IT GRC Leadership Panel:

A Discussion on How to Move IT GRC Programs from Compliance to Risk Management Centric

Governance Risk and Compliance – G33

- Panel Moderator:
  Michelle Nix, Relationship Leader, IRM
  PayPal

- Panelists:
- Carolyn Wong, Global Product Director,
  Symantec

- Robin Byon, Sr. Manager ITRM,
  McKesson

- Jennifer Burton, Sr. Manager ITRM,
  Juniper Networks

- Michelle Koblas, Director IT Security,
  Guardian Analytics

- Eddie Borrero, Director ITRM,
  Electronic Arts

- Claire McDonough, Security Engineering Manager
  Google

COMPLIANCE TO RISK CENTRIC IT GRC PROGRAM EVOLUTION

Carolyn Wong
Global Product Director, Symantec

CONNECTING IT RISK TO THE BUSINESS

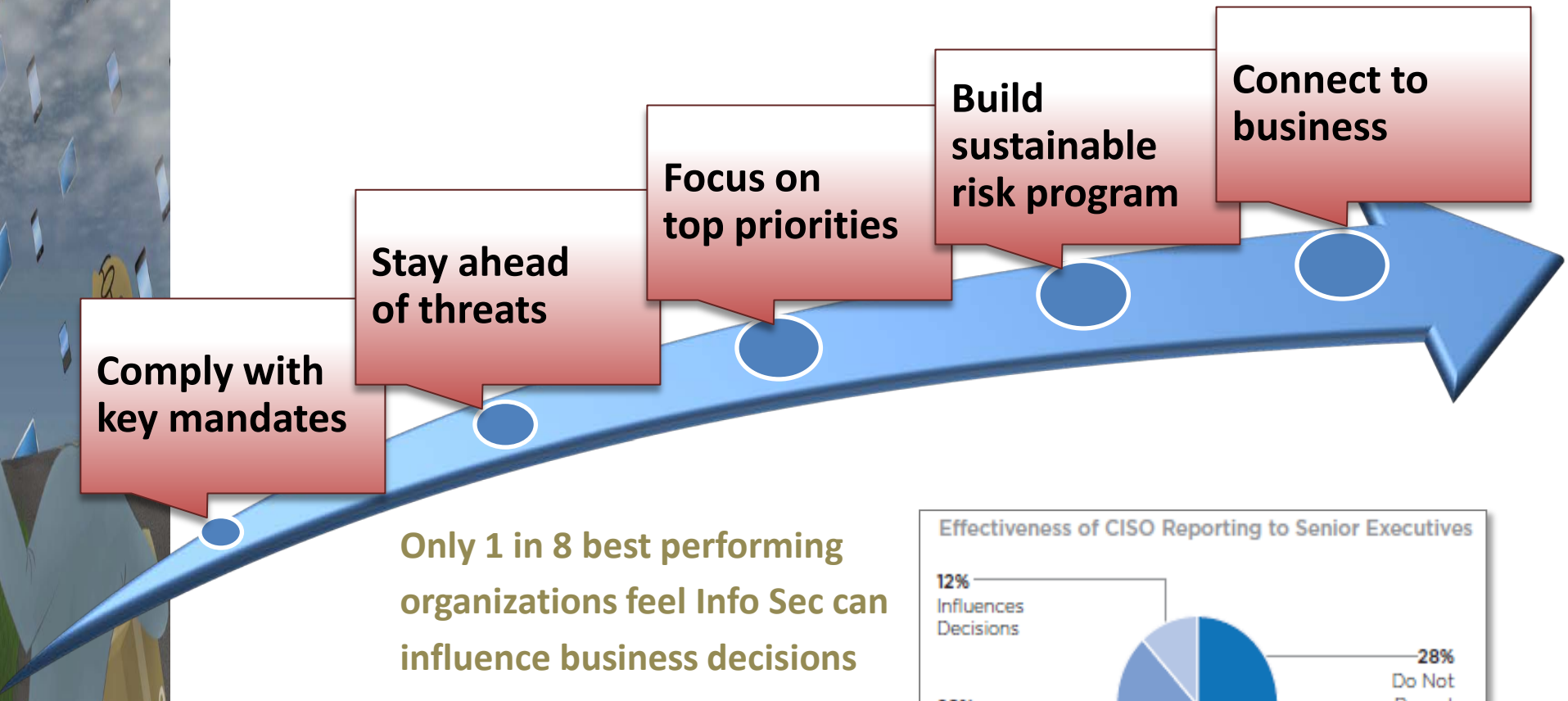
FORRESTER®

- **70%** of security decision makers report increased executive awareness of IT security due to high profile attacks and breaches
- Changes to IT risk management programs that would have the most positive impact on business counterparts
  - **47%:** better explain the value of security in business terms
  - **44%:** provide more accurate and timely data
  - **40%:** more frequent reporting of risk and compliance data

4

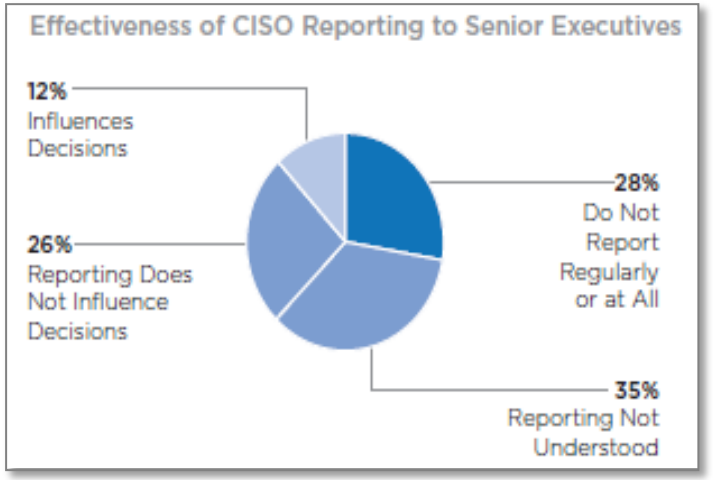
ORGANIZATIONAL EVOLUTION

FROM COMPLIANCE TO BUSINESS RISK MANAGEMENT



Only 1 in 8 best performing organizations feel Info Sec can influence business decisions

Source: Information Risk Executive Council, 2011



REGULATIONS, MANDATES, BEST PRACTICES

COSO Enterprise Risk Management

NERC CIP 002-009

ISO 18001

UK: Data Protection Act

Basel II

HITECH

ISO/IEC 27002:2005

DISA STIG

FIEL Guidance for J-SOX

CobiT 3, 4, 4.1

Sarbanes-Oxley

HIPAA

NIST SP 800-53 Rev. 3

PCI DSS v2.0

NIST SP 800-122

Gramm Leach Bliley Act

ISO 9001:2000

ISO/IEC 20000:2005

REGULATIONS, MANDATES, BEST PRACTICES

Regulations and Mandates	Best Practices and Frameworks
NERC CIP 002-009	COSO Enterprise Risk Management
Basel II	DISA STIG
PCI DSS v2.0	*ISO 18001*
UK: Data Protection Act	*ISO/IEC 20000:2005*
Sarbanes-Oxley	*ISO/IEC 27002:2005*
FIEL Guidance for J-SOX	CobiT 3, 4, 4.1
NIST SP 800-122	NIST SP 800-53 Rev. 3
Gramm Leach Bliley Act	
ISO 9001:2000	
HIPAA HITECH	

MOVING FROM COMPLIANCE TO RISK MANAGEMENT --
GETTING EMPLOYEES INVOLVED

Michelle Koblas
IT Security Director, Guardian Analytics

COMPLIANCE ENVIRONMENTS – EMPLOYEE EXPECTATIONS

Focused at what can be audited:

- ✓ Annual Training
- ✓ Knowing the Policies
  - Where are they?
  - Which ones are applicable to you?
  - What do you have to do to comply?
- ✓ Following the Rules
  - Did you do what the policy said?
- ✓ Dealing with Ambiguity
  - Ask the compliance/security teams

RISK MANAGED ENVIRONMENTS – EMPLOYEE EXPECTATIONS

- Empowering Employees to Manage Risk:
  - ✓ Annual Training
  - ✓ Knowing the Policies
    - Where are they?
    - Which ones are applicable to you?
    - What do you have to do to comply?
    - ➢ **WHY does the policy exist?**
  - ✓ Following the Rules
    - Did you do what the policy said?
  - ✓ Dealing with Ambiguity
    - ➢ **Understand the risk profile of the company**

UNDERSTANDING THE RISK PROFILE

- Different companies (or even different parts of the same company) can have different acceptance levels for risk.
  - Often called “Risk appetite” or “Risk tolerance”

- Differences occur due to:
  - Regulatory or Contractual Requirements
    - Health care, Government, Financial
    - Credit Card processors, Service providers
  - Type of Information handled
  - Impact on Competitive Advantage
  - Cross-organizational impacts (particularly within a company)

HOW DO I FIND MY COMPANY'S RISK PROFILE?

- Every company and every organization within the company may be unique, but there will be a lot of commonalities.
- Understand your business and your company's competitive advantage
- Perform a Risk Assessment - Talk to your executive and senior management about what is valuable within their part of the company and why

EMPLOYEE INVOLVEMENT – WHAT WORKS?

KEEP:

- All the compliance items –Annual training , Policies, Auditing

ADD:

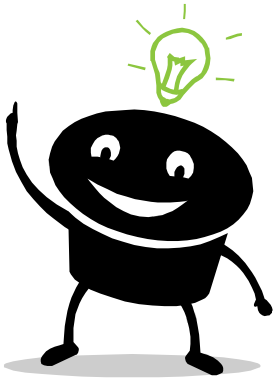
- More education – Short, frequent sessions to keep employees engaged on risk topics
- More empowerment – Allow employees to make appropriate risk decisions for the company.

BE PREPARED FOR:

- Steeper learning curves ("How" is a much easier concept than "Why")
- Initial pushback – Use your senior management support

REWARDS:

- More security, improved availability, improved process flow…
- Less overhead to the risk and compliance teams
- More employee satisfaction



QUESTIONS?
COMMENTS?

CERTIFIED OR CERTIFIABLE?

Robin Byon
Sr. Manager, IT Risk Management, McKesson
Jennifer Burton
Sr. Manager, IT Risk Management, Juniper Networks

KEY POINTS

- ✓ Why would anyone sign up for this?!
- ✓ Common types
  - Certification or Attestation?
  - IT or Security Focused?
- ✓ What is the right fit for your environment?

CERTIFICATION APPLICABILITY

- Financial Reporting
  - SOC 1 (SSAE 16)
- Information Security
  - ISO 27001
  - SOC 2 & 3 (also reports on availability, processing integrity, confidentiality and privacy)
  - HITRUST (healthcare focused)
  - DIACAP (DoD focused)
- Compliance Requirements (e.g. regulations, laws, etc.)
  - FISMA
  - HIPAA
  - PCI
  - SOX

YOU HAVE ONE, NOW WHAT?

- ✓ After the fact, market and communicate!
  - Increase awareness
  - Market differentiator
- ✓ Effective Usage
  - Winning new business
  - Customer requests and audits
- ✓ On the flip side, how do you leverage your vendors' certifications
  - Leverage a standard questionnaire
  - Understand the scope and results of your vendors certifications

LESSONS LEARNED

- Be engaged in the RFP and contract process
- Maintain your certification, *OR ELSE!*
- Limit the distribution

SOFT SKILLS FOR GRC LEADERS

(HOW TO SELL YOURSELF AND YOUR ROLE, WHY RELATIONSHIP MANAGEMENT AND BUSINESS ACUMEN IS MORE IMPORTANT THAN EVER)

Eddie Borrero
Director IT Risk Management, Electronic Arts

PERCEPTION IS EVERYTHING!

How GRC folks see their partnering Skills

How customers see GRC folks partnering Skills

THE FIRST 90 DAYS….
OR YOUR NEW FIRST 90 DAYS…

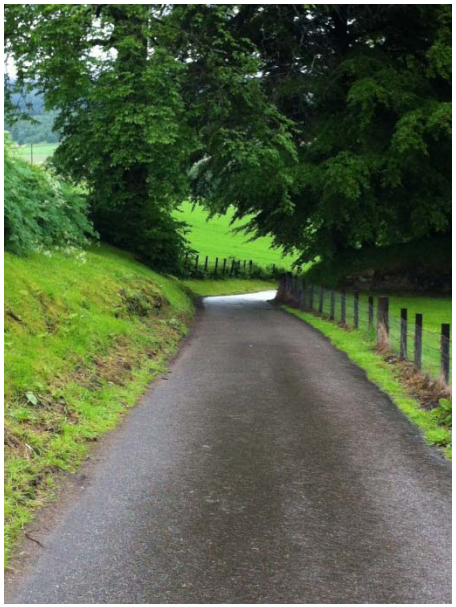
BUILDING TRUST AND COLLABORATION

- I always start with a 90 Day plan that:
  - Ensures I meet with all the right players to introduce myself and get to understand their experiences with GRC type folks.
    - Always better to meet people and ask how you can help them before asking them to do things.

WHAT AND HOW TO ASK…

- Ask open ended questions these increase engagement
  - ‘What keeps you up at night – anything at all – barking dogs – hackers – what???’
- Ask questions about what the short and long term business plans are.
  - Try to understand where the connections are for your role
- Ask questions about what their processes are.
  - ‘Do you have an SDLC? Where do we fit into that?’
  - ‘Is there someone in the group who is your process expert that we can talk more with?’

WHAT ARE YOU TRULY TRYING TO GET OUT OF THE DISCUSSION?



Everyone has different views of the same world you live in.

An effective GRC Leader will know based on interactions, actions and reactions what the view of the world looks like for the person you need to influence to drive GRC practice maturity.

INCLUDE ALL CRITICAL PARTIES

- A Big Mistake I see GRC teams make is to start making decisions around audit criteria, communicating audit results, and or start to solution without the input of all the appropriate parties.

Remember to Include the Right Teams!

SOLUTIONING…

- Work with them to develop a plan **(to be implemented ASAP where possible)** that addresses the opportunities for improvement that they are surely going to outline in your initial meetings.

- Look for quick WINS that benefit multiple parties!!!

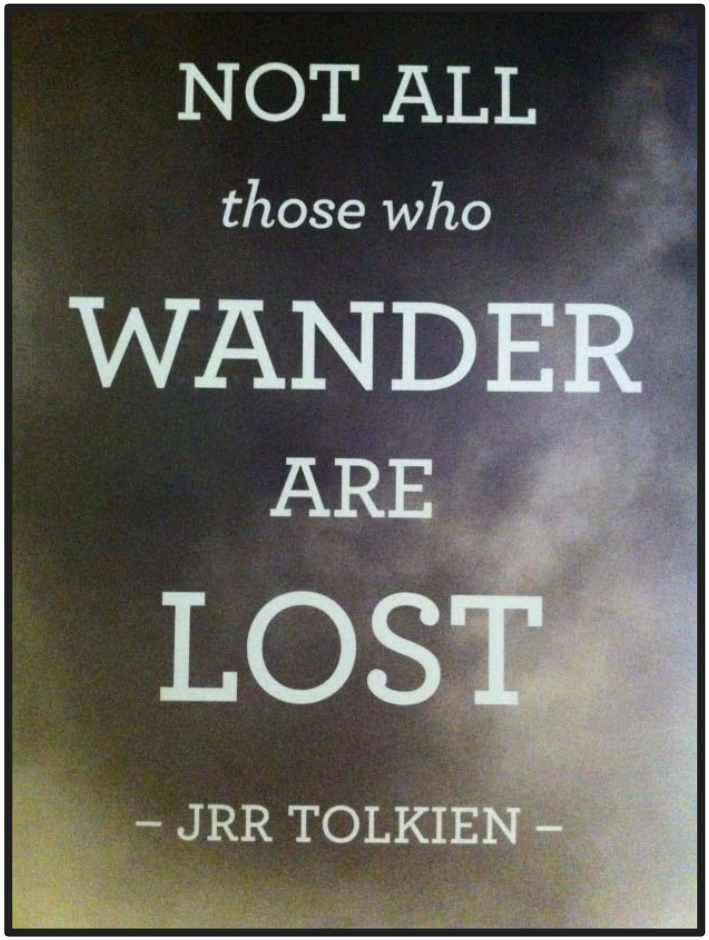
SETTING THE STAGE

(BUILDING FOR THE LONG HAUL)
(INCREASING BUSINESS CONFIDENCE)

- After 90 Days you should be clear on:
  - What improvement opportunities and or compliance gaps exist.
  - Who your advocates and/or resisters are.
  - How to create a roadmap that includes short and long term goals.
  - Understand the processes that exist to provide support to integration of the short and long term goals.

- THEN Develop a one to two year roadmap:
  - Socialize and execute against low hanging fruit (grab all the wins where you can)
  - Get your Roadmap approved and understood.
  - Focus on continuous communication
    - For example, if you have a WIN opportunity…SELL IT…repeatedly…to anyone who will listen!

QUESTIONS?



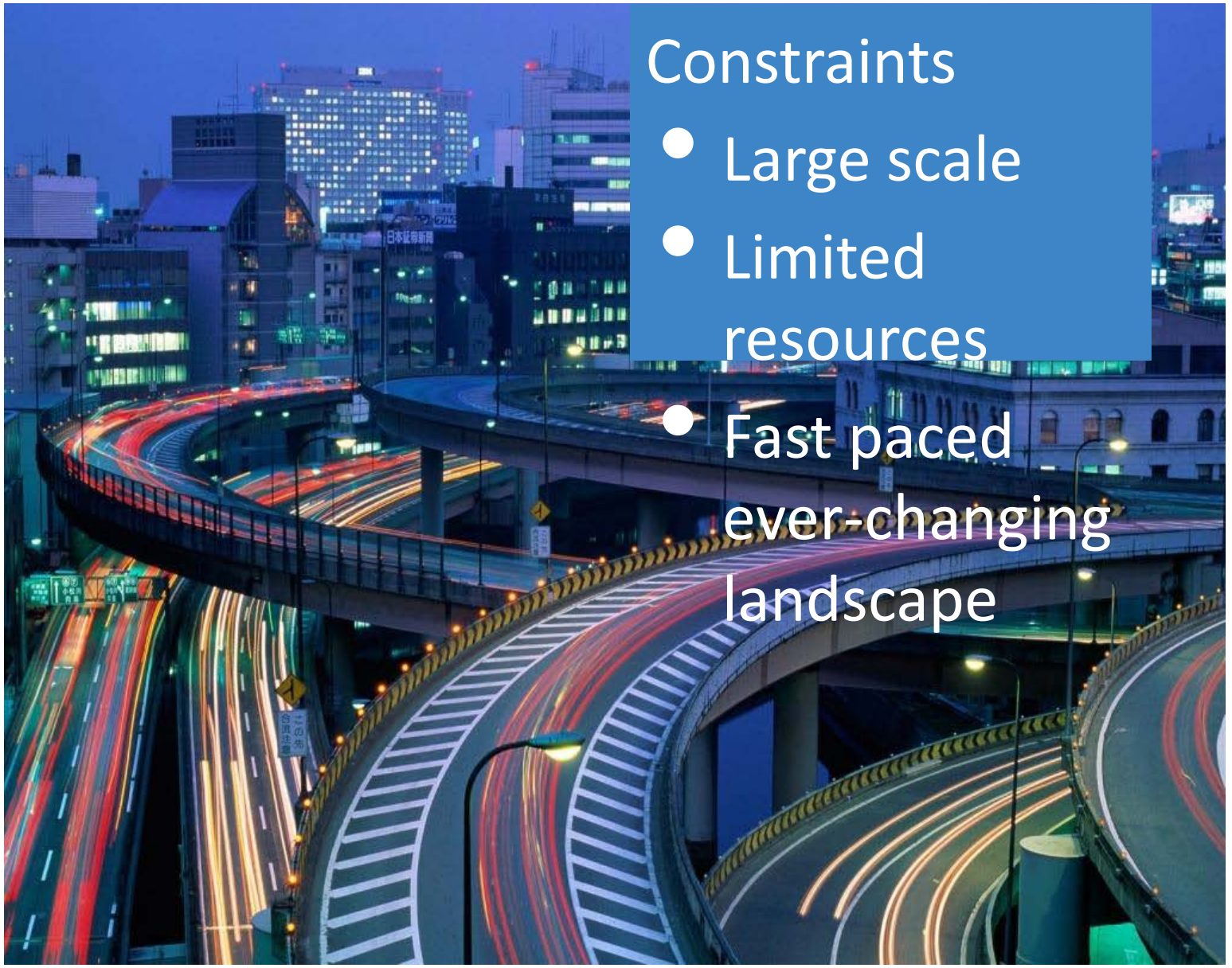
RISK MANAGEMENT IMPLEMENTATION

Claire McDonald
Google

IMPLEMENTING OBJECTIVES DESPITE CONSTRAINTS

Objectives

- Risk Management
- Resource Management



Constraints

- Large scale
- Limited resources
- Fast paced ever-changing landscape

IMPLEMENTATION SUCCESS

- Prioritization
  - Based on real life experience
  - Evidence-based threats
  - Ordered list of goals forces focus on only the highest
  - New requests compared to priority of current goals; only those that are higher priority force a change of focus
  - Avoid simply reacting / fighting fires all the time
- Focus Area Model
  - Small teams
  - Defined problem domain
- Quarterly planning
  - Objectives and Key Results
  - Difference between expected achievements and 'Stretch' goals
  - Important goals pushed to 'Stretch' status? Time to request additional resources with specific high priority tasks in mind

BALANCE

- 1/3rd Reactive
  - Operational and consultative tasks
- 1/3rd Proactive
  - Risk initiated project work
- 1/3rd Continual Improvement
  - Automation
  - Tooling

QUESTIONS?