net

A top security program goes unnoticed

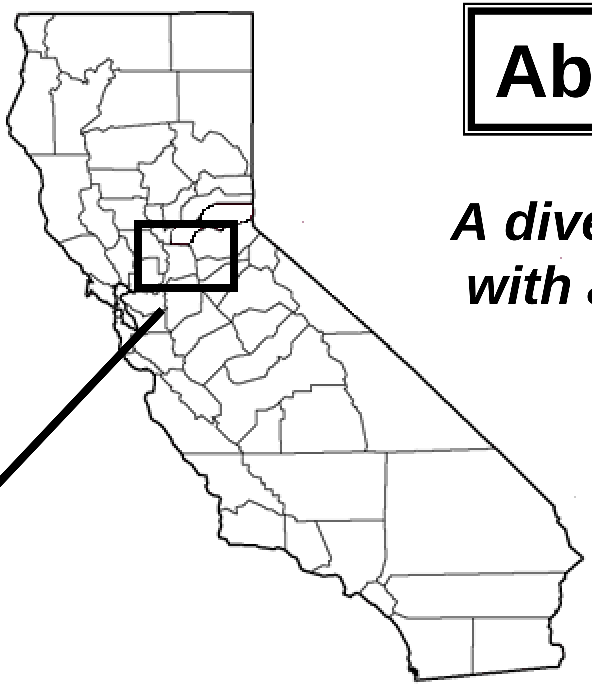
But…

A bad security program, on the other hand, has the power to ruin all your efforts

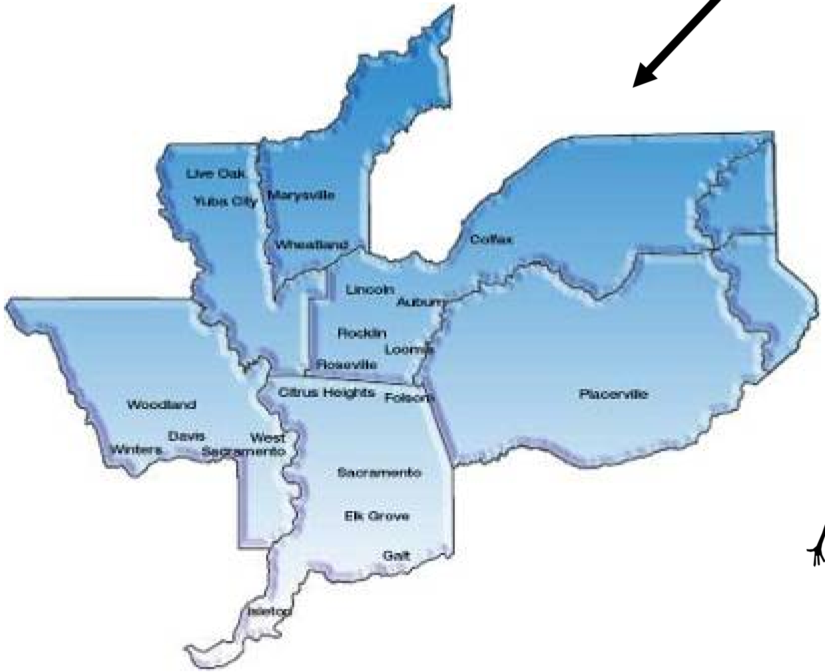
About us

The Sacramento County region

- ➢Projection: 2,340,000 by 2010.
- ➢28% are under age 18.
- ➢Patient visits to County clinics have increased 15% a year each of the last three years.



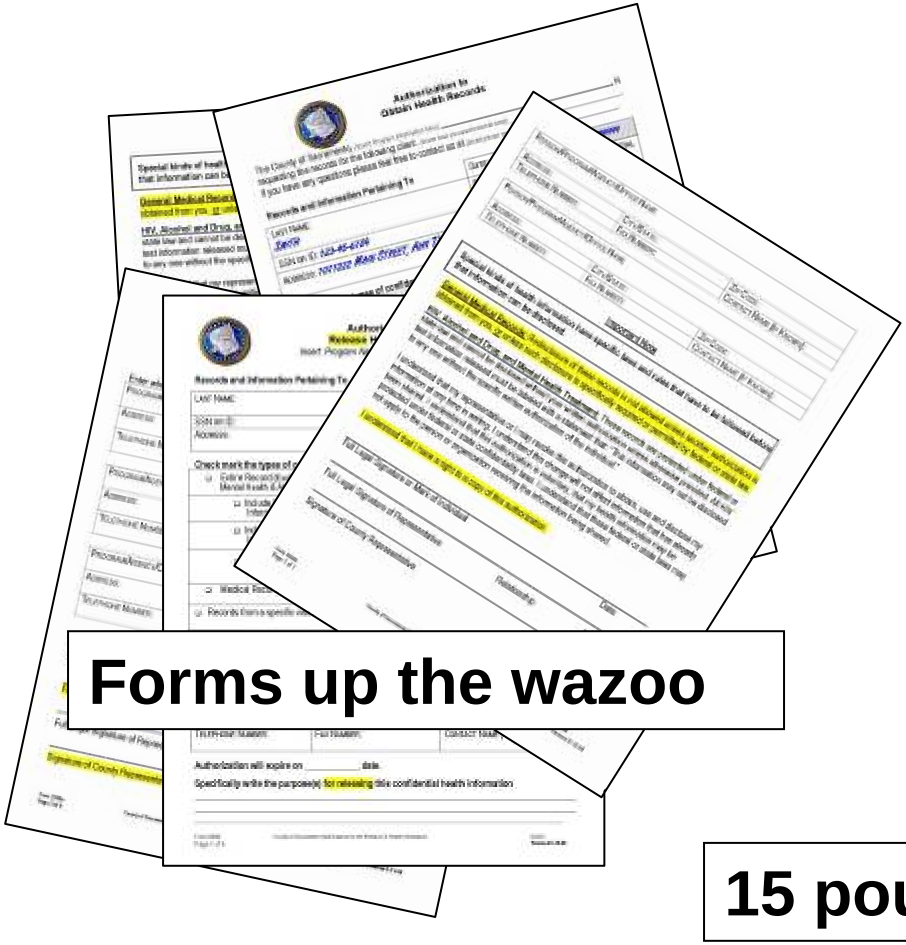
A diverse population with a growing need for health care



Sacramento County Government

- $3.5 Billion annual budget
- 13,500 employees
- 2,500 covered by HIPAA
- 67 work sites covered
- 250,000+ patient visits / year

We ‘rushed’ to compliance with the Privacy Rule



Forms up the wazoo

8 hours of talking head video training

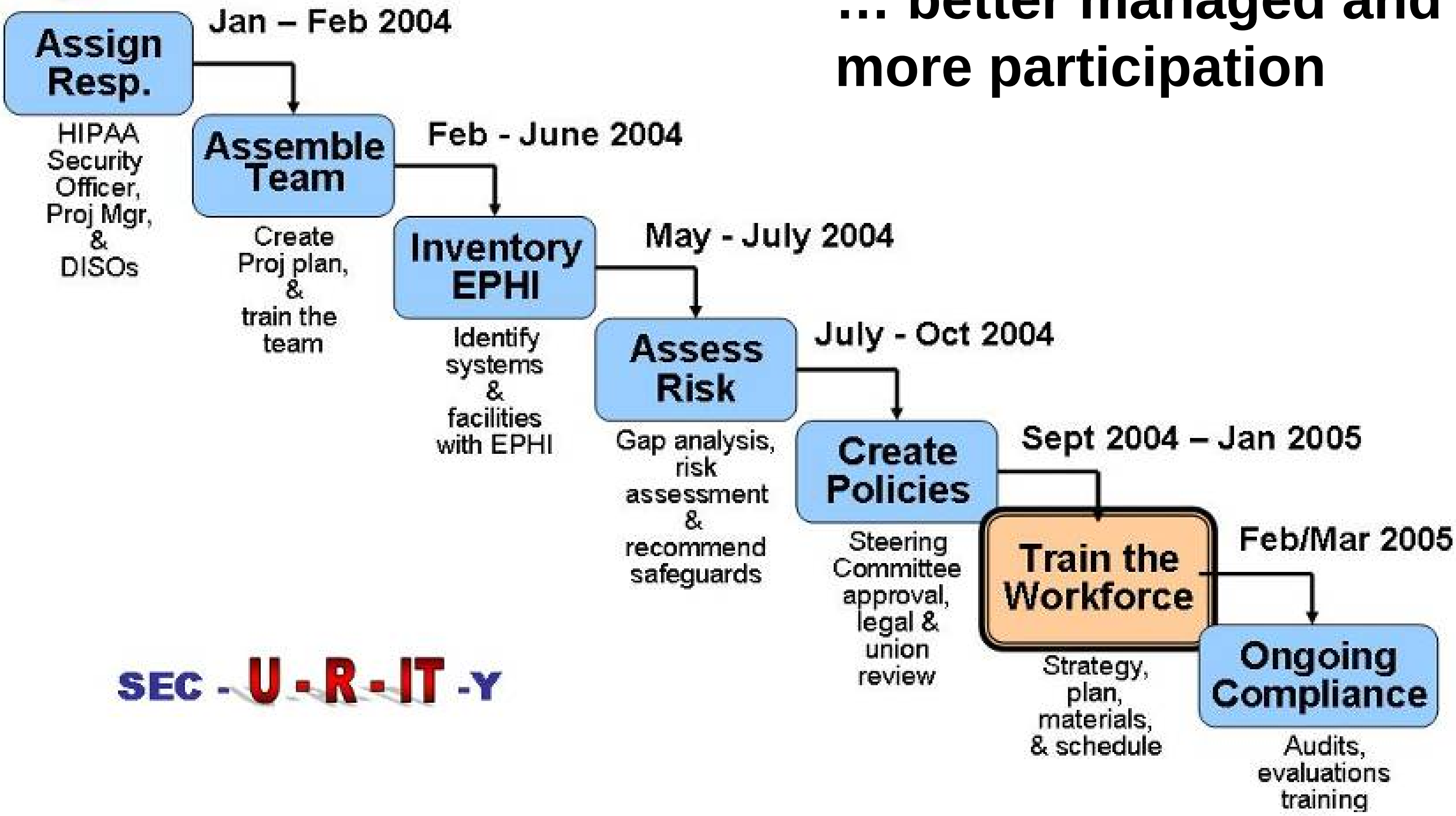
Training ad-nausea

OCR - 1
SAC - 0

15 pounds of policies

HIPAA Security Rule Project

… better managed and more participation



Assign Resp. Jan – Feb 2004

HIPAA Security Officer, Proj Mgr, & DISOs

Assemble Team Feb - June 2004

Create Proj plan, & train the team

Inventory EPHI May - July 2004

Identify systems & facilities with EPHI

Assess Risk July - Oct 2004

Gap analysis, risk assessment & recommend safeguards

Create Policies Sept 2004 – Jan 2005

Steering Committee approval, legal & union review

Train the Workforce Feb/Mar 2005

Strategy, plan, materials, & schedule

Ongoing Compliance

Audits, evaluations training

SEC - U - R - IT -Y

Information Security – Everyone's Responsibility

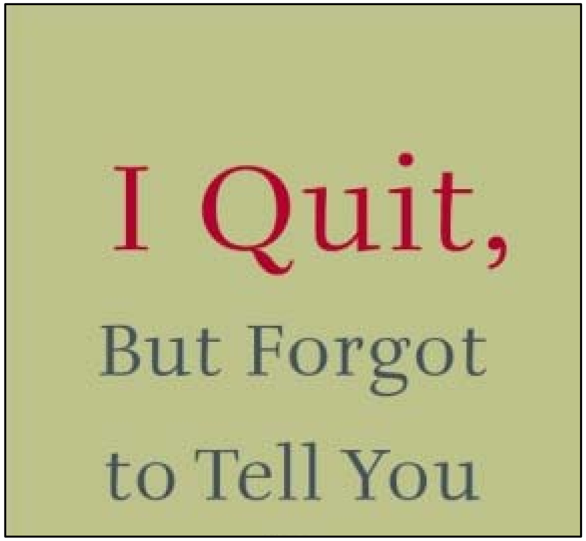
And we moved into ongoing audits, continual training, & incident mgt …

Compliance Report for 2005 - 2006

… but, then something happened

I looked around and saw how things had changed…

Lost interest, priority, support; complacent



I Quit,

But Forgot to Tell You

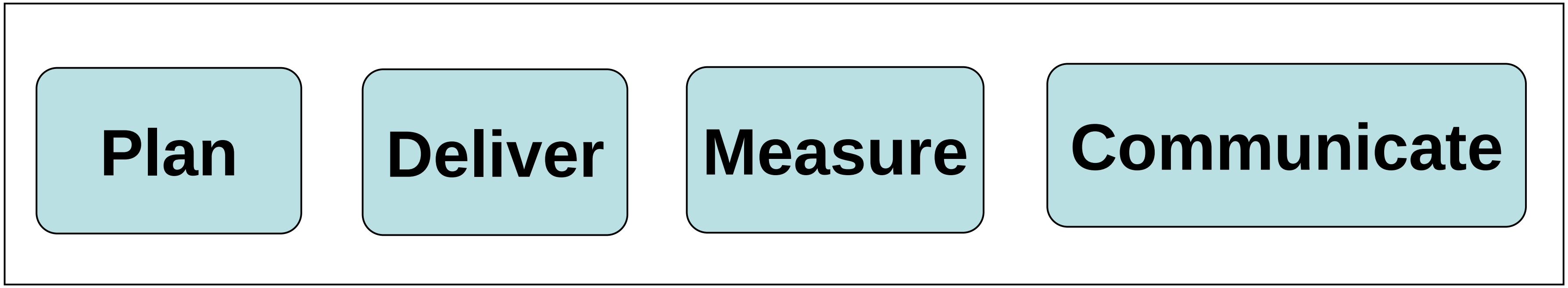
Staff turnover

Questioned why we worked on what we did

… and I saw the adversary within

Our problem: surprising, simple, but not unusual

I needed to (re)create a business case for security.



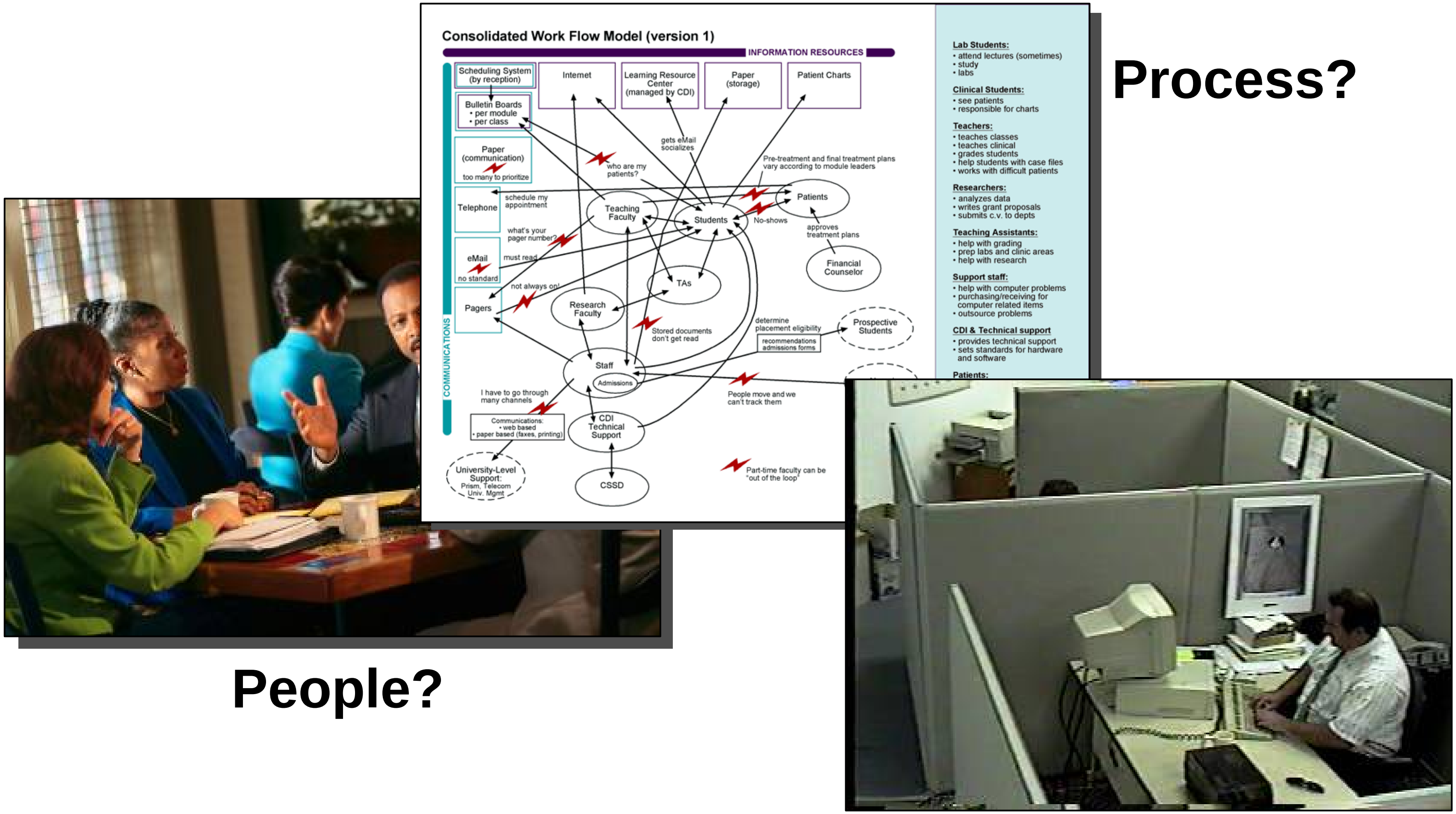
Plan

Deliver

Measure

Communicate

What do industry analysts say is the hottest security challenge?



Consolidated Work Flow Model (version 1)

Lab Students:
- attend lectures (sometimes)
- study
- labs

Clinical Students:
- see patients
- responsible for charts

Teachers:
- teaches classes
- teaches clinical
- grades students
- help students with case files
- works with difficult patients

Researchers:
- analyzes data
- writes grant proposals
- submits c.v. to depts

Teaching Assistants:
- help with grading
- prep labs and clinic areas
- help with research

Support staff:
- help with computer problems
- purchasing/receiving for computer related items
- outsource problems

CDI & Technical support
- provides technical support
- sets standards for hardware and software

Patients:

Process?

People?

Technology?

Conclusion: There is no quick fix

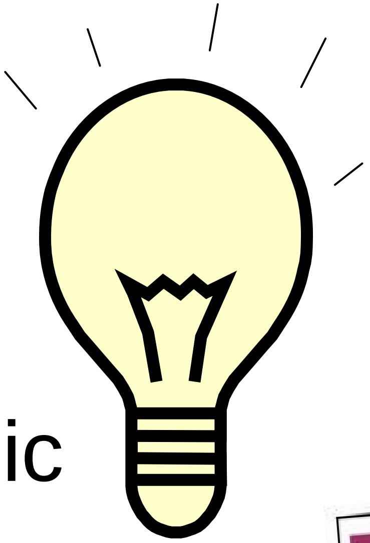
Areas I need to work on:

- – Governance
- – Risk Management
- – Metrics

Things I need to do:

- – Enforce existing policies
- – Share best practices

My Big A-HA!

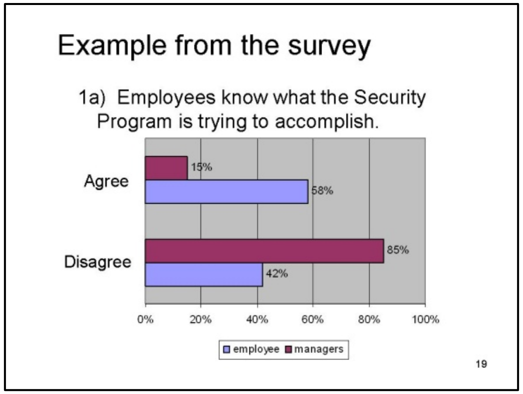


- This is similar to business strategic planning.
- A similar process could be used to plan, execute, and communicate

County of Sacramento
Information Technology Plan
2006
March 28, 2006

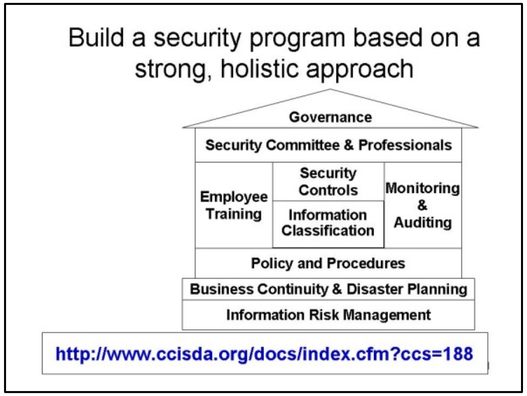
http://www.saccounty.net/itpb/it-plan/index.html.

Armed with this realization, I took action:


Example from the survey

1a) Employees know what the Security Program is trying to accomplish.

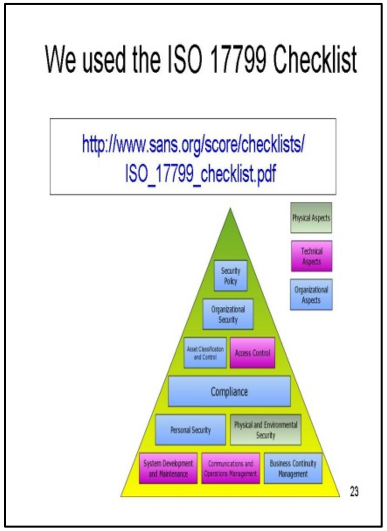
1. survey employees


Build a security program based on a strong, holistic approach

Governance
Security Committee & Professionals
Employee Training
Security Controls
Information Classification
Monitoring & Auditing
Policy and Procedures
Business Continuity & Disaster Planning
Information Risk Management

http://www.ccisda.org/docs/index.cfm?ccs=188

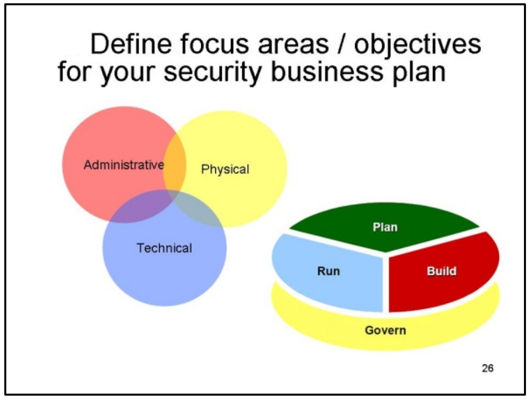
2. model for structure


We used the ISO 17799 Checklist

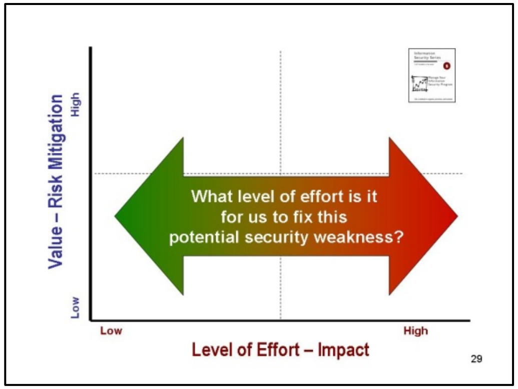
http://www.sans.org/score/checklists/ISO_17799_checklist.pdf

Physical Aspects
Technical Aspects
Organizational Aspects
Security Policy
Organizational Security
Asset Classification and Control
Access Control
Compliance
Personal Security
Physical and Environmental Security
System Development and Maintenance
Communications and Operations Management
Business Continuity Management
23

3. self program audit


Define focus areas / objectives for your security business plan

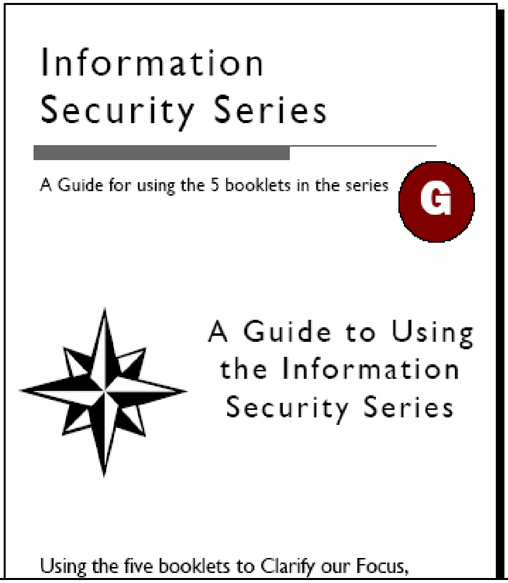
4. define focus areas



Value – Risk Mitigation
High
Low
What level of effort is it for us to fix this potential security weakness?
Low
High
Level of Effort – Impact
29

5. a method to manage

Why on earth haven’t more ISOs who struggle with their security been told this?



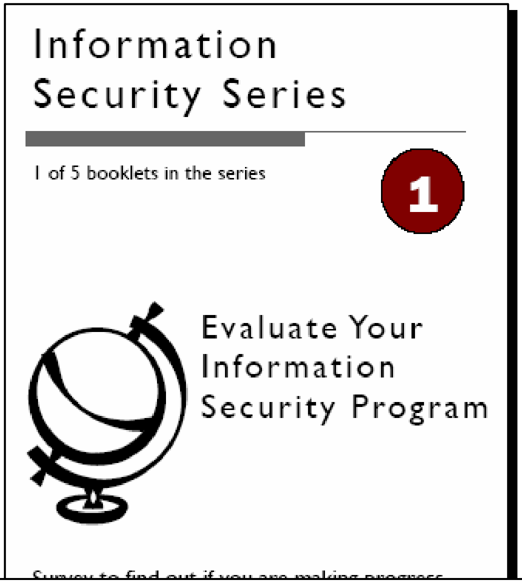
Information Security Series

A Guide for using the 5 booklets in the series

G

A Guide to Using the Information Security Series

Using the five booklets to Clarify our Focus,



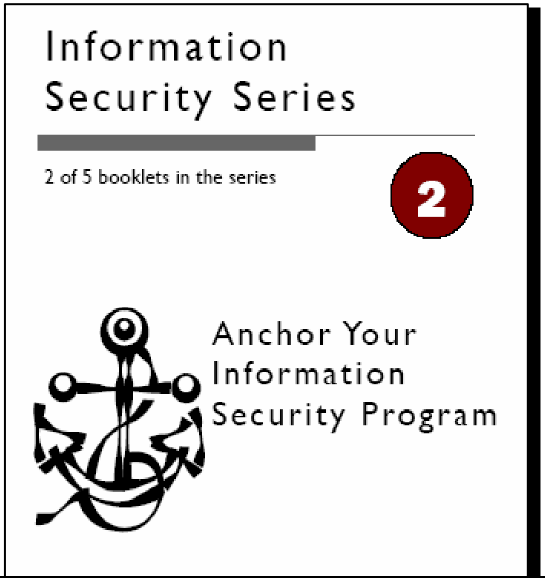
Information Security Series

1 of 5 booklets in the series

1

Evaluate Your Information Security Program

Survey to find out if you are making progress



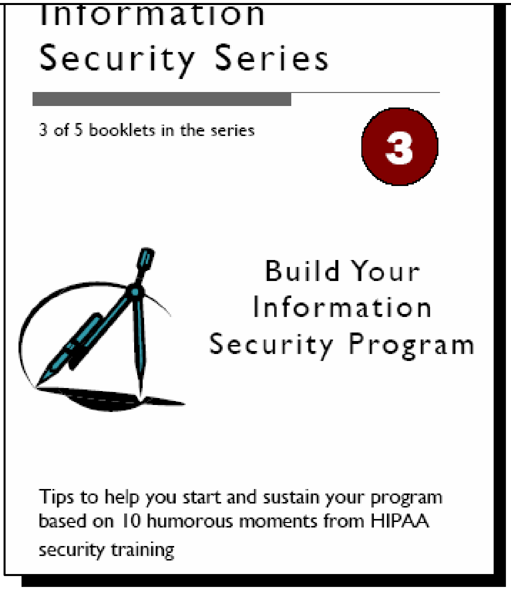
Information Security Series

2 of 5 booklets in the series

2

Anchor Your Information Security Program

www.ocit.saccounty.net/InformationSecurity/index.htm



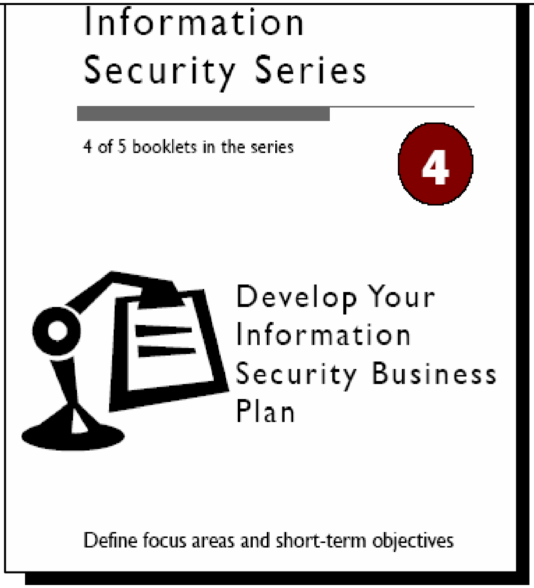
Information Security Series

3 of 5 booklets in the series

3

Build Your Information Security Program

Tips to help you start and sustain your program based on 10 humorous moments from HIPAA security training



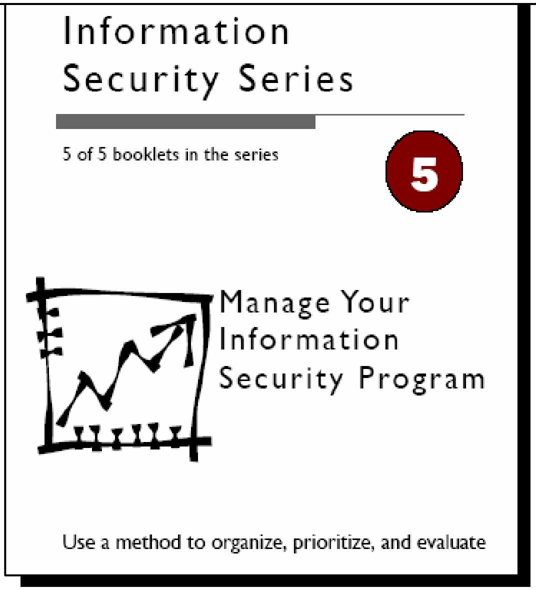
Information Security Series

4 of 5 booklets in the series

4

Develop Your Information Security Business Plan

Define focus areas and short-term objectives



Information Security Series

5 of 5 booklets in the series

5

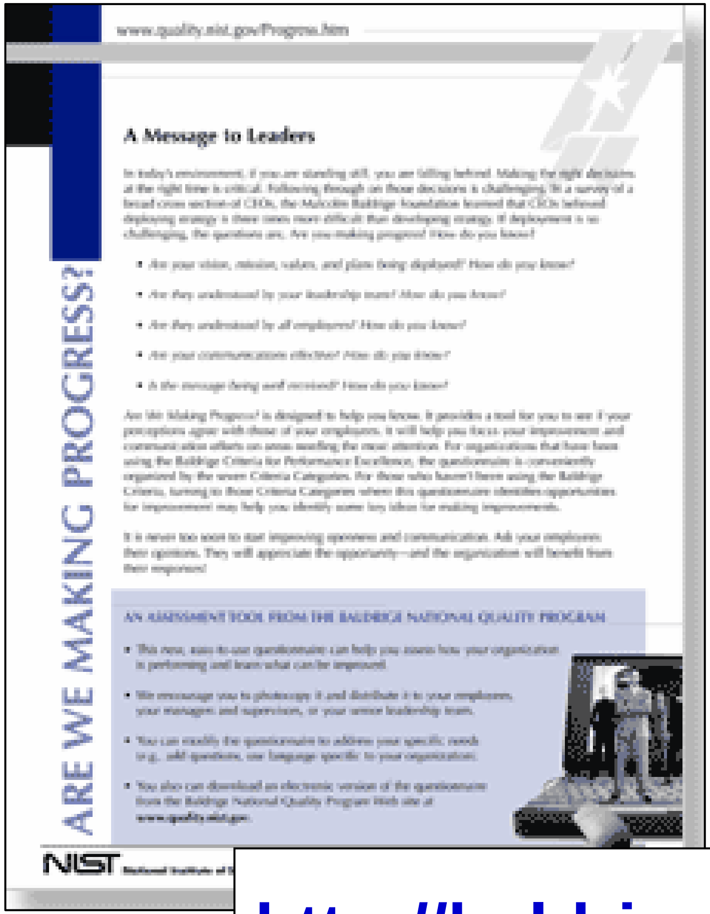
Manage Your Information Security Program

Use a method to organize, prioritize, and evaluate

1. Evaluate from the perspective of managers and employees

- Leadership
- Planning
- Customer focus
- Measurement
- Human resource focus
- Process management
- Business results

Get ‘actionable’ feedback



www.quality.nist.gov/Progress.htm

ARE WE MAKING PROGRESS?

A Message to Leaders

In today's environment, if you are standing still, you are falling behind. Making the right decisions at the right time is critical. Following through on those decisions is challenging. In a survey of a broad cross section of CEOs, the Malcolm Baldrige Foundation learned that CEOs believed deploying strategy is three times more difficult than developing strategy. If deployment is so challenging, the questions are, Are you making progress? How do you know?

- *Are your vision, mission, values, and plans being deployed? How do you know?*
- *Are they understood by your leadership team? How do you know?*
- *Are they understood by all employees? How do you know?*
- *Are your communications effective? How do you know?*
- *Is the message being well received? How do you know?*

Are We Making Progress? is designed to help you know. It provides a tool for you to see if your perceptions agree with those of your employees. It will help you focus your improvement and communication efforts on areas needing the most attention. For organizations that have been using the Baldrige Criteria for Performance Excellence, the questionnaire is conveniently organized by the seven Criteria Categories. For those who haven't been using the Baldrige Criteria, turning to those Criteria Categories where this questionnaire identifies opportunities for improvement may help you identify some key ideas for making improvements.

It is never too soon to start improving openness and communication. Ask your employees their opinions. They will appreciate the opportunity—and the organization will benefit from their responses!

AN ASSESSMENT TOOL FROM THE BALDRIGE NATIONAL QUALITY PROGRAM

- This new, easy-to-use questionnaire can help you assess how your organization is performing and learn what can be improved.
- We encourage you to photocopy it and distribute it to your employees, your managers and supervisors, or your senior leadership team.
- You can modify the questionnaire to address your specific needs (e.g., add questions, use language specific to your organization).
- You also can download an electronic version of the questionnaire from the Baldrige National Quality Program Web site at **www.quality.nist.gov**.

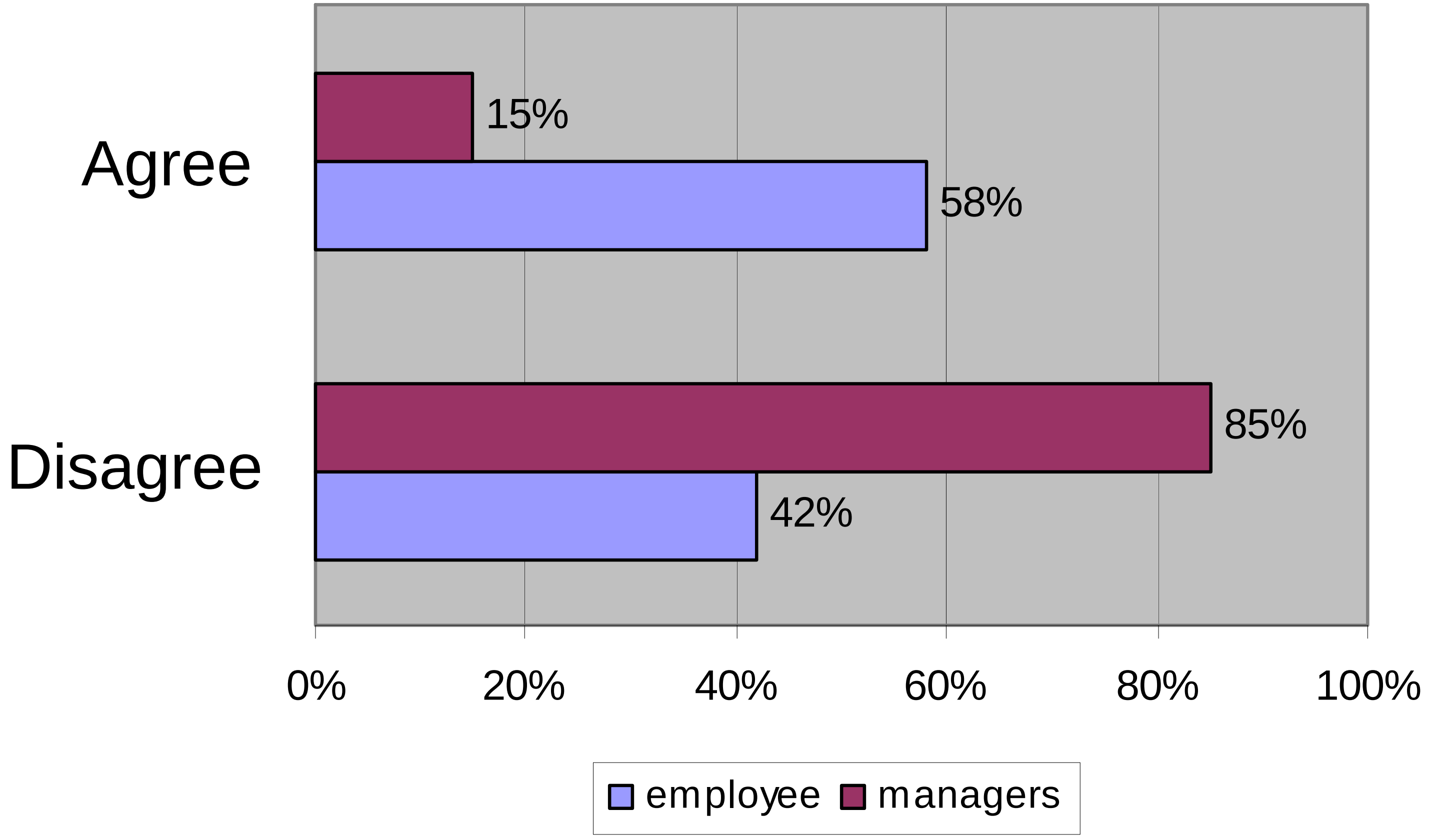
NIST National Institute of S

I adapted a best practices survey for our security program

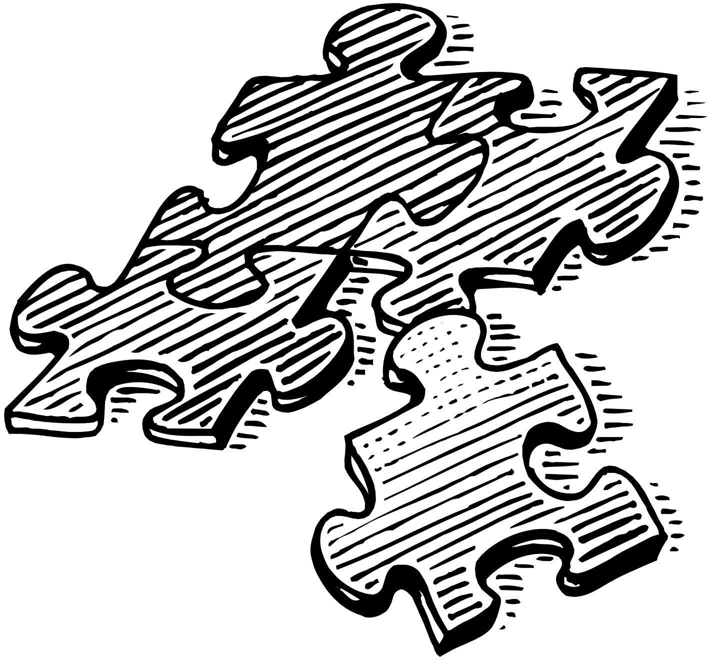
http://baldrige.nist.gov/Progress.htm

Example from the survey

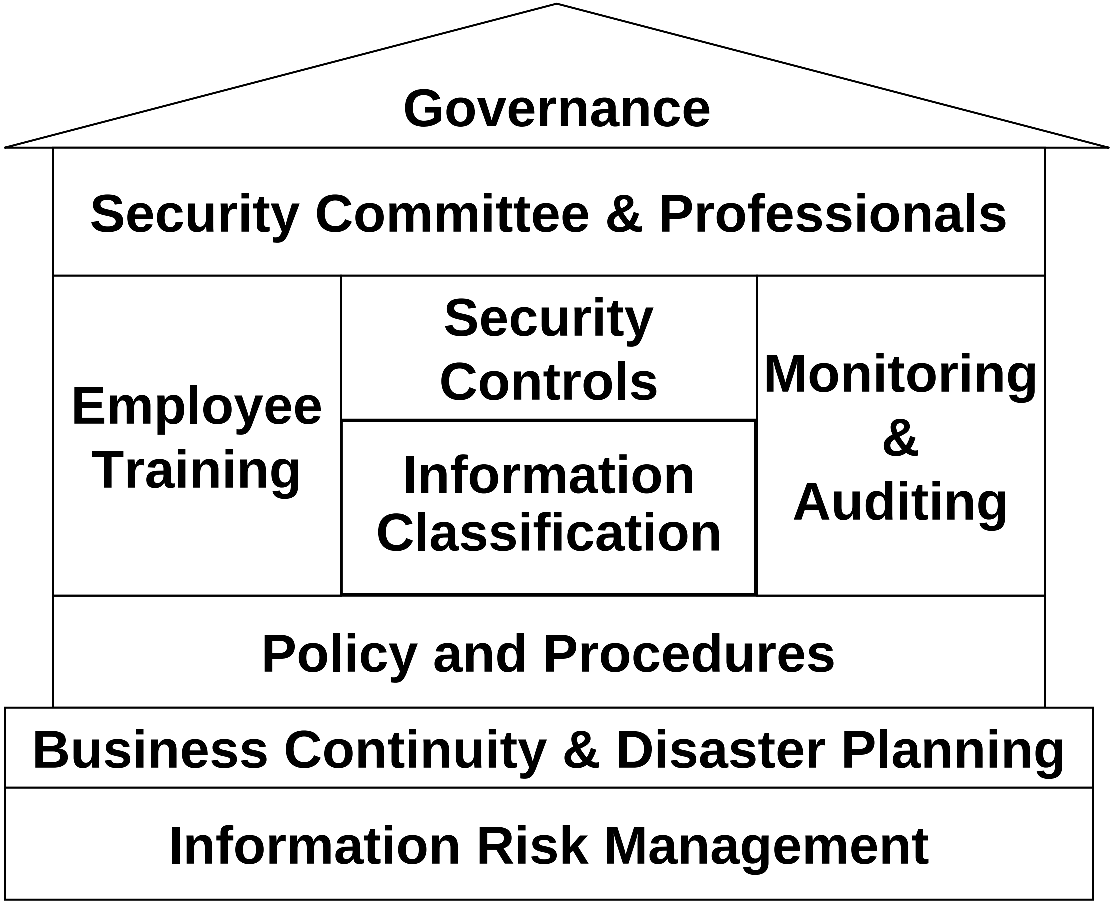
1a) Employees know what the Security Program is trying to accomplish.



2. I needed a structured program to fit the puzzle pieces all together



Build a security program based on a strong, holistic approach



Governance

Security Committee & Professionals

Employee Training

Security Controls

Information Classification

Monitoring & Auditing

Policy and Procedures

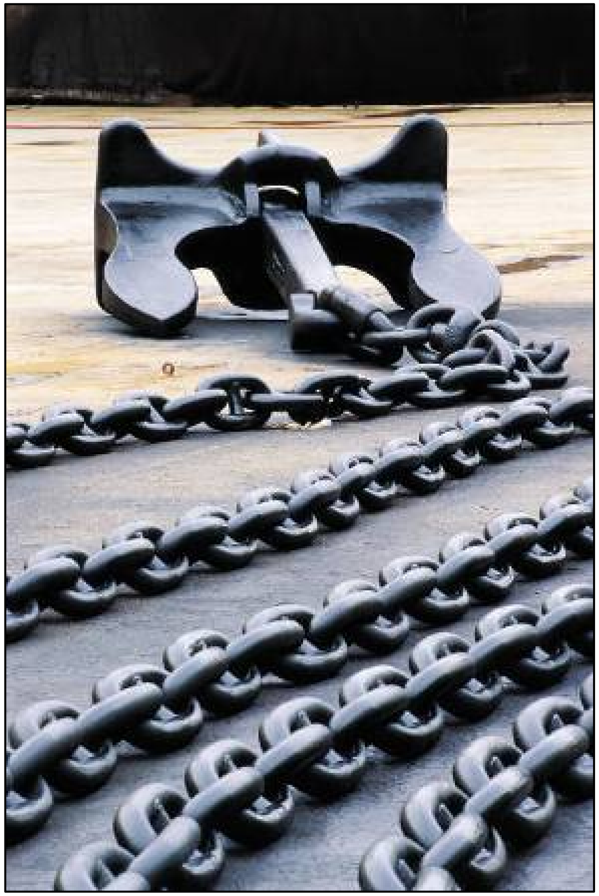
Business Continuity & Disaster Planning

Information Risk Management

http://www.ccisda.org/docs/index.cfm?ccs=188

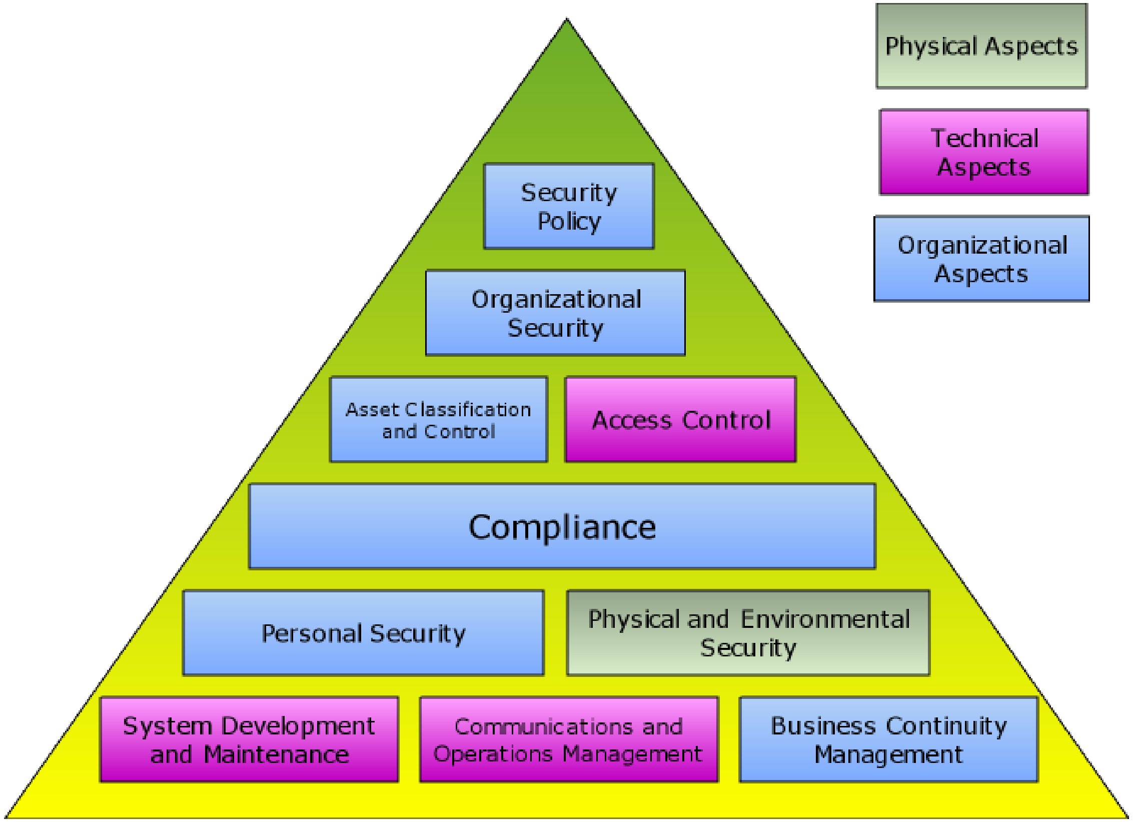
3. I took the best next step to anchor my security program

Conduct a self-audit assessment determine gap with generally accepted best practice



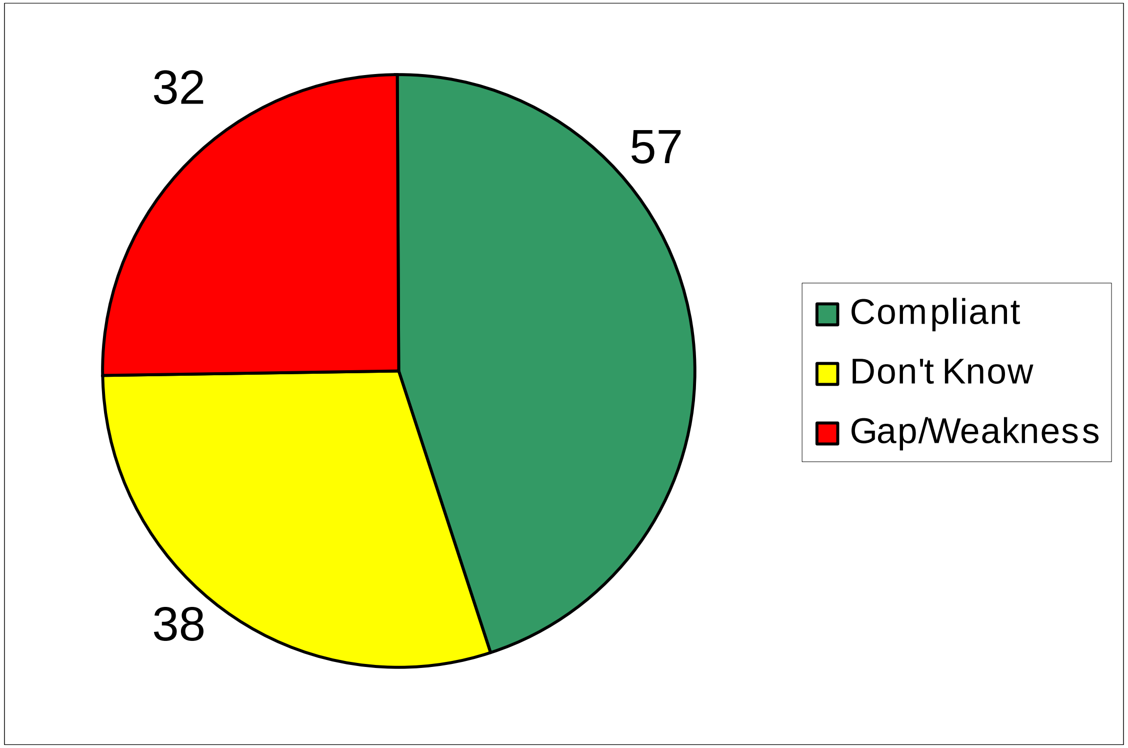
We used the ISO 17799 Checklist

http://www.sans.org/score/checklists/ISO_17799_checklist.pdf

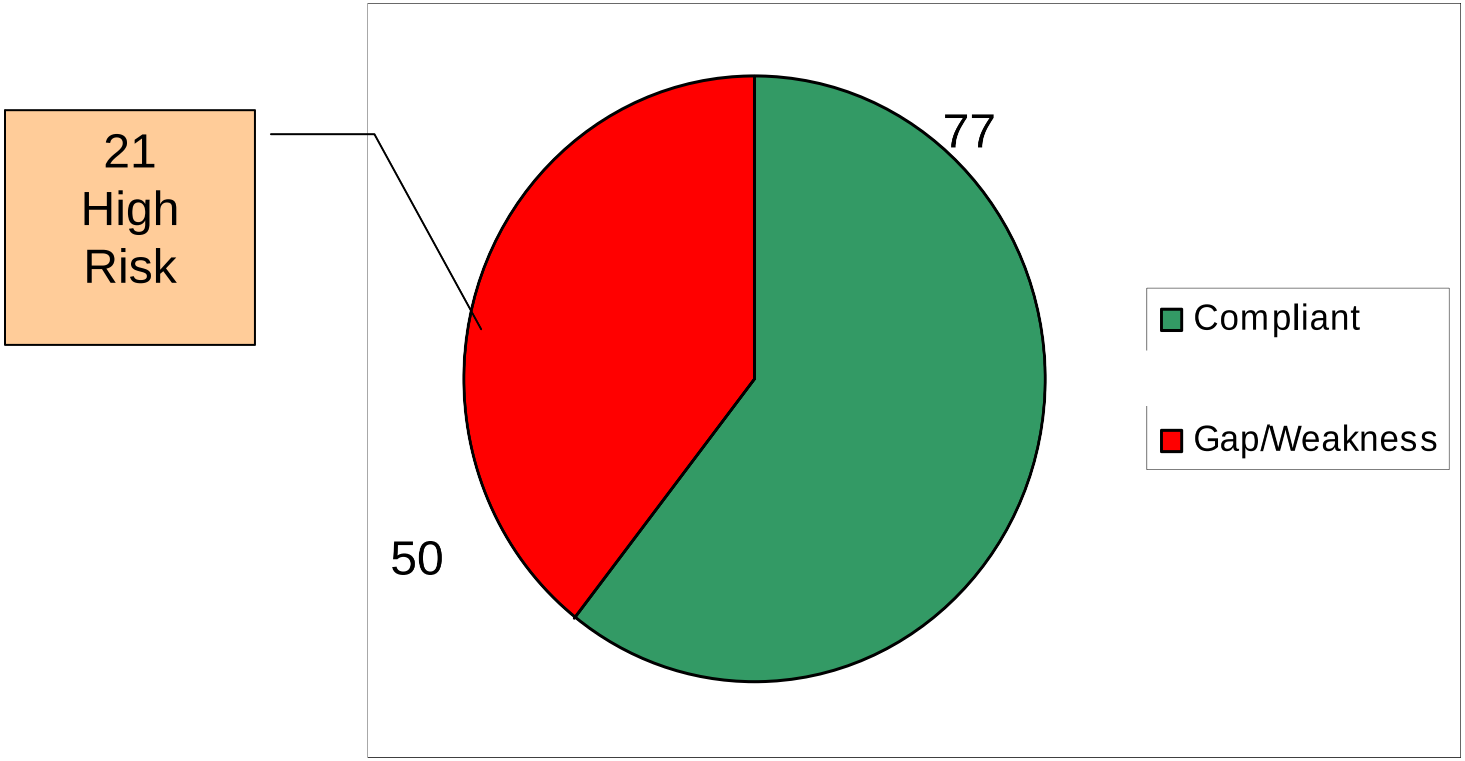

Physical Aspects
Technical Aspects
Organizational Aspects
Security Policy
Organizational Security
Asset Classification and Control
Access Control
Compliance
Personal Security
Physical and Environmental Security
System Development and Maintenance
Communications and Operations Management
Business Continuity Management

ISO 17799 Audit Initial Results

10 audit topics – 127 individual items

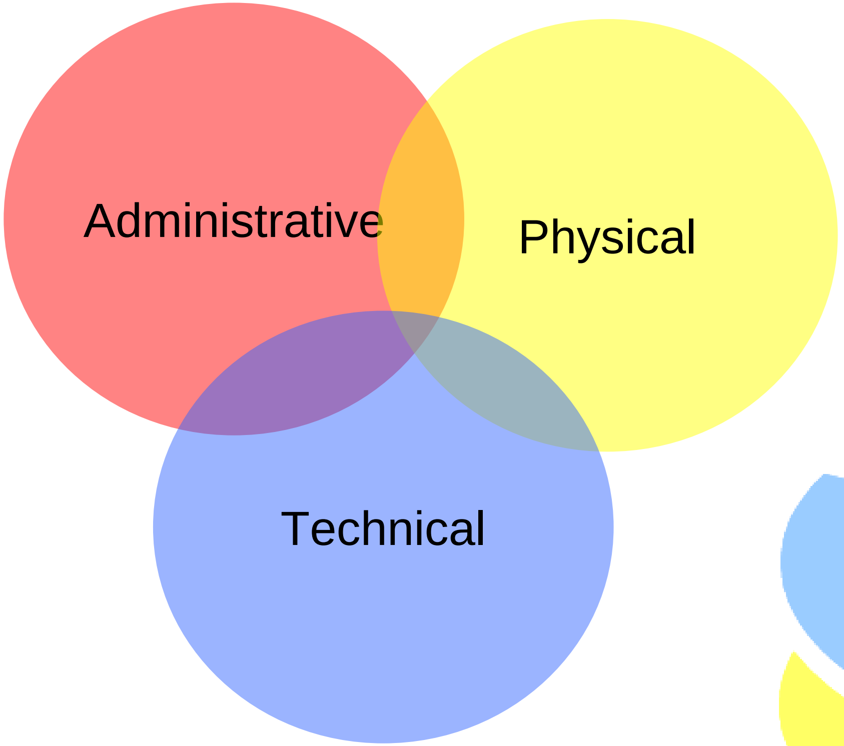


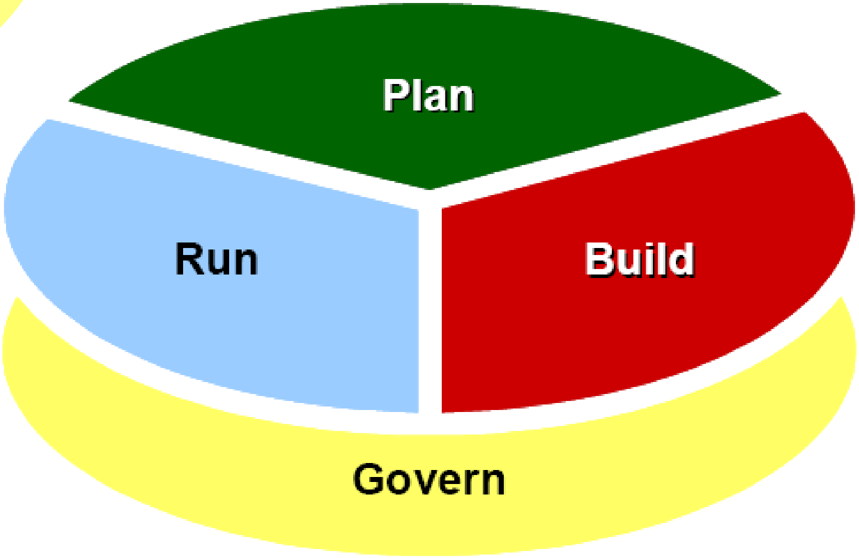
Audit Final Results



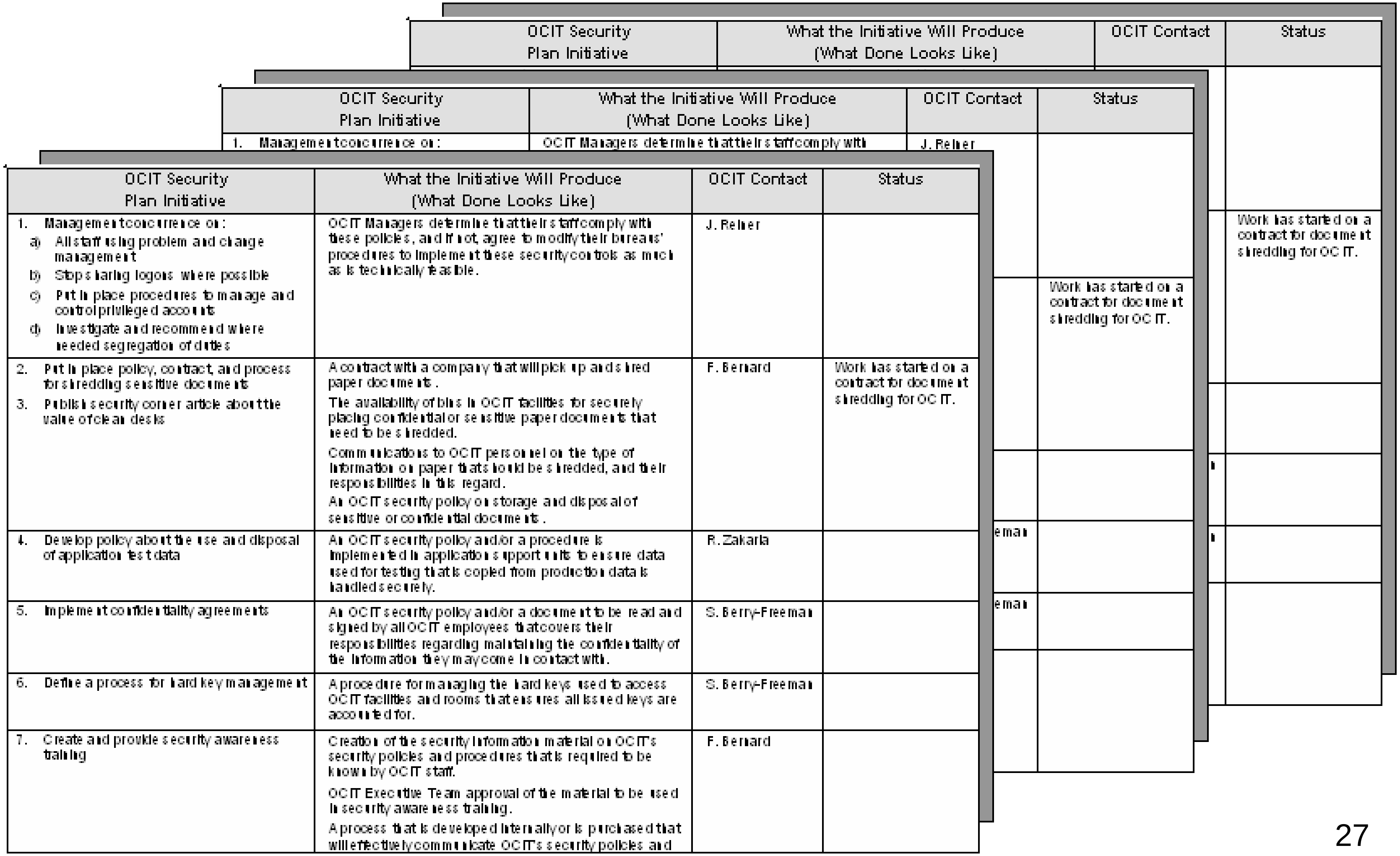
21
High
Risk

4. Define focus areas / objectives for your security business plan

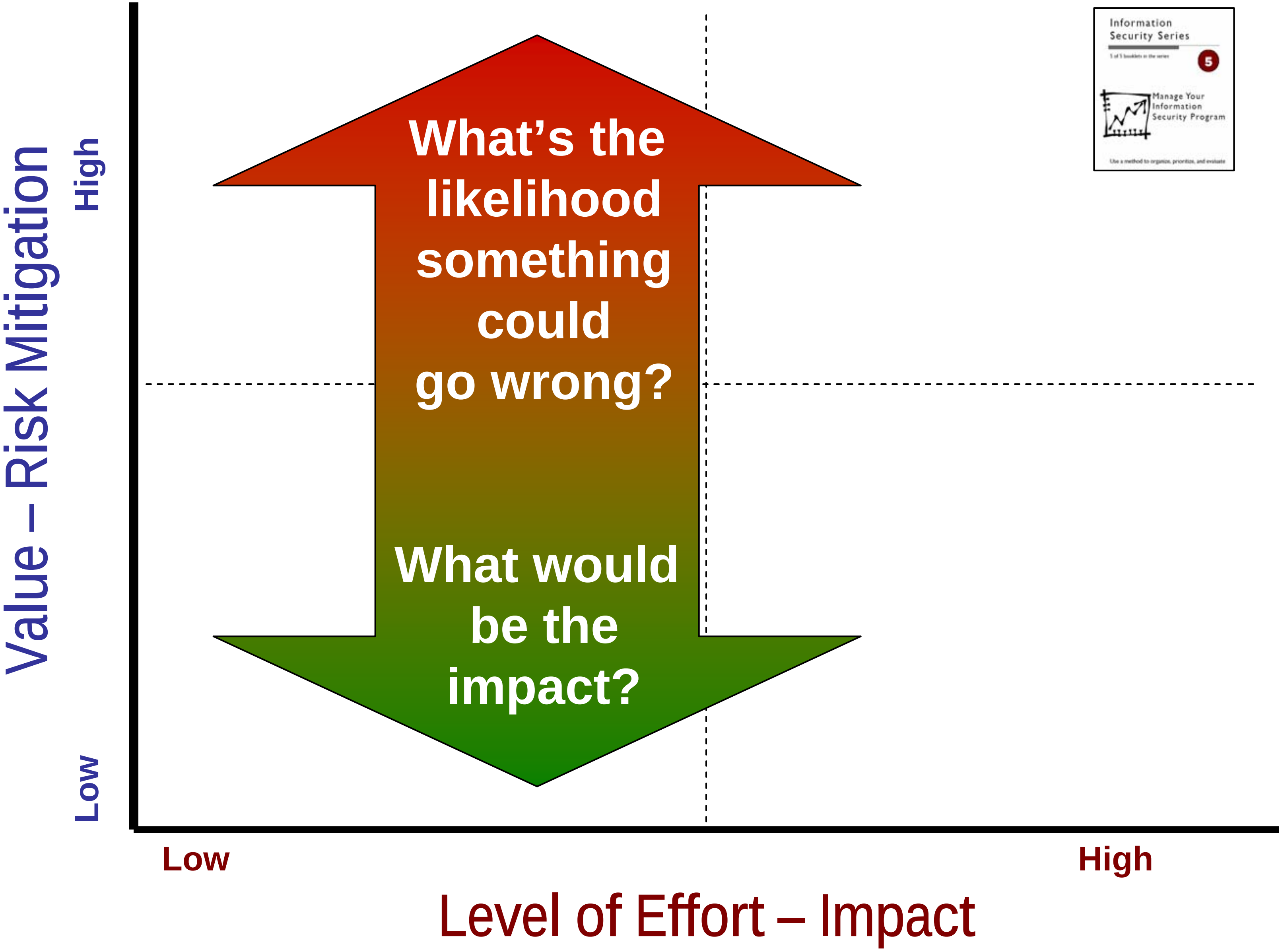




5. Use a method to organize, prioritize, and evaluate the program



OCIT Security Plan Initiative	What the Initiative Will Produce (What Done Looks Like)	OCIT Contact	Status
1. Management concurrence on: a) All staff using problem and change management b) Stop sharing logons where possible c) Put in place procedures to manage and control privileged accounts d) Investigate and recommend where needed segregation of duties	OCIT Managers determine that their staff comply with these policies, and if not, agree to modify their bureaus' procedures to implement these security controls as much as is technically feasible.	J. Reiner	
2. Put in place policy, contract, and process for shredding sensitive documents 3. Publish security corner article about the value of clean desks	A contract with a company that will pick up and shred paper documents. The availability of bins in OCIT facilities for securely placing confidential or sensitive paper documents that need to be shredded. Communications to OCIT personnel on the type of information on paper that should be shredded, and their responsibilities in this regard. An OCIT security policy on storage and disposal of sensitive or confidential documents.	F. Bernard	Work has started on a contract for document shredding for OCIT.
4. Develop policy about the use and disposal of application test data	An OCIT security policy and/or a procedure is implemented in application support units to ensure data used for testing that is copied from production data is handled securely.	R. Zakaria	
5. Implement confidentiality agreements	An OCIT security policy and/or a document to be read and signed by all OCIT employees that covers their responsibilities regarding maintaining the confidentiality of the information they may come in contact with.	S. Berry-Freeman	
6. Define a process for hard key management	A procedure for managing the hard keys used to access OCIT facilities and rooms that ensures all issued keys are accounted for.	S. Berry-Freeman	
7. Create and provide security awareness training	Creation of the security information material on OCIT's security policies and procedures that is required to be known by OCIT staff. OCIT Executive Team approval of the material to be used in security awareness training. A process that is developed internally or is purchased that will effectively communicate OCIT's security policies and	F. Bernard	



What's the likelihood something could go wrong?

What would be the impact?

Value – Risk Mitigation

High

Low

Low

High

Level of Effort – Impact

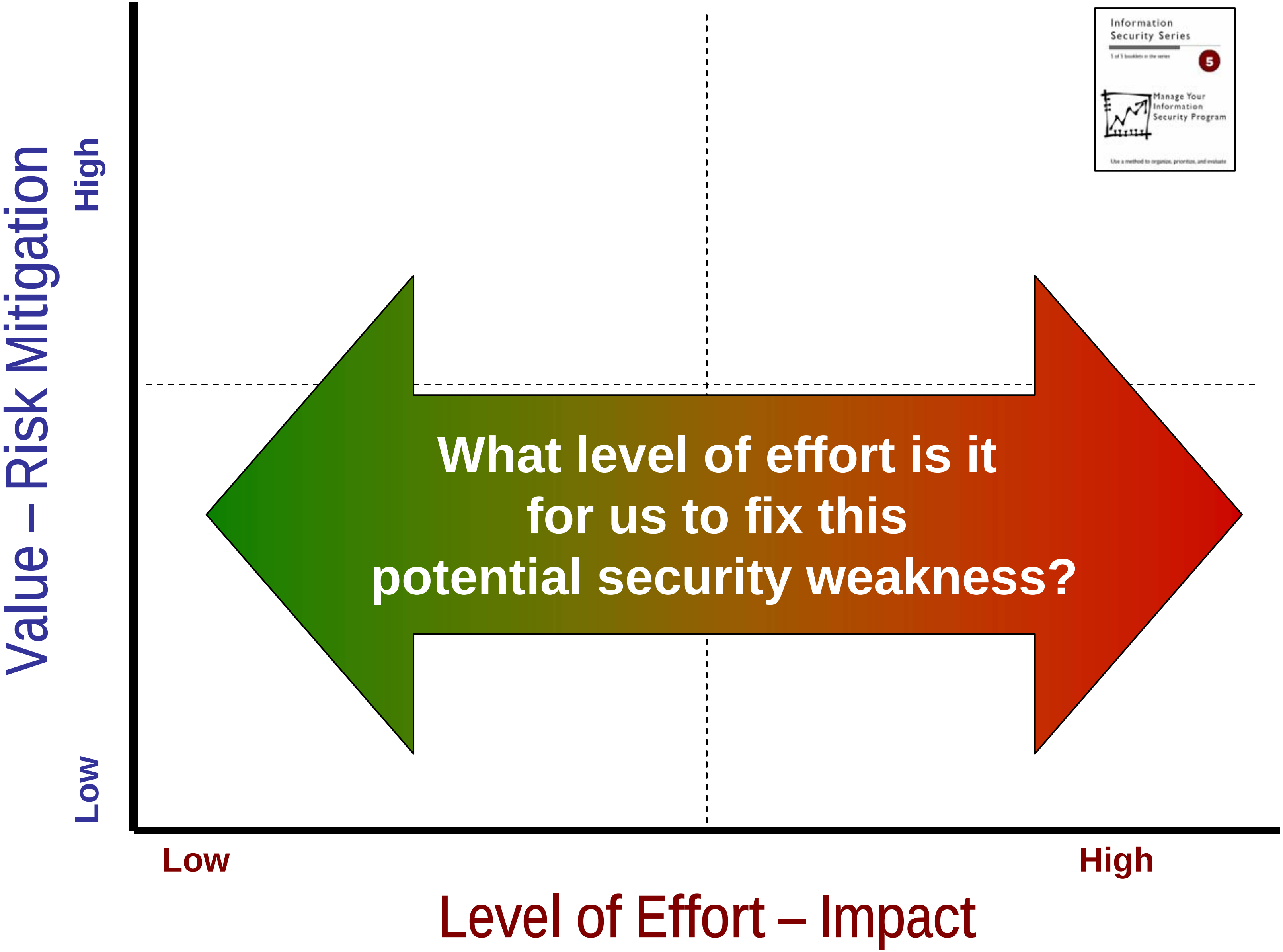
Information Security Series

5 of 5 booklets in the series

5

Manage Your Information Security Program

Use a method to organize, prioritize, and evaluate



Value – Risk Mitigation

High

Low

What level of effort is it
for us to fix this
potential security weakness?

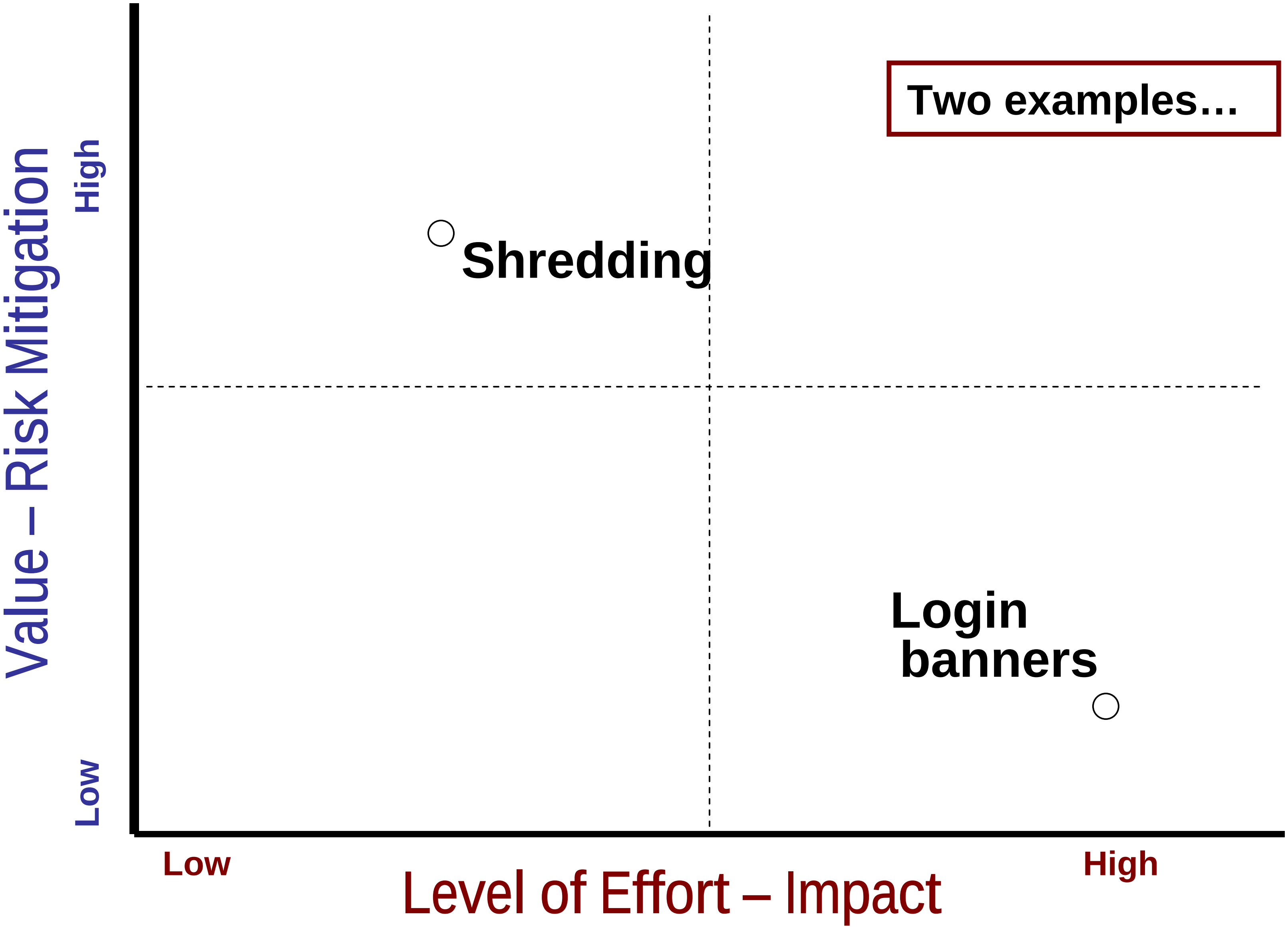
Low

High

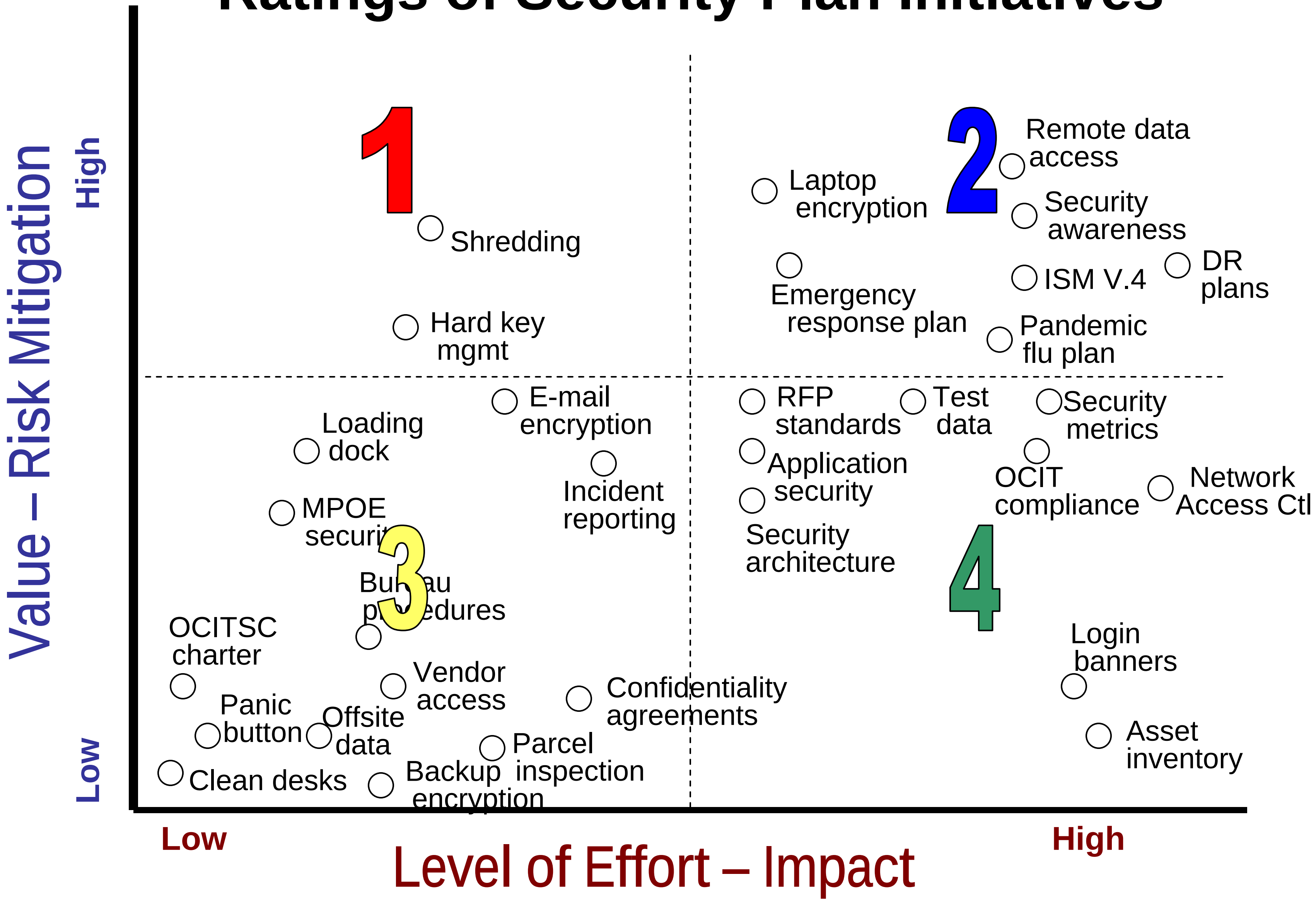
Level of Effort – Impact

Information
Security Series
5 of 5 booklets in the series
5
Manage Your
Information
Security Program
Use a method to organize, prioritize, and evaluate

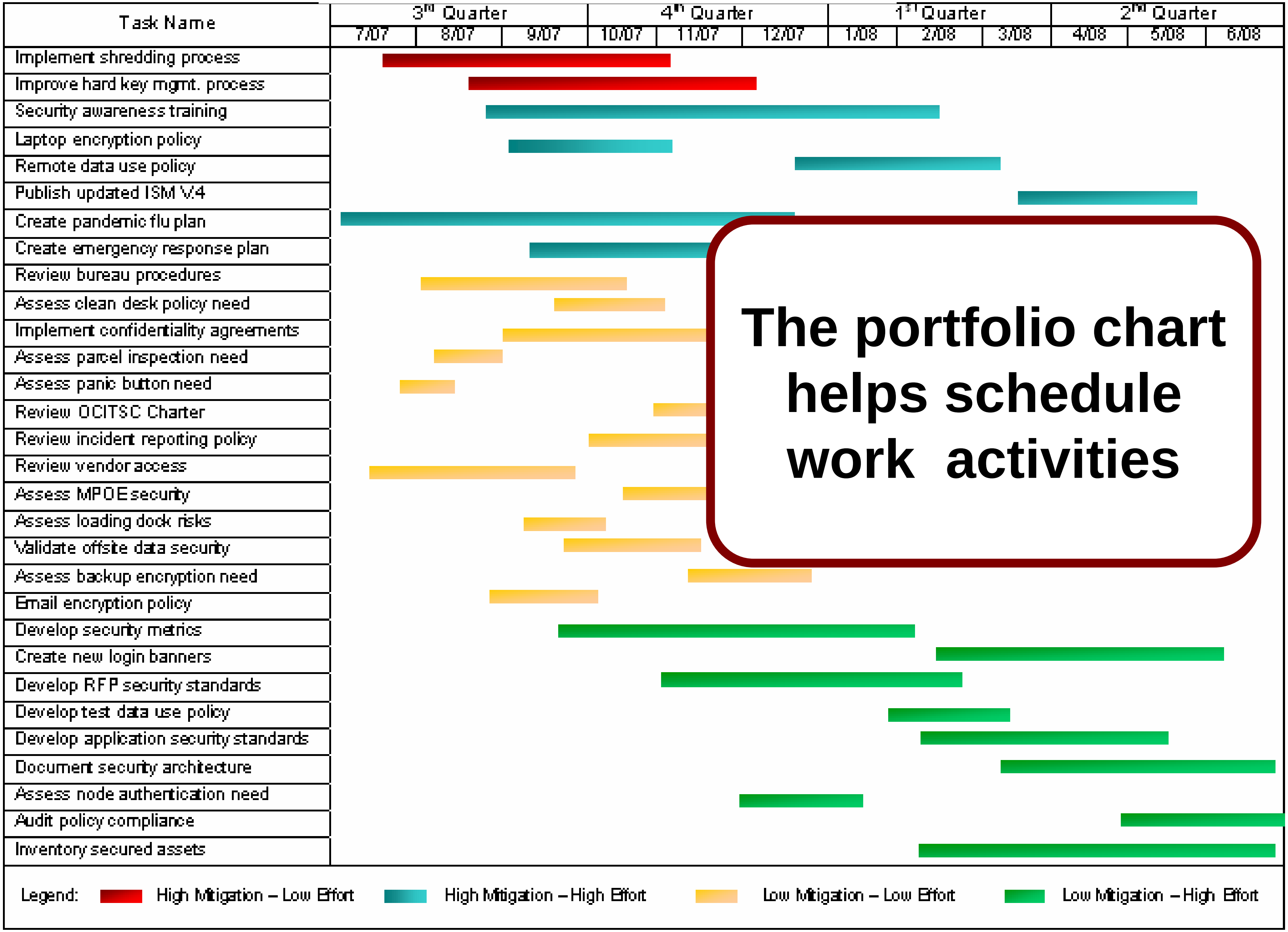
Two examples…



Ratings of Security Plan Initiatives

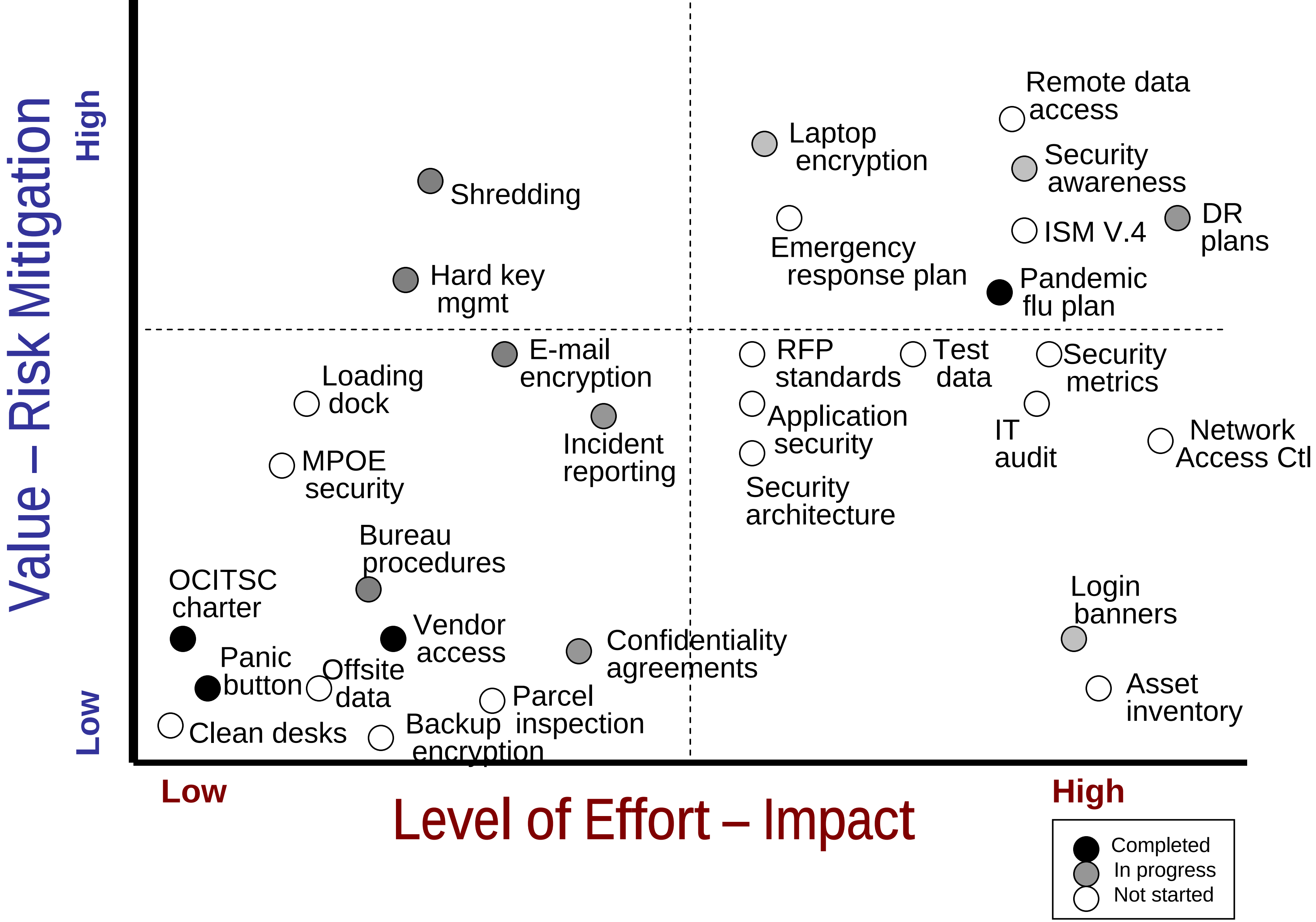


2007 security plan draft schedule

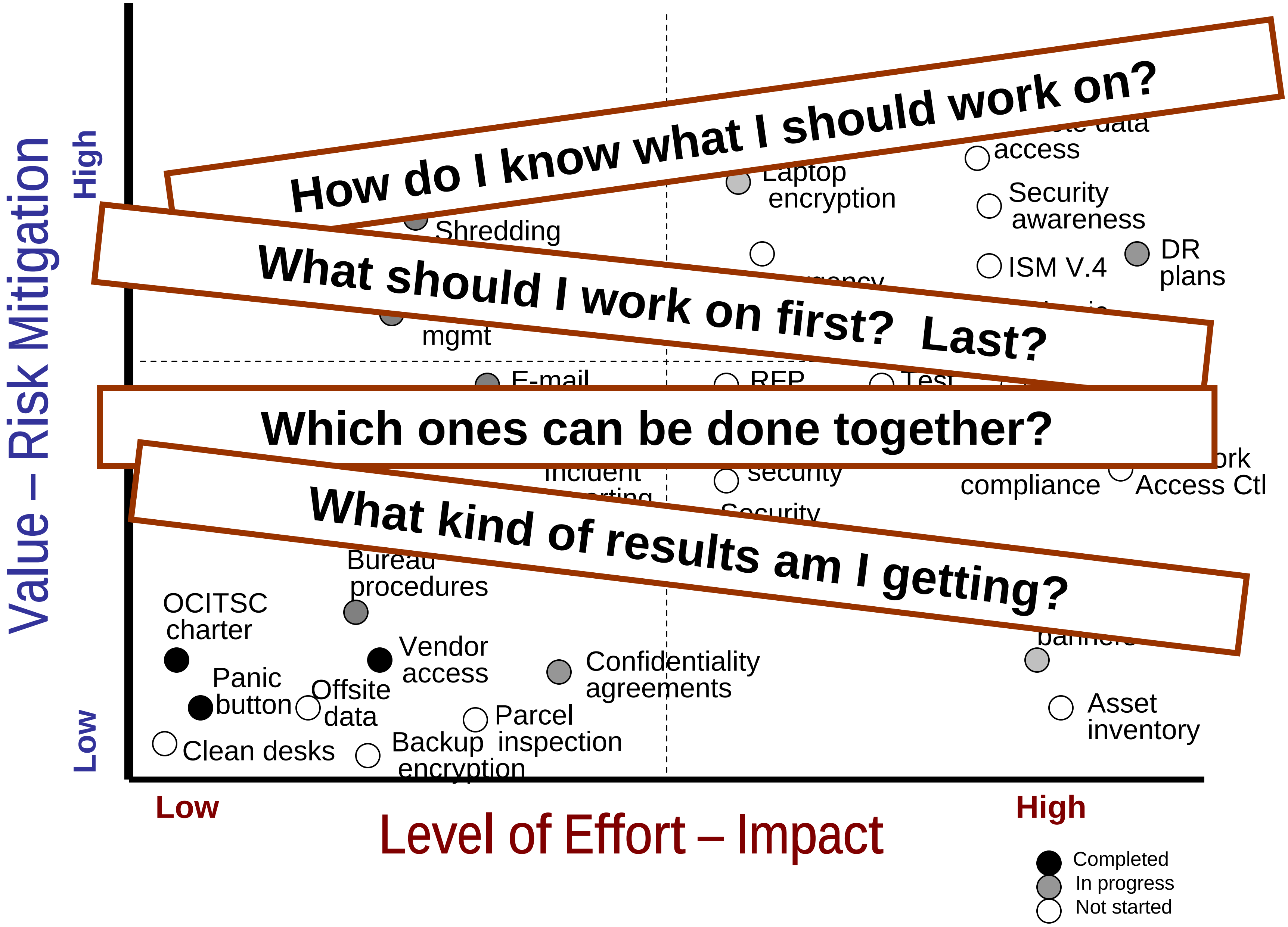


The portfolio chart helps schedule work activities

Managing the 2007 Security Plan



What kind of questions does this help you answer?



How do I know what I should work on?

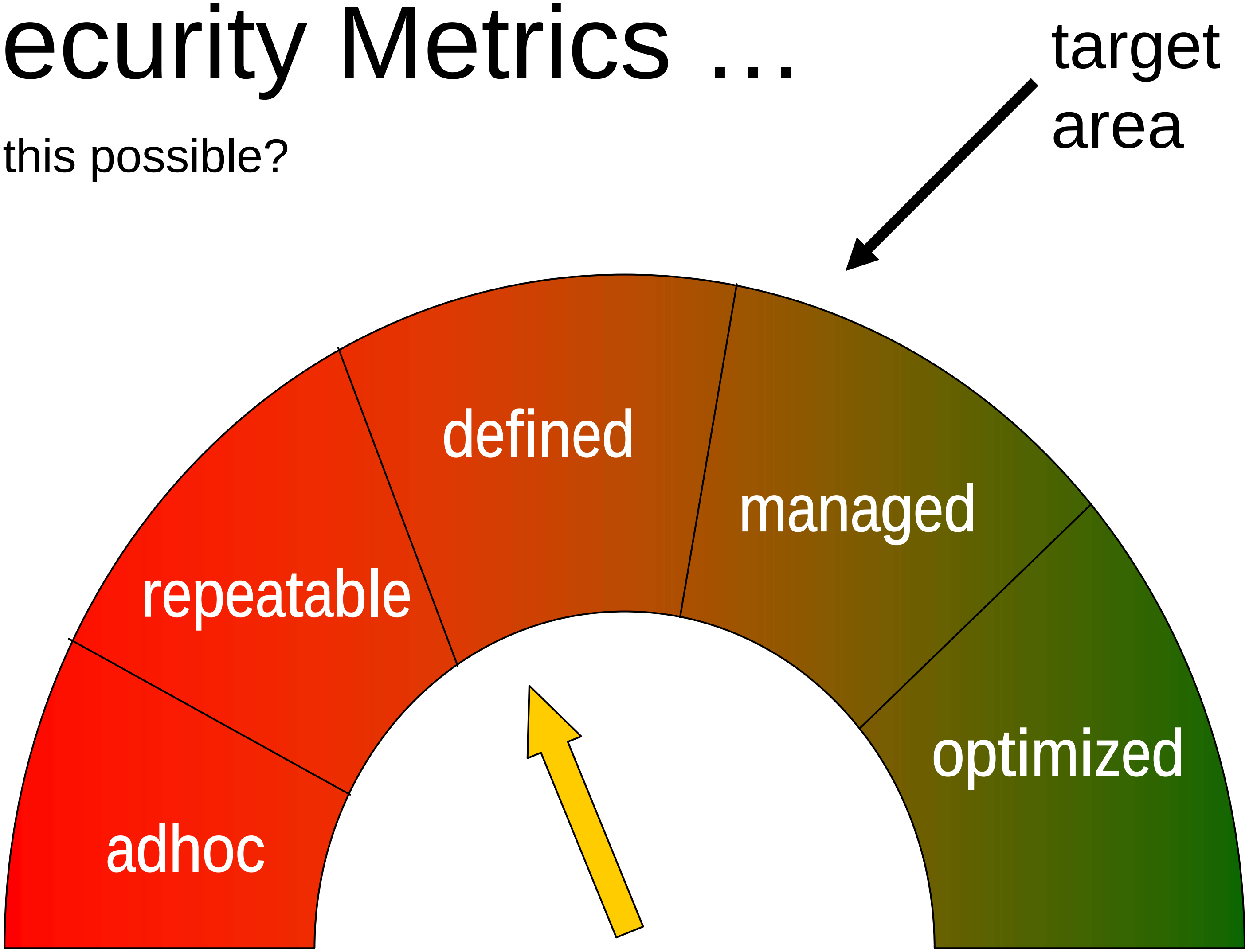
What should I work on first? Last?

Which ones can be done together?

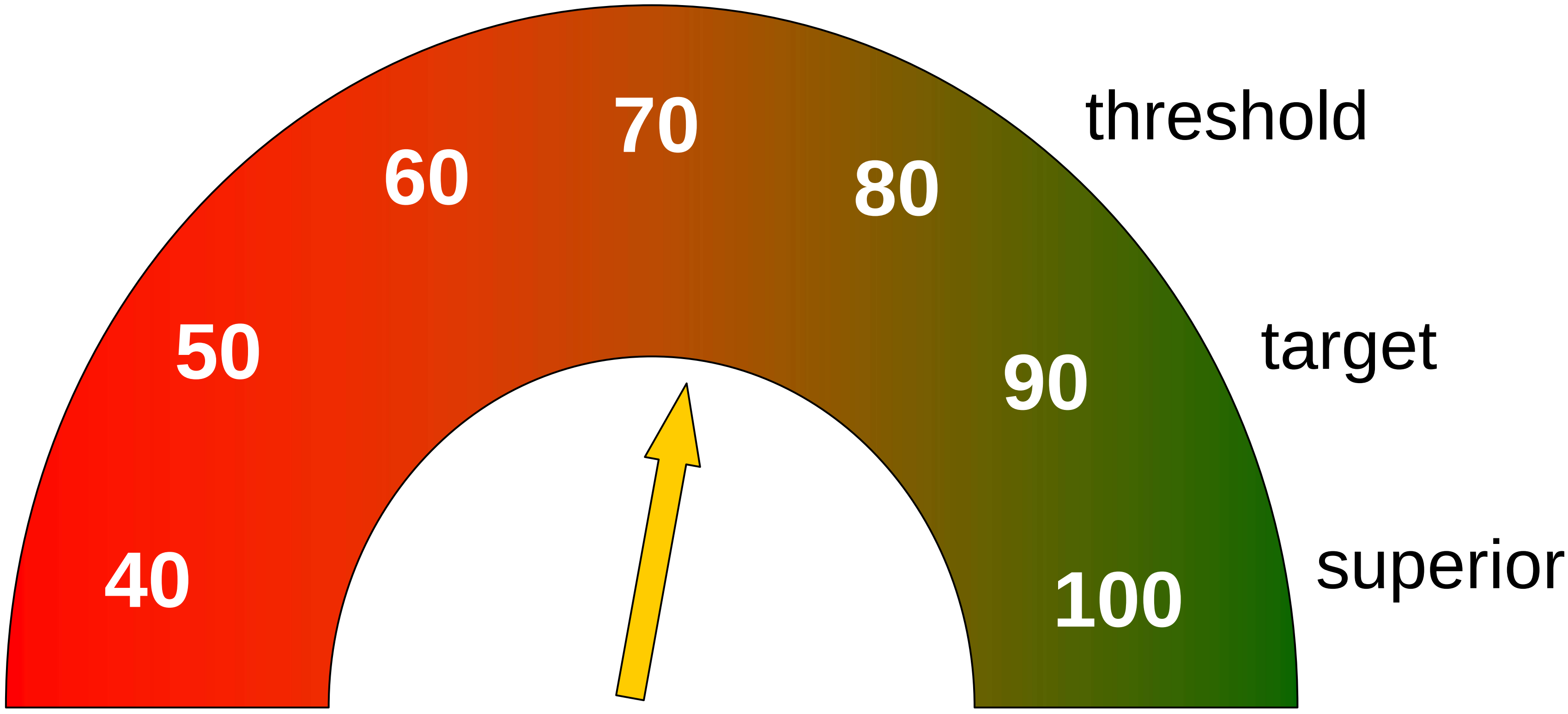
What kind of results am I getting?

Security Metrics …

Is this possible?



Information Security Risk Posture



Information Security Confidence Level

Making IT Work

Summary

- Pre compliance date:
  - involvement and action; energy and attention was high

- Post-compliance date:
  - loss of interest and attention; we got tired

- Re-focus and energize; use tools to plan, deliver, measure, and communicate

Contact Information

- Jim Reiner, Information Security Officer, HIPAA Security Manager
- reinerj@saccounty.net
- County of Sacramento – www.saccounty.net
- 916-874-6788