Strategies for Maturing Your Information Security Program

Susanne Elizer, Practice Director, Accretive Solutions

Professional Techniques – T23

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

SF ISACA FALL CONFERENCE NOVEMBER 9-11, 2015 HOTEL NIKKO-SAN FRANCISCO

Discipline

4 S's – Slides, Seesaws, Swings, Sandboxes

PLAYGROUND

6 items
49 prims total
25 different poses
Mod/copy

Fun for both kids and grown-ups!

L$550

SLIDE - SANDBOX - SWING - SEESAW - MONKEYBARS - MERRY GO ROUND

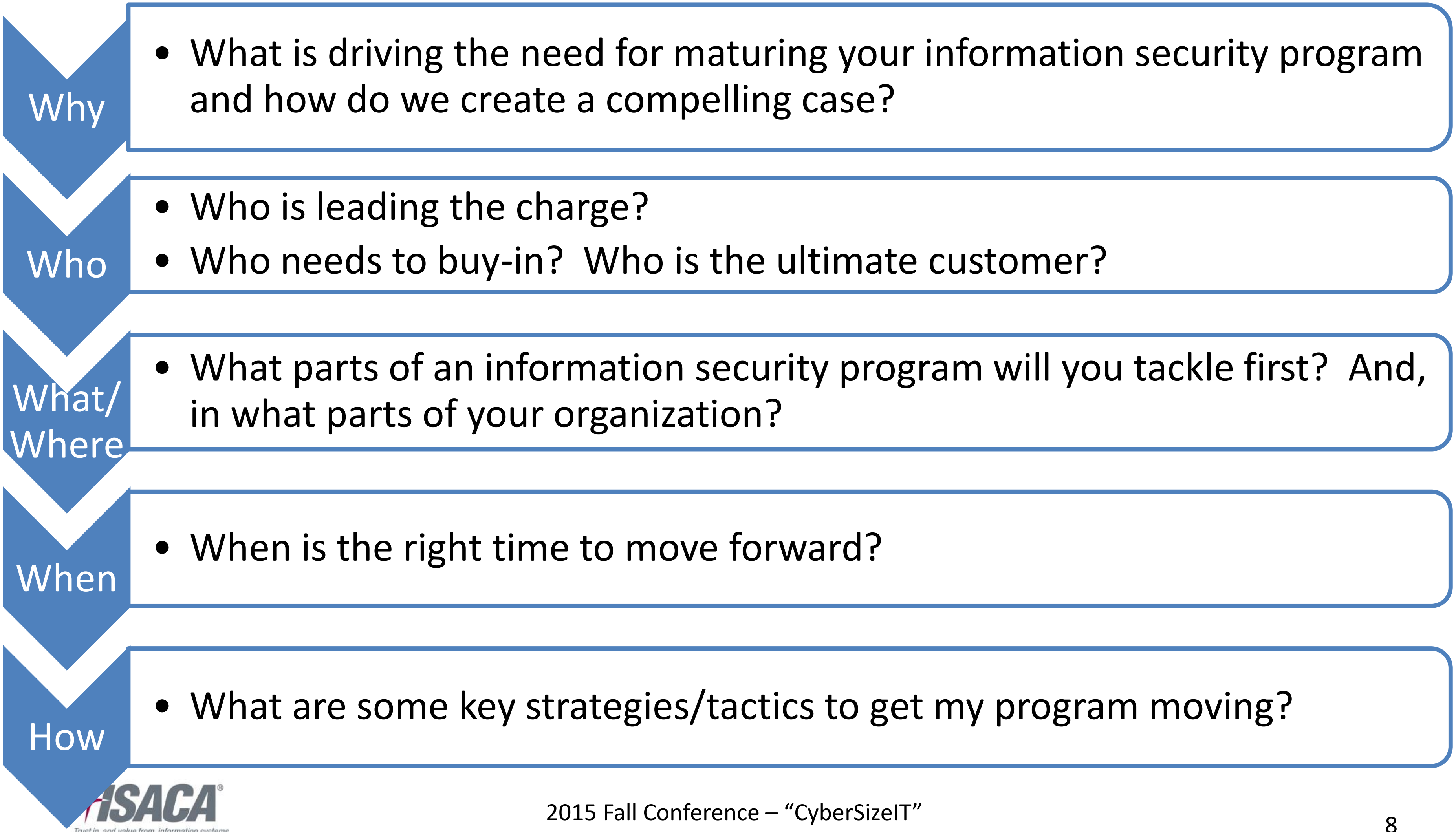
Junkyard and Adventure Playgrounds

Unintended Consequences

Growing Your Child's Brain Imagination Playgrounds

Agenda

- Objective: Identify and share strategies for maturing your information security program



Why

- What is driving the need for maturing your information security program and how do we create a compelling case?

Who

- Who is leading the charge?
- Who needs to buy-in? Who is the ultimate customer?

What/ Where

- What parts of an information security program will you tackle first? And, in what parts of your organization?

When

- When is the right time to move forward?

How

- What are some key strategies/tactics to get my program moving?

WHY

Why

- If you don't know why you are headed down a road, it's hard to know which direction to take and how fast to move
- How will maturing my information security program affect:
  - Opportunity (new markets, products, customers, competitors)
  - Threats to my business objectives
    - What are emerging trends/threats that my organization needs to meet?

Why – Examples

- We will not be able to sell our new cloud-based product into certain markets
- Our customers are demanding more transparency and we are losing business to our competitors
- Our business is facing new threats that we are not prepared to meet
- We aren’t very strong in cybersecurity and we really need to make some improvements

Compelling Case

S – Specific **M** – Measurable **A** – Attainable **R** – Results – Oriented **T** – Time-Based

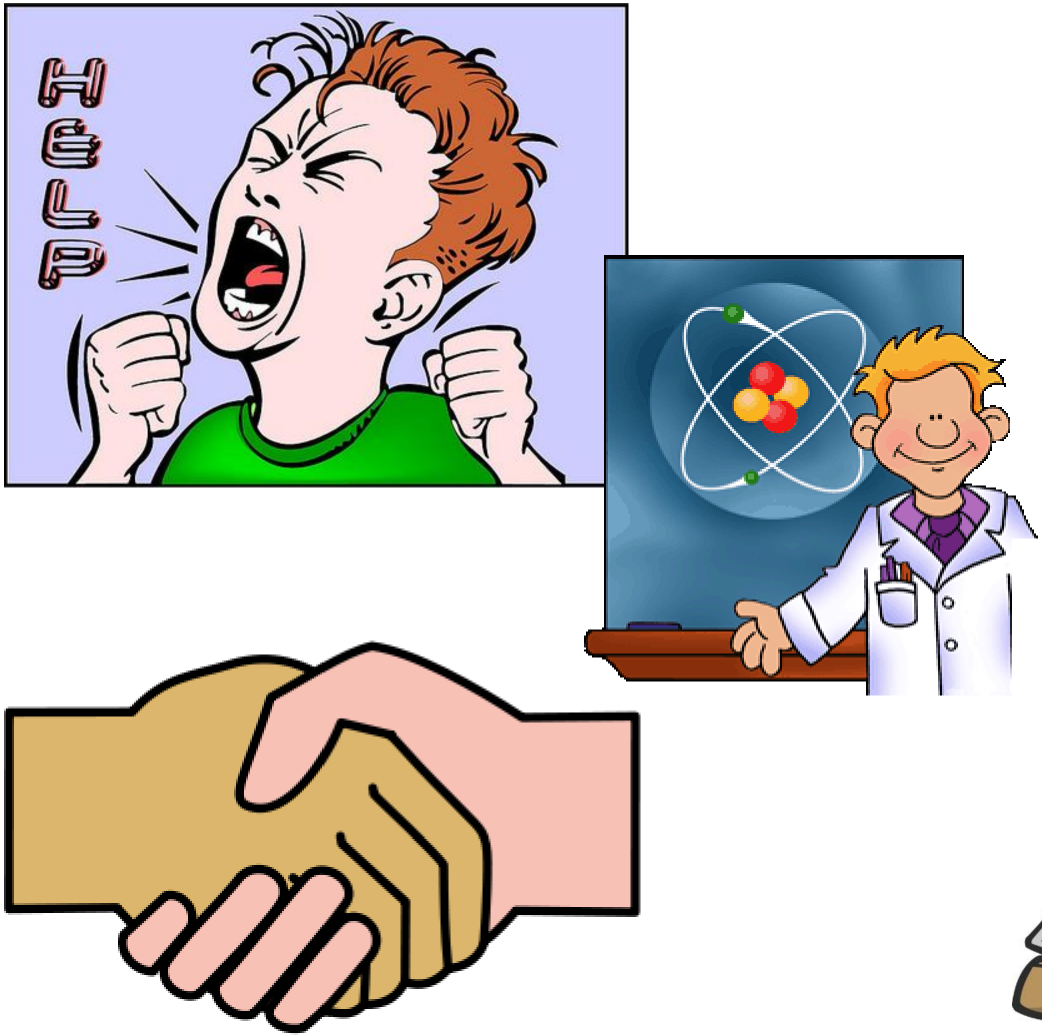
- Our strategic goal is to increase revenue by 25% through Product Awesome. Product Awesome customers require more robust and transparent information security practices than we currently have as we've now lost 3 major accounts to competitors due to our security practices. If we do not address our security gaps within the next 6 months, we are at risk of not meeting this goal.
- Our strategic goal is to increase revenue by 25% through Product Awesome. Product Awesome customers want more robust and transparent information security practices than we currently have. Our competitors who are currently serving this market do not meet these requirements. If we mature our information security practices, we have the opportunity to capture an even larger market share than planned.
- Within the last 6 months, the FBI has identified a rise in Organized Crime around cyber attacks. Due to our financial and market position, we are at increased risk for these types of attacks which could result in the loss of $XB and need to immediately make the following changes to our information security program.

What's The Vision

- Clear Vision and Goals
- Keep it Simple
- Vision examples:
  - –Recognized leader in information security
  - –No incidents as a result of lack of best practices
  - –Efficient enforcement
  - –Information security is a selling point

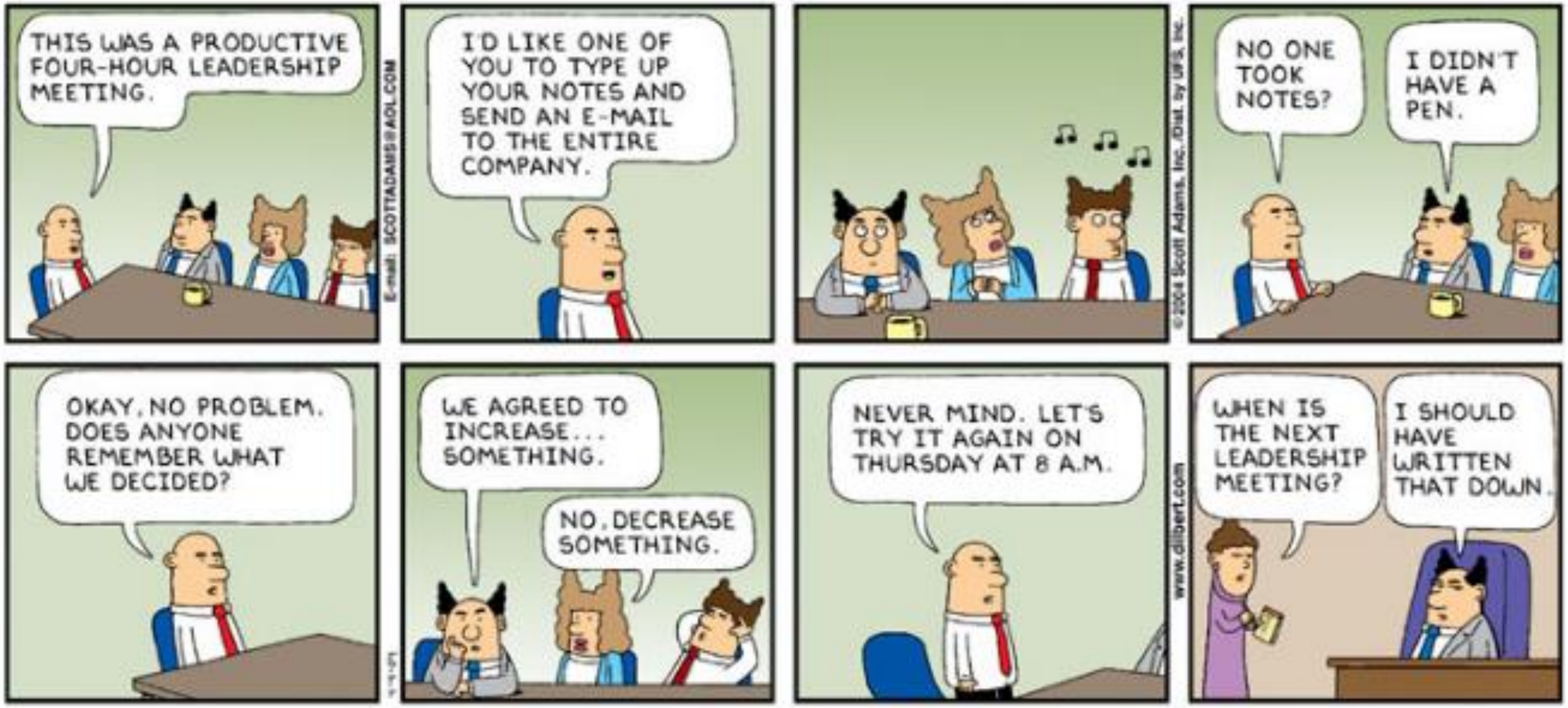
The Messenger

- The Alarmist
- The Scientist
- The Bulldozer
- The Partner



WHO

Why Care About Roles?


THIS WAS A PRODUCTIVE FOUR-HOUR LEADERSHIP MEETING.
E-mail: SCOTTADAMS@AOL.COM
I'D LIKE ONE OF YOU TO TYPE UP YOUR NOTES AND SEND AN E-MAIL TO THE ENTIRE COMPANY.
♫ ♫ ♫
© 2004 Scott Adams, Inc./Dist. by UFS, Inc.
NO ONE TOOK NOTES?
I DIDN'T HAVE A PEN.
OKAY, NO PROBLEM. DOES ANYONE REMEMBER WHAT WE DECIDED?
WE AGREED TO INCREASE... SOMETHING.
NO, DECREASE SOMETHING.
NEVER MIND. LET'S TRY IT AGAIN ON THURSDAY AT 8 A.M.
www.dilbert.com
WHEN IS THE NEXT LEADERSHIP MEETING?
I SHOULD HAVE WRITTEN THAT DOWN.

Key Roles

Role	Definition
Customer	Single person desiring a specific outcome
Driver	Single person accountable for driving outcome within your organization
Challengers	People with conflicting agendas
Advocates	People who will support outcome

Customer

- Customer Requirements:
  - Authority
  - Competency
  - Vision
  - Capacity
- Customer Role:
  - Value
  - Air Cover
  - Budget and Resources
  - Intervention as needed
  - Build advocates
  - Help to address challengers

Driver

- Driver Requirements:
  - Authority
  - Competency
  - Vision
  - Capacity
- Driver Role:
  - Ensure project management (scope, resource, execution, communications, risk, integration, quality, schedule, procurement)
  - Escalates blockers and concerns
  - Customer and Stakeholder Satisfaction
  - Continuously Assess Value provided against business case
  - Build advocates
  - Help to address challengers

Customer-Driver Challenges

- Single person
- Explicitly identified
- Explicit commitment
- Commitment is voluntary
- Committed to mutual value and mutual success
- Lack of authority/ authority changes
- Other competing priorities
- Competence
- When your customer is your biggest challenger

Challengers and Advocates

- Every challenger is a potential advocate
- Concerns should be explicit and if politically feasible public
- Advocacy should be explicit and public
- Exercise pristine project management at an enterprise level, with particular focus on communications management
- Communications should be tailored to address what your challengers and advocates care about most
- Continuously monitor
- Expect movement between challengers and advocates

WHAT/WHERE

Building a roadmap

1. **Define most critical products, businesses and locations within your organization**
2. **Assess current state and identify change strategy**
   - **Choose tool or framework**
3. **Determine future state**
4. **Prioritize assessment gaps based upon goals**
5. **Create roadmap and align**

- **Pick your strategies. Be practical and tactical**

Products, Businesses and Locations

- Most critical to achieve strategic objectives
- Least control
- Most complex

Evaluating Current State

If you don't know where you are, a map won't help

Sample Characteristics of Effective Evaluations:

- Scope covers most critical areas
- Agreed upon evaluation criteria
- Risks, Issues, Capabilities
- Results can be input into other strategic discussions
- Duration
- Competence
- Action-oriented

Tools and Frameworks

BSIMM	SAMM	C2M2
NIST CSF	Gartner	COBIT
CMMI	RMM RIMS	SSE-CMM
O-ISM3	Hi-Trust	Other

Tools and Frameworks – How to Choose the Best Framework for Your Organization

Sample Criteria:

- Compliance Requirements and Industry
- Level of Maturity
- Target Audience
- Organizational Appetite
- Culture

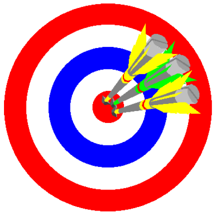
Determining Future State

If you don't know where you are going, any road will take you there

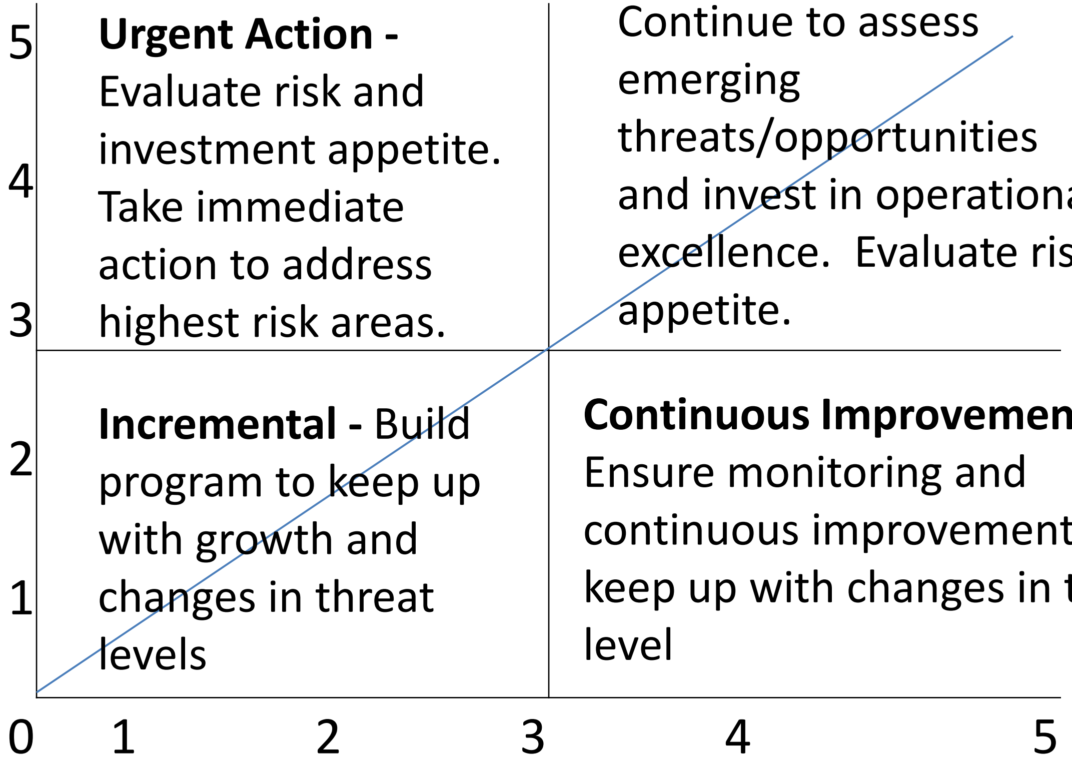
- Based upon corporate goals and objectives and information security goals and objectives
- Time Horizon (6 month/18 months)
- Establish measurements
- Establish checkpoints
- Project management

Change Strategy

Threat Level



How big of a target are you?



Urgent Action - Evaluate risk and investment appetite. Take immediate action to address highest risk areas.

Targeted investments- Continue to assess emerging threats/opportunities and invest in operational excellence. Evaluate risk appetite.

Incremental - Build program to keep up with growth and changes in threat levels

Continuous Improvement - Ensure monitoring and continuous improvement to keep up with changes in threat level

Maturity Level

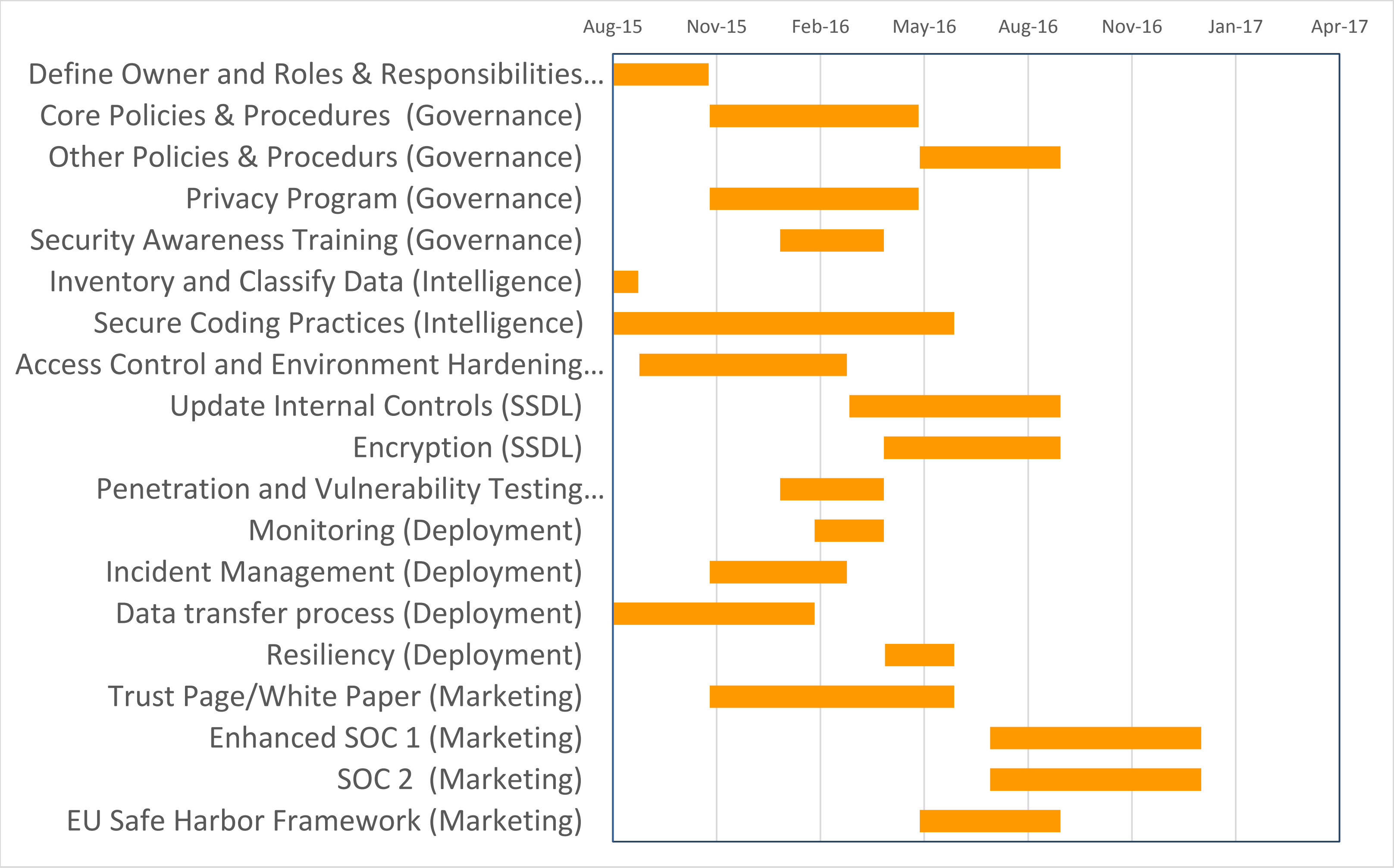
What level of maturity are you at?

Sample Prioritization Criteria

- **Business Objectives -** What business objectives or changes are most important over the next 6-12 months?
- **Information Security Goals –** What actions will most directly achieve goals and address the most risks or issues?
- **Most Prevalent Risks and Issues -** What information security risks and issues are you currently facing? (e.g. incidents, lost customers, etc.)
- **Changes –** Are business changes coming within the next 6-12 months that could make specific information security areas more likely to be exploited or the damage potential higher?
- **Opportunities -** Are there changes coming where failure to address certain information security challenges could mean you aren’t leveraging an opportunity?

Establishing a Roadmap

A Roadmap is purely actions set out in a sequence



WHEN

Change Readiness Indicator

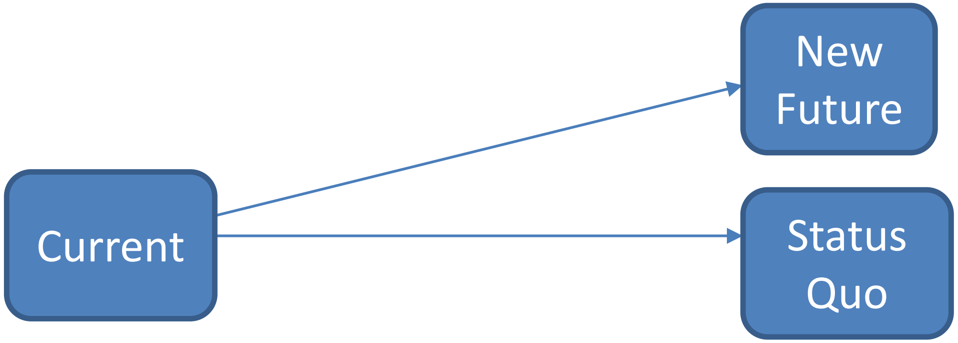
- **Why?**
  - How well understood is need for change?
  - How clear is vision for change?
- **Who?**
  - How strong are advocates and customers?
  - How influential are challengers?
- **What?**
  - What other priorities are competing for attention?
  - What business changes are coming up?
  - Is change in flight?
  - What is organizational appetite?

Increasing Readiness

Readiness Type	Action
Ready to Go	Implement Roadmap
Change is underway	Ensure roles are clearly defined and advocates are public. Assess challengers. Publicize value.
Change blocked - Internal Conflict or no commitment to action	Focus on Why; Define key decision makers; Focus on Alignment; maybe wait for right time; change your customer
Maintenance Mode	Ensure continuous improvement mechanisms are in place. Assess need 18 months out. Targeted investments. Focus on business value.
Unaware	Create compelling business case and define key roles. Conduct current state assessment and/or security testing if resources allow.

HOW

Declaring Action



Effective Declarations:

- Speaker and a listener. Declaration is explicit.
- New possibilities address concerns of the listener
- Each persons role in the new possibility is clear
- Speaker has the Authority
- Listener is important to the change
- The action is aligned to other corporate declarations

Alignment

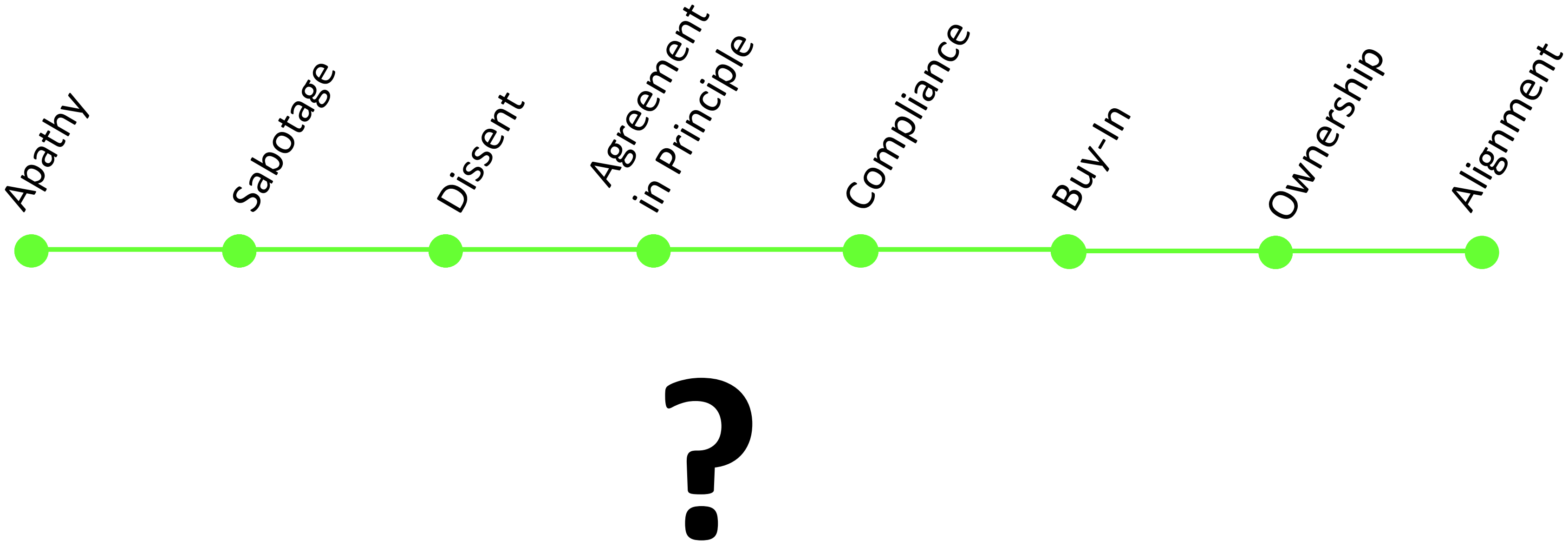
- The intention of *alignment* is to produce, and maintain **unity** of action

- It is a position that a person takes in relation to a decision or action

- A person can be:
  - On board the train
  - Not on the train
  - On the tracks

Alignment: necessary

- Alignment is not always necessary or worth the effort
- Decide (in advance) your minimum standard for how your team needs to relate to a decision



Alignment: how do you get it

- Align with the decision / direction yourself
- Engage stakeholders in dialogue
  - Demonstrate full and complete understanding of the decision / direction
  - Describe the implications
  - Clarification discussion
  - Invite concerns or considerations. Ask what's needed to support the decision. Encourage action to address concerns.
  - Offer why this decision or direction makes sense
  - Declare commitment
- Make an explicit request for each team members' alignment
- Receive an explicit response

Project Management

- Define time horizon
- Treat the change as a project (or many projects) with beginning and an end that can be measured
  - Integration, scope, schedule, cost, quality, people, communications, risk, procurement

Outsource or Insource?

- When to outsource?
  - Skillset or methodology
  - Capacity
  - Focus
  - Independence

Key Takeaways

- There is no “right way” to mature your information security program. False starts and unintended consequences are opportunities to learn.
- Be clear on roles and ensure that your customer and drivers have the authority, competence, vision, and capacity to fill the role
- Challengers and advocates can be brought together with alignment
- Use SMART messages to explain the why and have a clear vision and goal
- You have to know where you are to figure out where you want to go
- If you don’t know where you are headed, it’s easy to get lost.
- Tools and Frameworks help to determine the path, but can’t get you there
- If your organization is not ready, assess how to help get it ready or wait
- All change starts with a declaration
- Alignment of key decision makers is critical
- Treat maturing your information security program like a project