IT / CYBER RISK ASSESSMENTS

DEVELOPING A RISK HIERARCHY & AN EFFECTIVE CYBER RISK STRATEGY

Presented by

Michael Addo-Yobo

Managing Principal, Cyber Risk Advisory

Coalfire

PREAMBLE

- Cyber risk is now a high priority for organizations globally, and for a variety of reasons
- Board/C-Suite and executives at large are concerned
- Regulators are prescribing increasingly stringent requirements for cyber risk management
- Many organizations lack of a holistic enterprise-wide approach to proactive cyber risk management
- How does an organization establish a practical and sustainable framework for long-term, proactive, cyber risk mitigation?
- How can the value of risk assessments be optimized to proactively identify and minimize IT/cyber risks?

CALFIRE

SESSION OBJECTIVES

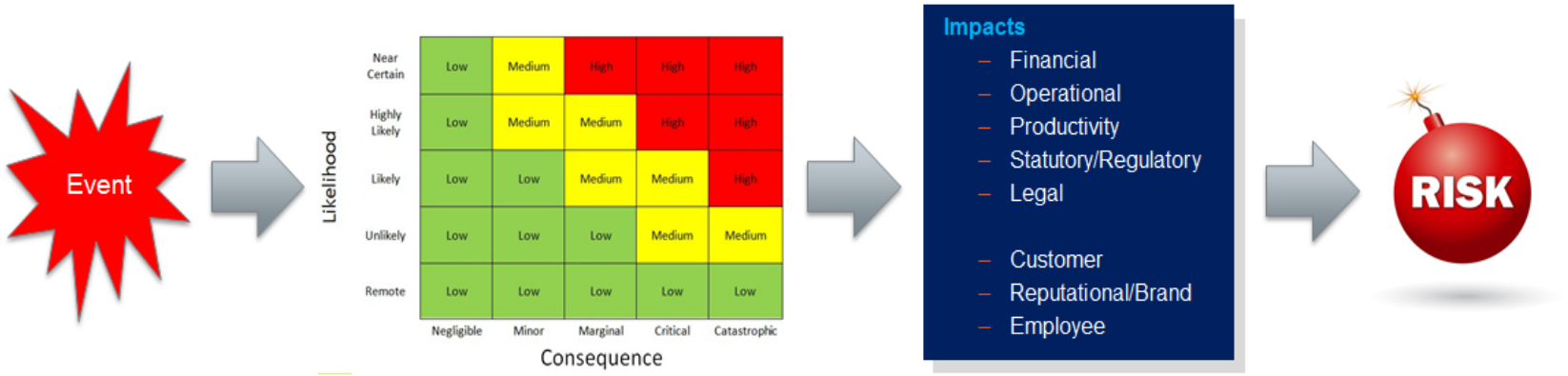
- Setting context – IT/Cyber Risk
- The IT/Cyber Risk Landscape
- Sources of IT/Cyber Risk
- How to develop an IT/Cyber Risk Management Strategy
- Building an IT/Cyber Risk Program (Strategy Execution)
- Optimizing the value of IT/Cyber Risk Assessments
- Strategy and program sustainment

CALFIRE

THE CONCEPT OF IT / CYBER RISK

IT / CYBER RISK – THE CONTEXT

- The ***business*** risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise



IT risks can range from inconsequential (tolerable) to catastrophic (intolerable) in scale

COALFIRE

THE IT / CYBER RISK LANDSCAPE

THE IT/CYBER RISK LANDSCAPE

We are in an era where many enterprises are fearful of being victims of a cyber breach and suffering intolerable impacts

Source: ISACA

Key Questions from Board / C-Suite

- What is our cyber risk management strategy?
- Functionally and operationally, are we progressively reducing cyber risks to acceptable levels?
- Do we know our key threats and vulnerabilities and our real cyber risks and business impacts?
- Are current cyber risk management practices effective?
- What are our security related compliance obligations?
- Who is after our data? Are we susceptible to a breach? How do we know if we are a target?
- Are we prepared to respond to and recover from breaches or operational disruptions
- Are our employees cyber risk conscious?

CALFIRE

SOURCES OF IT / CYBER RISK

IT / CYBER RISK SOURCES

- IT risks come from threats, vulnerabilities and operational weaknesses with the use, ownership, operation, involvement, influence and adoption of IT

Operational
The potential for technology failures to disrupt core business processes

Security
Security threats such as malware and hackers; vulnerabilities such as weak passwords and poorly designed software

Continuity
Major operational disruptions including natural and man-made scenarios (e.g. earthquake, terrorism, pandemic/epidemic

Third Party
The potential for an IT vendor or service to fail to meet their obligations to an enterprise

Quality
Failures of quality assurance and other quality related practices such as service management

Changes
A failure to control IT changes – people, process, information systems and their configurations

- Other sources of risk
  - *Management decisions*
  - *Resourcing*
  - *Innovation*
  - *integration*
  - *Compliance violations*
  - *Procurement*
  - *Contracts*
  - *Assets management*
  - *Facility*
  - *Single Points of Failure*

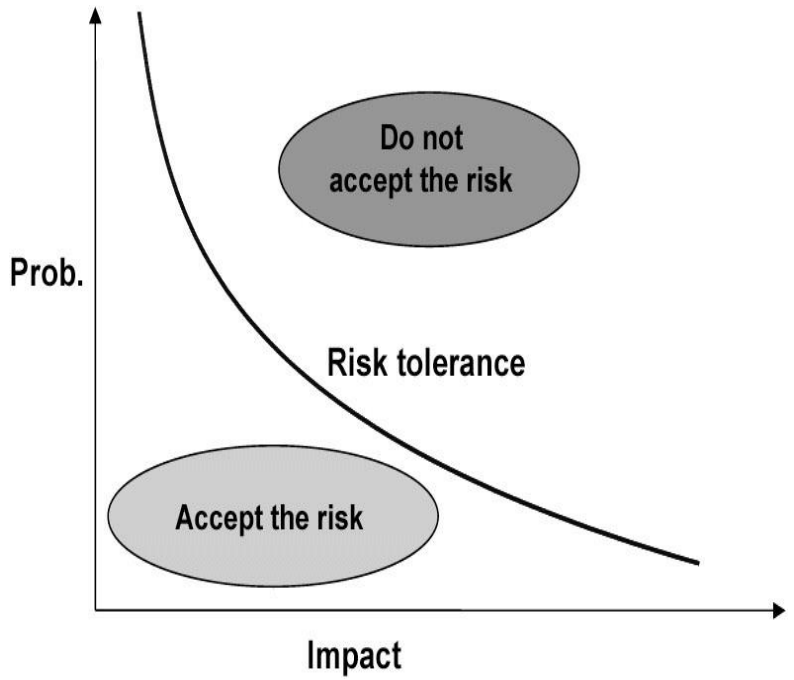
- IT risks should be assessed/measured more holistically for organizational benefit

CALFIRE

HOW TO DEVELOP AN IT RISK MANAGEMENT STRATEGY

IT RISK STRATEGY

- Key considerations for a **successful** IT Risk Management Strategy include the following:
  - Current state analysis
  - Organizational risk tolerance
  - Risk culture
  - Strategic alignment
  - Risk management vision
  - Key goals and objectives (including regulatory and non-regulatory compliance)



CALFIRE

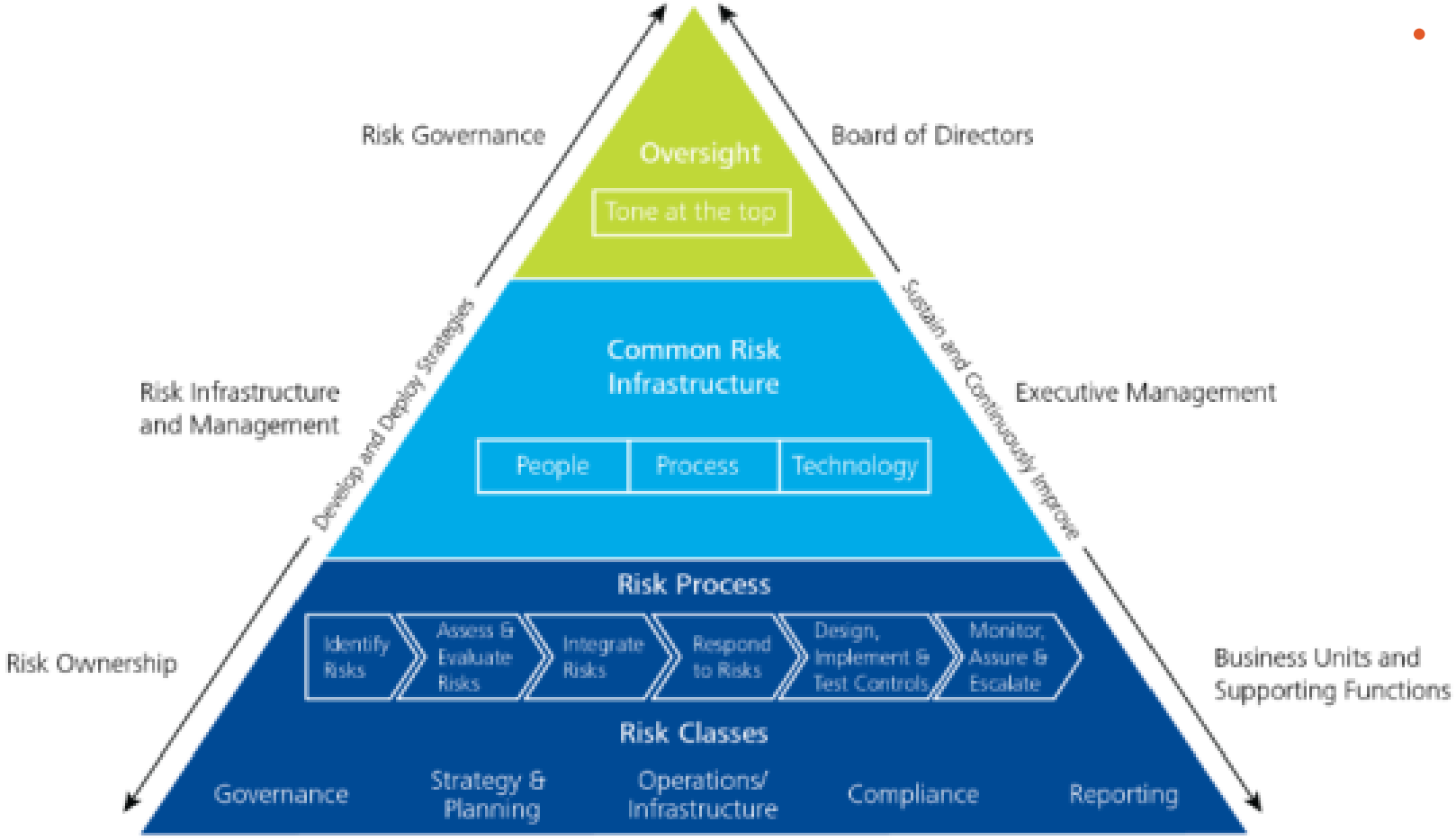
BUILDING AN IT RISK PROGRAM

IT RISK PROGRAM

- A successful IT Risk Program relies on a well defined IT Risk Management Strategy
- An effective IT Risk Program includes the following:
  - Operational/tactical initiatives required to achieve IT risk management goals and objectives
  - Governance (e.g. risk policies, standards, procedures)
  - Operating model
  - Stakeholders, roles and responsibilities
  - Control frameworks and standards
  - Tools and templates
  - Information management
  - Continuous improvement/sustainment

COALFIRE

IT RISK HIERARCHY



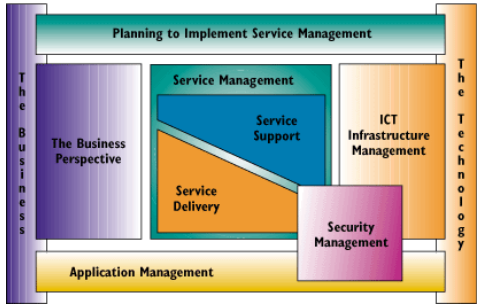
- A holistic approach to IT risk management that involves strategic and tactical levels of an organization is essential for success

COALFIRE

IT RISK MANAGEMENT ARCHITECTURE

Business Drivers

- Business objectives
- Legislative/regulatory requirements
- Accountability
- Implementation of internal control
- Ongoing assessment
- Positive evidence of control effectiveness



IT Management Best Practices

- ITIL, CMM, etc.
- Best practice IT service delivery
- Process oriented
- Publicly available
- Designed to gather, use and maintain information

IT/Cyber Risk Management Architecture

Optimized IT Risk Management

IT Risk & Control Framework

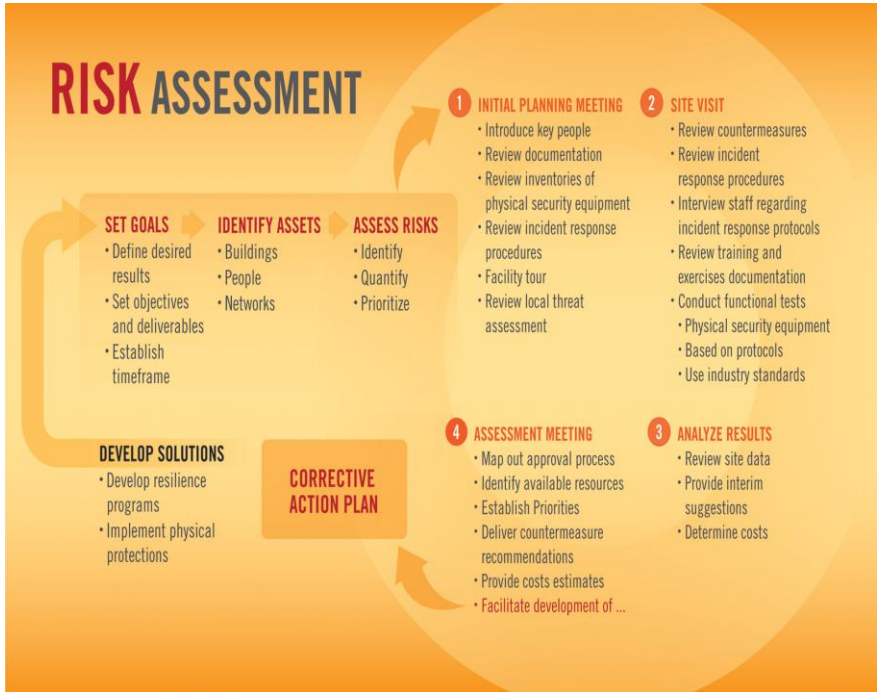
- CobiT, ISO 17799, Balanced Scorecards, Common Criteria, etc.
- Commonly accepted control framework
- Objectives, practices, measures
- Maturity assessment
- Publicly available & maintained

COALFIRE

LEVERAGING THE STRATEGY & PROGRAM FOR HIGH VALUE IT RISK ASSESSMENTS

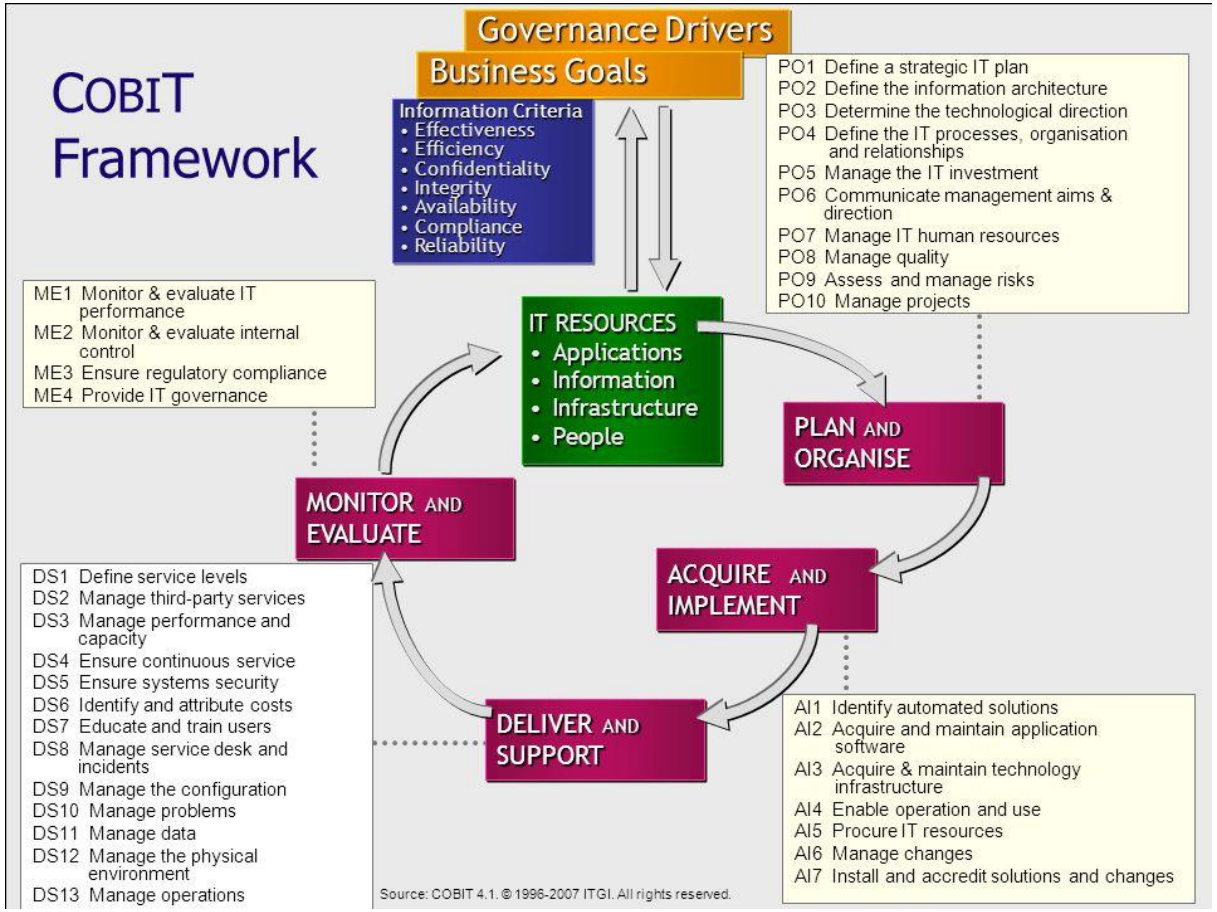
IT RISK ASSESSMENTS

- A successful IT Risk Program relies on a well defined IT Risk Management Strategy
- Key considerations for building an effective IT Risk Program include the following:
  - Assessment goals and objectives
  - Planning and scoping
  - Approach and methodology
    - Corroborative inquiry vs. Substantive testing
    - Design and/or operating effectiveness assessment
  - Applicable control framework/standard
    - COBIT, NIST, ISO, ITIL or Hybrid
  - Data gathering
  - Benchmarking and analysis
  - Documentation & reporting
    - Working papers / test evidences
  - Remediation and risk mitigation
  - Follow-up/tracking



CALFIRE

SAMPLE FRAMEWORKS / STANDARDS

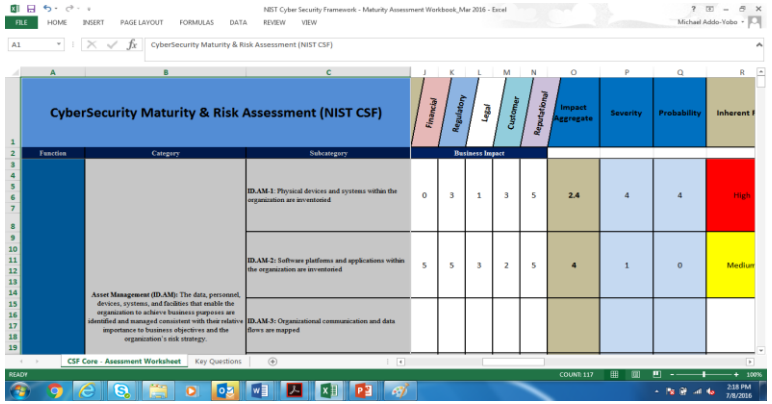


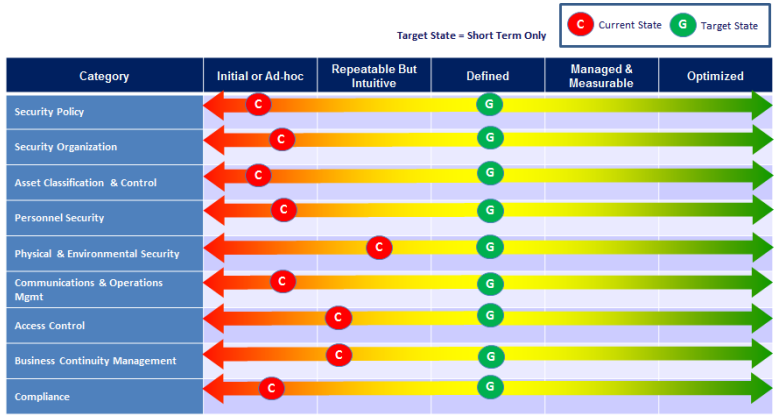
- **Information Security**
  - NIST 800-53
  - NIST CSF
  - ISO-27001
  - SANS Top 20
  - COBIT Security
  - FedRAMP
  - PCI
  - HITRUST
  - CSCC Cloud Security Standard
  - ISA/IEC 62443
- **Information Risk**
  - COBIT
  - Risk-IT Framework
  - ITIL
- **IT Governance**
  - COBIT
  - VAL-IT
  - ITIL / ISO-20000
  - TOGAF
- **IT Compliance**
  - ISO-19600

COALFIRE

SAMPLE TOOLS/TEMPLATES …

A snapshot of some of the tools and templates that could be leveraged to support IT risk assessments are illustrated below:





- **Controls Assessment Workbooks** – Assessment workbooks may leverage various benchmarking frameworks and standards (e.g. ISO-27001, NIST-CSF, NIST 800 Series, COBIT)

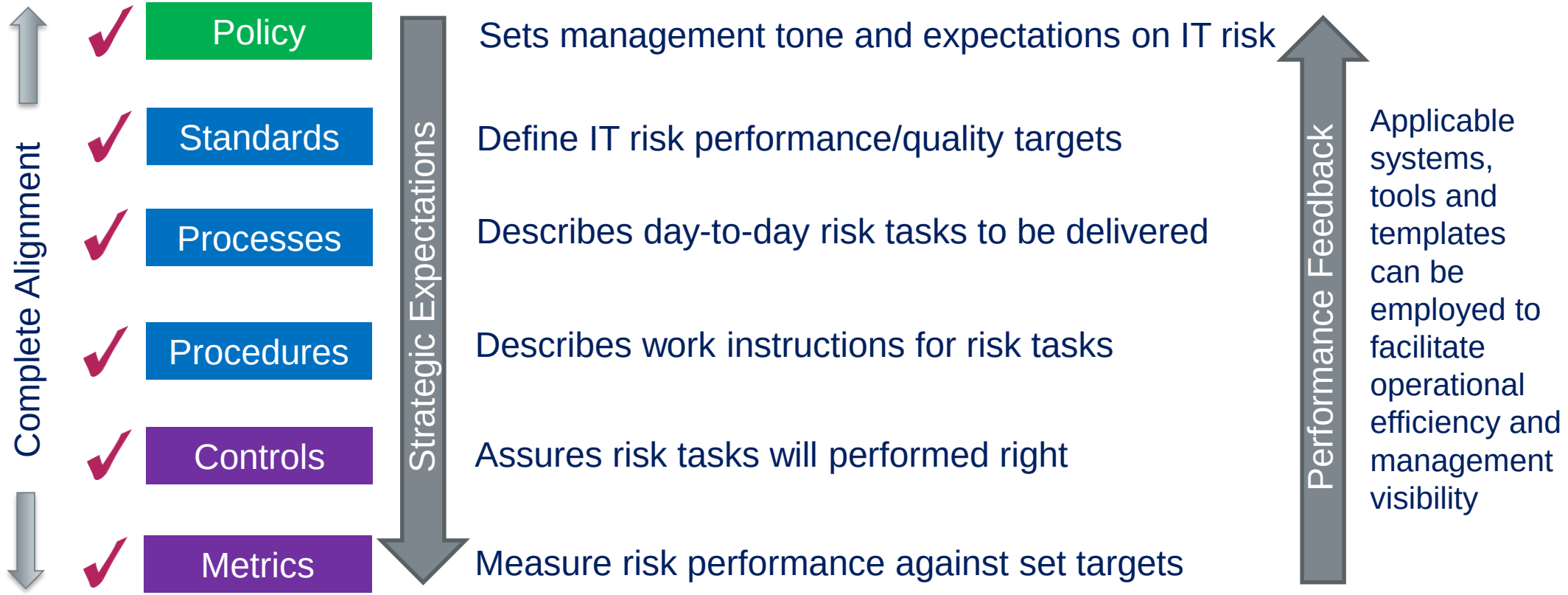
- **Risk/Maturity Scorecards** – Scorecards will facilitate determination of the levels of risk and maturity of operational practices and controls relative to the assessment domain area, comparing current state to short/long term target states. Scorecards may facilitate measurement of progress in reducing IT risks to acceptable levels

COALFIRE

SUSTAINING AN IT RISK STRATEGY AND PROGRAM

IT RISK GOVERNANCE

Risk governance incorporates provisions that sustain, and advance the realization of desired outcomes from IT Risk Management strategy and programs



CALFIRE

KEY TAKEAWAYS

- Effective IT risk management is more than just security
- A successful IT Risk Program relies on a well defined IT Risk Management Strategy
- A well planned and executed schedule of IT Risk Assessments can add significant value to IT risk mitigation
- It is essential to apply relevant frameworks/standards
- Embedding governance provisions help to sustain risk mitigation for the long term

CALFIRE

Q & A