FORRESTER LEADERSHIP BOARDS
Security & Risk Council

Information Security Metrics – Information that Matters to the Business

CISOs need to create high impact security reports

Jinan Budge, Global Council Manager

Forrester Research

September 18, 2011

FORRESTER®

20 minutes of fame pays off for 30 years

FORRESTER LEADERSHIP BOARDS
Security & Risk Council

© 2010 Forre

Agenda

- Who is your new audience
- The 4 steps to creating a high impact report
  - The current reporting landscape
  - Group exercise: Understanding your audience
  - Plan and design the report
  - Implement
- Recommendations and next steps

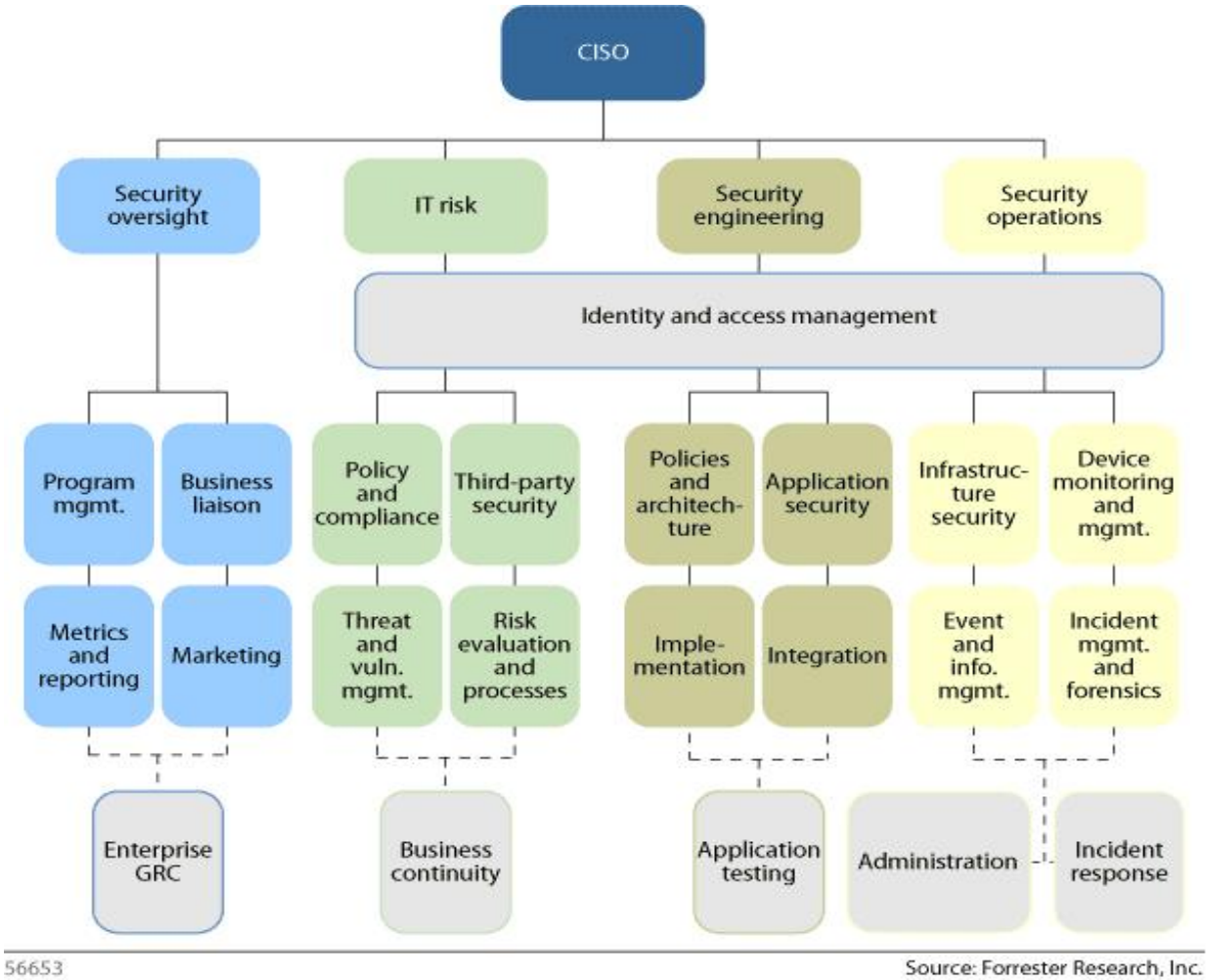
© 2010 Forrester Research, Inc. Reproduction Prohibited

The CISO is a business leader and a security leader – Use business driven security metrics to prove it.

Forrester Leadership Boards
Security & Risk Council

© 2010 Forrester Research, Inc. Reproduction Prohibited

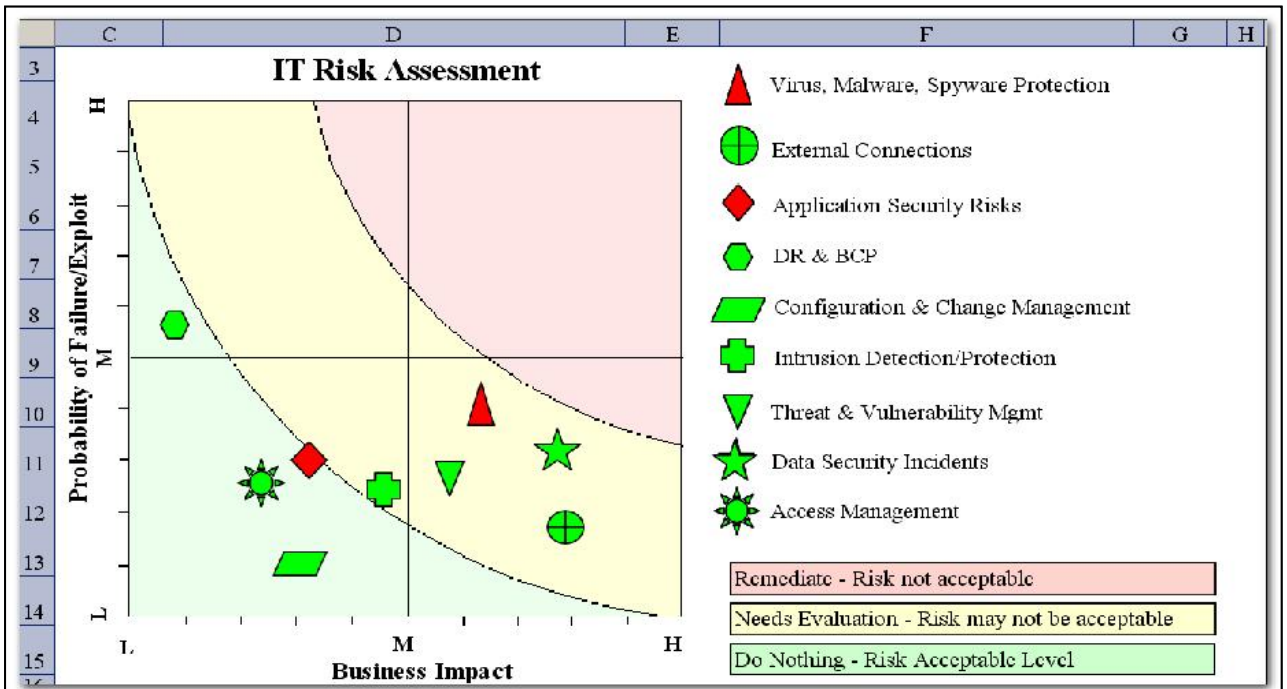
Changing reporting structures



© 2010 Forrester Research, Inc. Reproduction Prohibited

Risk Management Dashboard – Traditional Security Metrics

- CISOs often focus on operational metrics when reporting to senior leadership:
  - Percentage of users who undergo background checks each year
  - The number of virus infections addressed during the year
  - Etc.



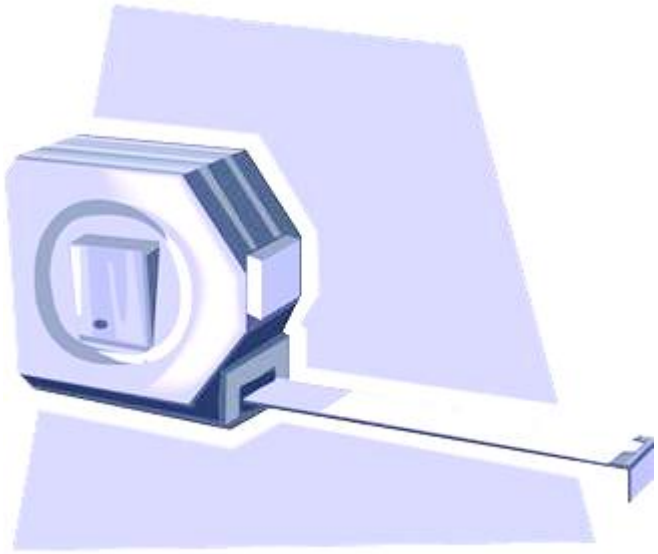
Source: Eastman Kodak Company's Global IT Security Risk Dashboard

FORRESTER LEADERSHIP
Security & Risk Council

© 2010 Forrester Research, Inc. Reproduction Prohibited

Security Leadership

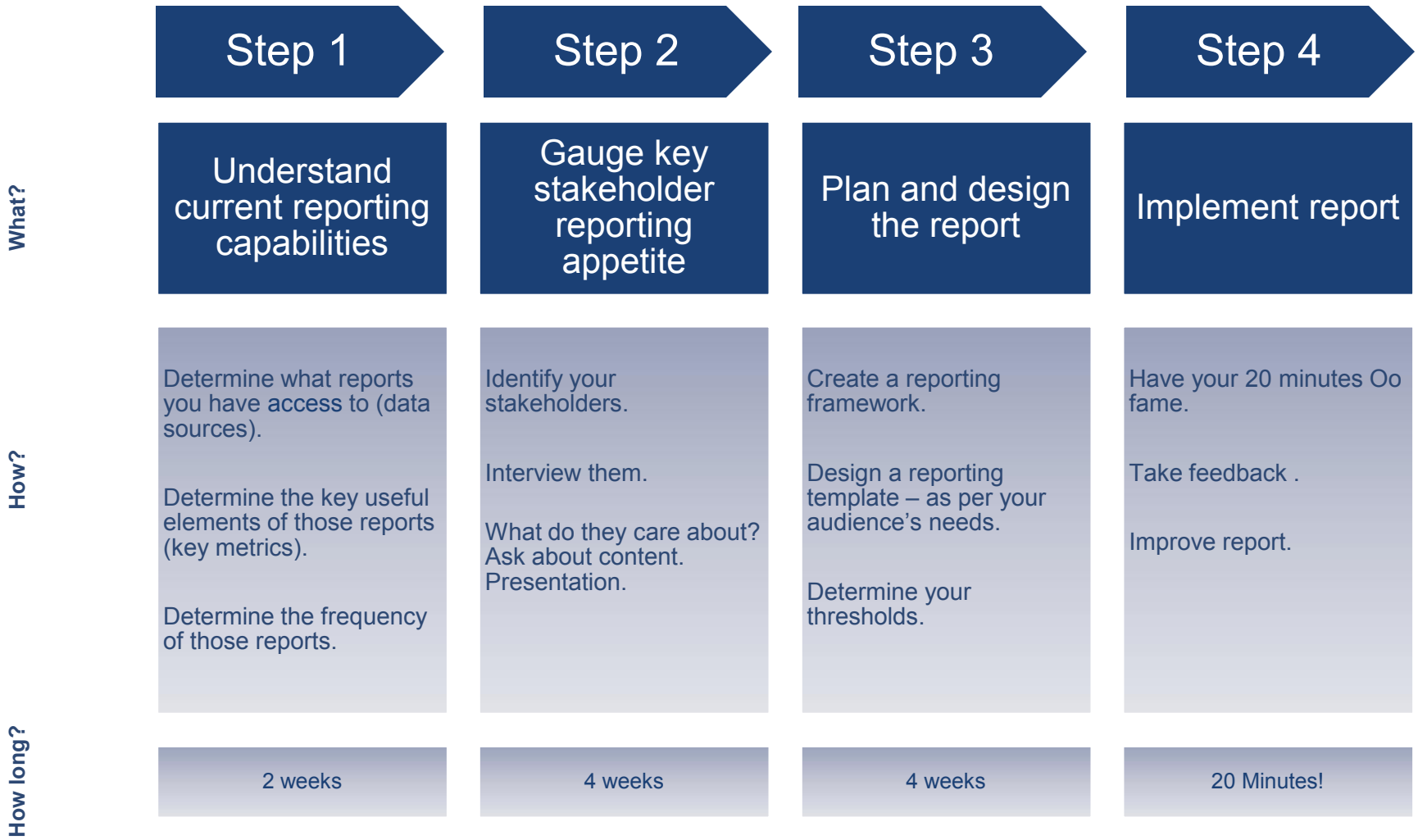
"You Get What You Measure"



- **Security has much broader responsibilities than just operational security issues:**
  - Economic, Legal, Regulatory
  - Human Resources, Compliance
  - Traditional IT information security concerns
- **Security needs information for better decision-making**.
  - Security metrics need to support decision-making and should drive broad based risk management strategies…"
- **Security needs information to demonstrate the value that their programs provide.**
  - Security metrics need to demonstrate business alignment, and support for the strategic and tactical goals of the business**.**

© 2010 Forrester Research, Inc. Reproduction Prohibited

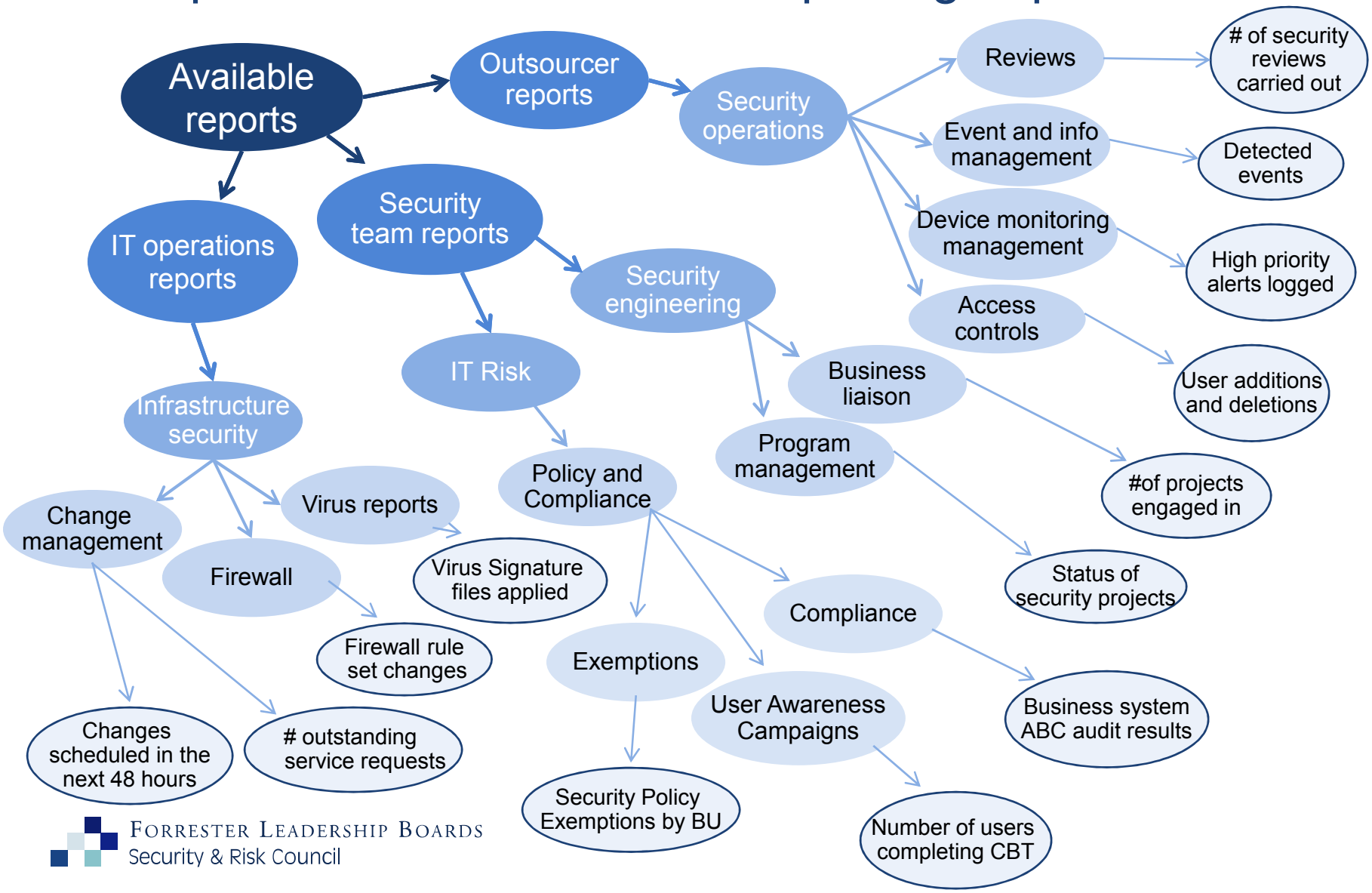
Steps to creating a high impact executive report



FORRESTER LEADERSHIP BOARDS
Security & Risk Council

© 2010 Forrester Research, Inc. Reproduction Prohibited

Step 1: Understand current reporting capabilities



FORRESTER LEADERSHIP BOARDS
Security & Risk Council

© 2010 Forrester Research, Inc. Reproduction Prohibited

Classify Operational Security Metrics

	Control Objective	Example Security Metric	Confi-dentiality	Integrity	Avail-ability	Com-pliance
PO	Plan & Organize					
PO2	Define the Information Architecture	% of Systems compliant with Security Information Architecture	Secondary	Primary	-	-
PO6	Communicate Management Aims and Direction	% of Employees Participating and Passing Security Awareness Training	-	-	-	Secondary
PO7	Manage IT Human Resources	% Users who have undergone yearly background checks. % of position descriptions defining IS roles, responsibilities, skills, and certifications.	Secondary	Secondary	Secondary	Secondary
PO8	Manage Quality	Number of Lines of Code Scanned w/o security bug or concern.	-	Secondary	-	-
PO9	Assess and Manage IT Risks		Primary	Primary	Primary	Secondary
PO9.1	IT and Business Risk Alignment	% critical assets / functions residing on compliant systems	Primary	Primary	Primary	Secondary
PO9.2	Establishment of Risk Context	% critical assets / functions reviewed for physical security risks	Primary	Primary	Primary	Secondary
PO9.3	Event Identification	% of events identified as potentially threatening to critical assets / functions.	Primary	Primary	Primary	Secondary
PO9.4	Risk Assessment	% critical assets / functions reviewed for quantitative risk assessment.	Primary	Primary	Primary	Secondary
PO9.5	Risk Response	% critical assets / functions modified in response to quantiative risk assessment.	Primary	Primary	Primary	Secondary
PO9.6	Maintenance and Monitoring of a Risk Action Plan		Primary	Primary	Primary	Secondary

Source: COBIT – IT Governance Board, Jaquith, 2009

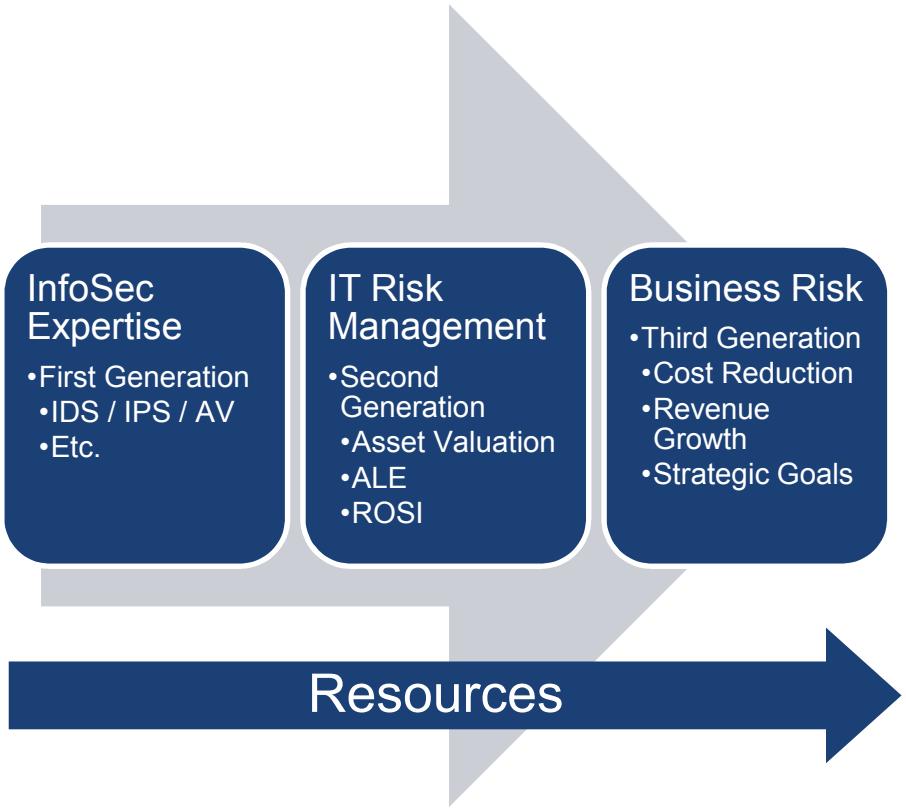
© 2010 Forrester Research, Inc. Reproduction Prohibited

Step 2: Gauge key stakeholder reporting appetite

Forrester Leadership Boards
Security & Risk Council

© 2010 Forrester Research, Inc. Reproduction Prohibited

Think like a CEO / CFO

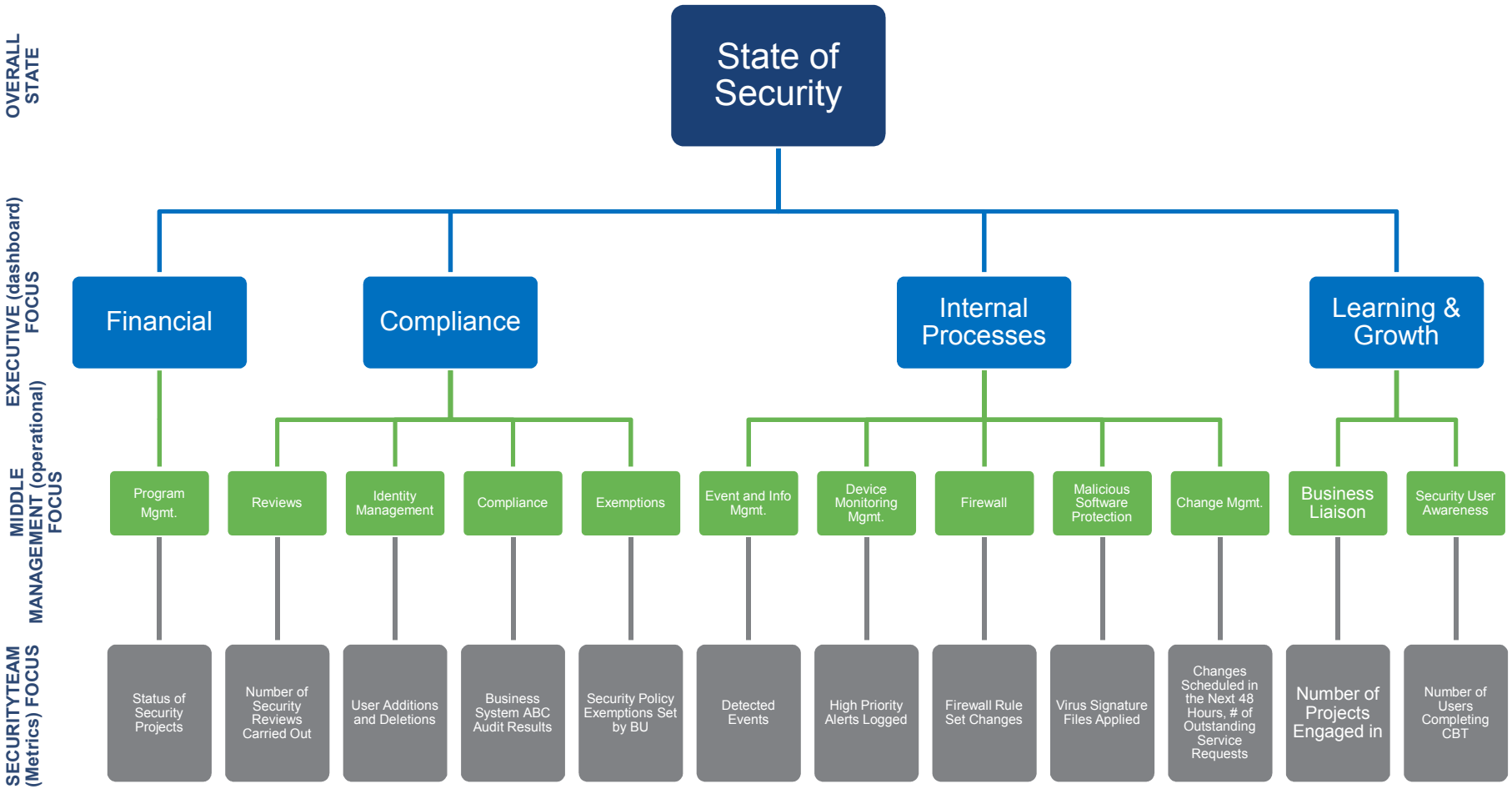


- Responsibilities for CISOs grow but not necessarily the resources to support these new responsibilities.
- How does the CISO get the recognition and resources needed?
- How does the CISO project credibility?

Forrester Leadership Boards
Security & Risk Council

© 2010 Forrester Research, Inc. Reproduction Prohibited

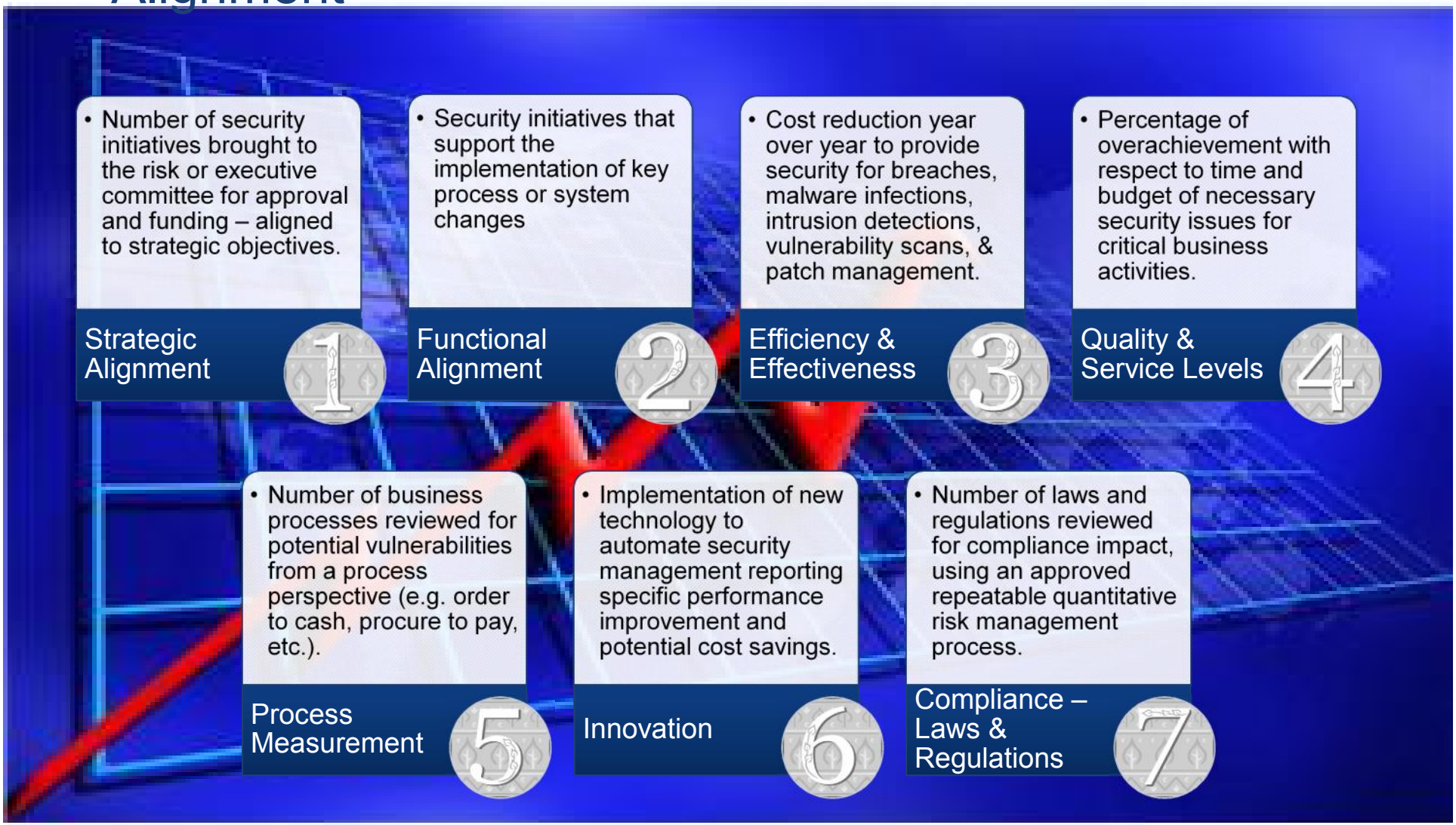
Step 3: Plan an IT security executive reporting framework



FORRESTER LEADERSHIP BOARDS
Security & Risk Council

© 2010 Forrester Research, Inc. Reproduction Prohibited

Step 4: Implement Report – Secure Business Alignment



Use Effective Metrics

- **Consistently Measured** - Provides Benchmarks, opportunity for continuous improvement,
- **Cheap to Gather** – If metrics are expensive to gather they will not be gathered.
- **Use Cardinal Numbers** – Use numbers that show relationships.
- **One Unit of Measure Across Two Dimensions** – Use numbers to show trends.

- **Relevant to Decision Makers** – Are these the numbers the CEO and CFO care about? Why?
- **Actuarially Sound** - Can the information be used for continuous improvement and technical and business risk?
- **Presented Graphically -** A picture speaks a thousand words.

© 2010 Forrester Research, Inc. Reproduction Prohibited

Recommendations

- Focus the benefits of ‘going-live.’
- This is not about fancy products.
- Refine your requirements as you go.
- Improve relationships with vendors.
- Always ask yourself: Who cares?
- Present with confidence.

© 2010 Forrester Research, Inc. Reproduction Prohibited

Thank you

Jinan Budge

+44 (0) 2073237717

+44 (0) 7850203892

jbudge@forrester.co.uk

www.forrester.com

Entire contents © 2010 Forrester Research, Inc. All rights reserved.

FORRESTER LEADERSHIP BOARDS
Security & Risk Council

© 2010 Forrester Research, Inc. Reproduction Prohibited