15.571 Generating Business Value from Information Technology
Spring 2009

Monday April 13, 2009

IT Risk:
Turning Business Threats Into Competitive Advantage

George Westerman
Research Scientist
Center for Information Systems Research (CISR)
MIT Sloan School of Management

This research was made possible by the support of CISR sponsors and patrons.

Preview: Five Ways Executives Can Turn IT Risk Management Into Competitive Advantage

1. Treat IT risk as business risk (The 4 A's).
2. Fix the IT foundation.
3. Create IT risk governance process and structure.
4. Build a risk aware culture.
5. Lead by example.

"My number one issue is around IT risk… The stakes are getting higher every day."
—Financial Services CIO

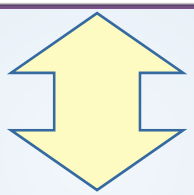
Make IT Risk Relevant: The Four A's

Source: Westerman, G. & Hunter, R., *IT Risk: Turning Business Threats into Competitive Advantage,* Harvard Business School Press, 2007.

The Four A's As Alignment

Enterprise IT Risks

Availability	Access	Accuracy	Agility
• Availability • Business continuity • Disaster recovery	• Information protection • Knowledge sharing • Privacy	• Data accuracy • Data integration	• Cost and speed of strategic change



IT Risk Factors

Technology & Infrastructure	Applications & Information	People & Skills	Vendors & Other Partners	Policy & Process	Organizational
• Infrastructure management effectiveness • Degree of standardization • Technology age	• Architecture complexity • Redundancy • Data consistency • Business process links	• Turnover • Skills planning • Recruiting/ training • IT/Business relationship	• SLAs • Use of firm's methods/ standards • Sole source • Customer risk tolerance	• Controls architecture • IT usage policies • IT governance processes • Regulatory requirements	• Cost cutting • Organizational complexity • Funding processes • Risk history

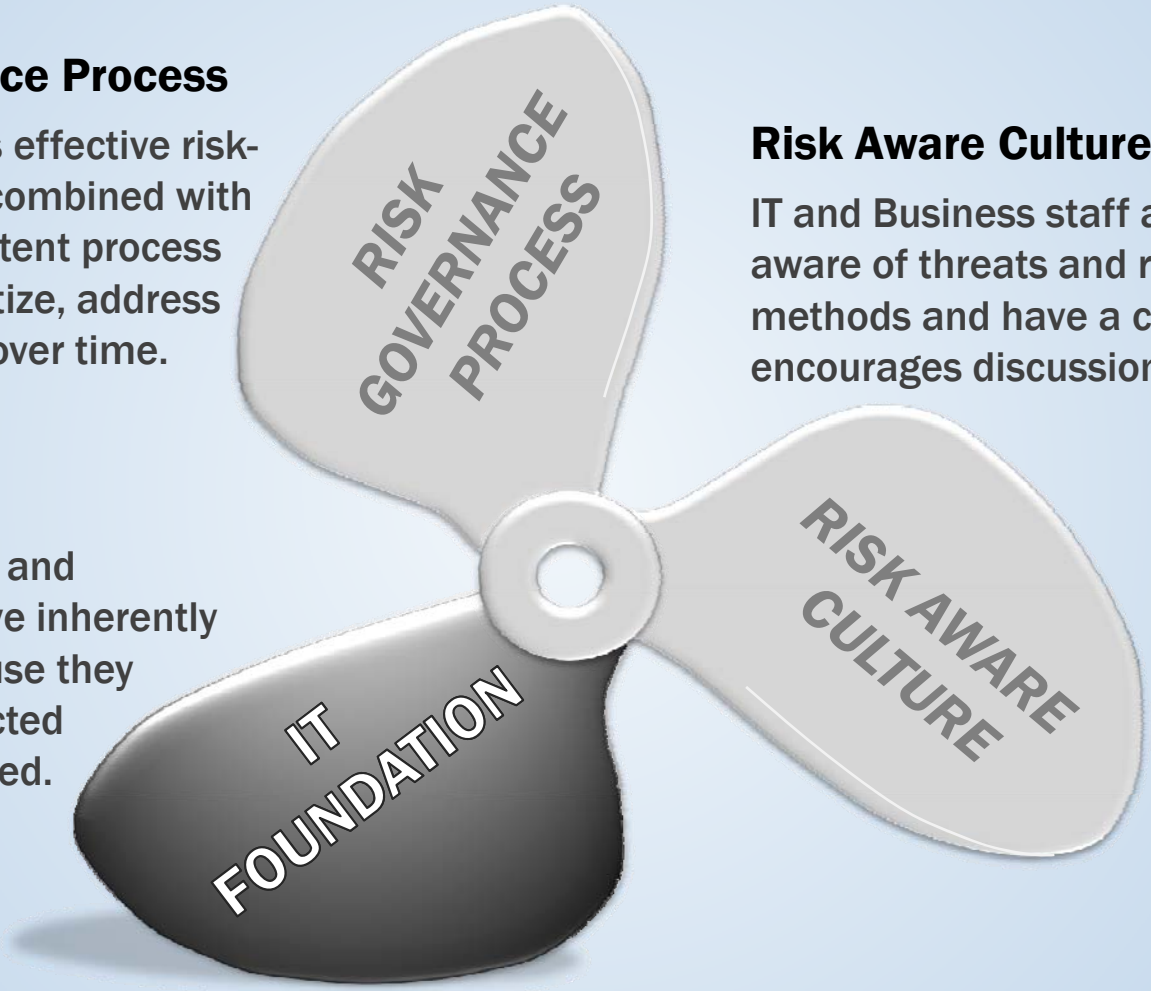
Three Core Disciplines of IT Risk Management

Risk Governance Process

Organization has effective risk-related policies combined with a mature, consistent process to identify, prioritize, address & monitor risks over time.

IT Foundation

IT infrastructure and applications have inherently lower risk because they are well-architected and well-managed.

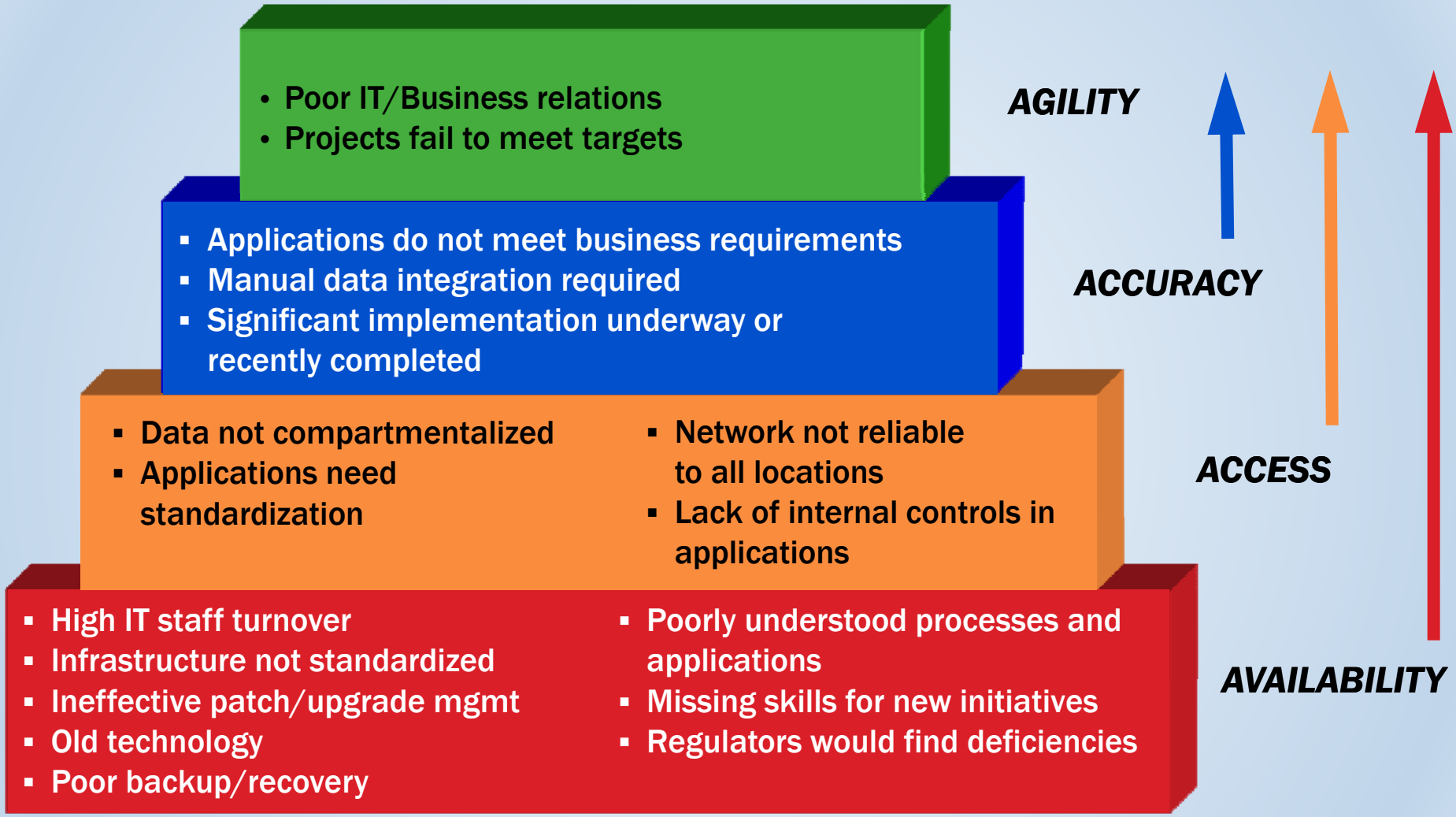


Risk Aware Culture

IT and Business staff are appropriately aware of threats and risk management methods and have a culture that encourages discussion of risk.

Source: Westerman, G. & R. Hunter, *IT Risk: Turning Business Threats into Competitive Advantage*, Harvard Business School Press, 2007.

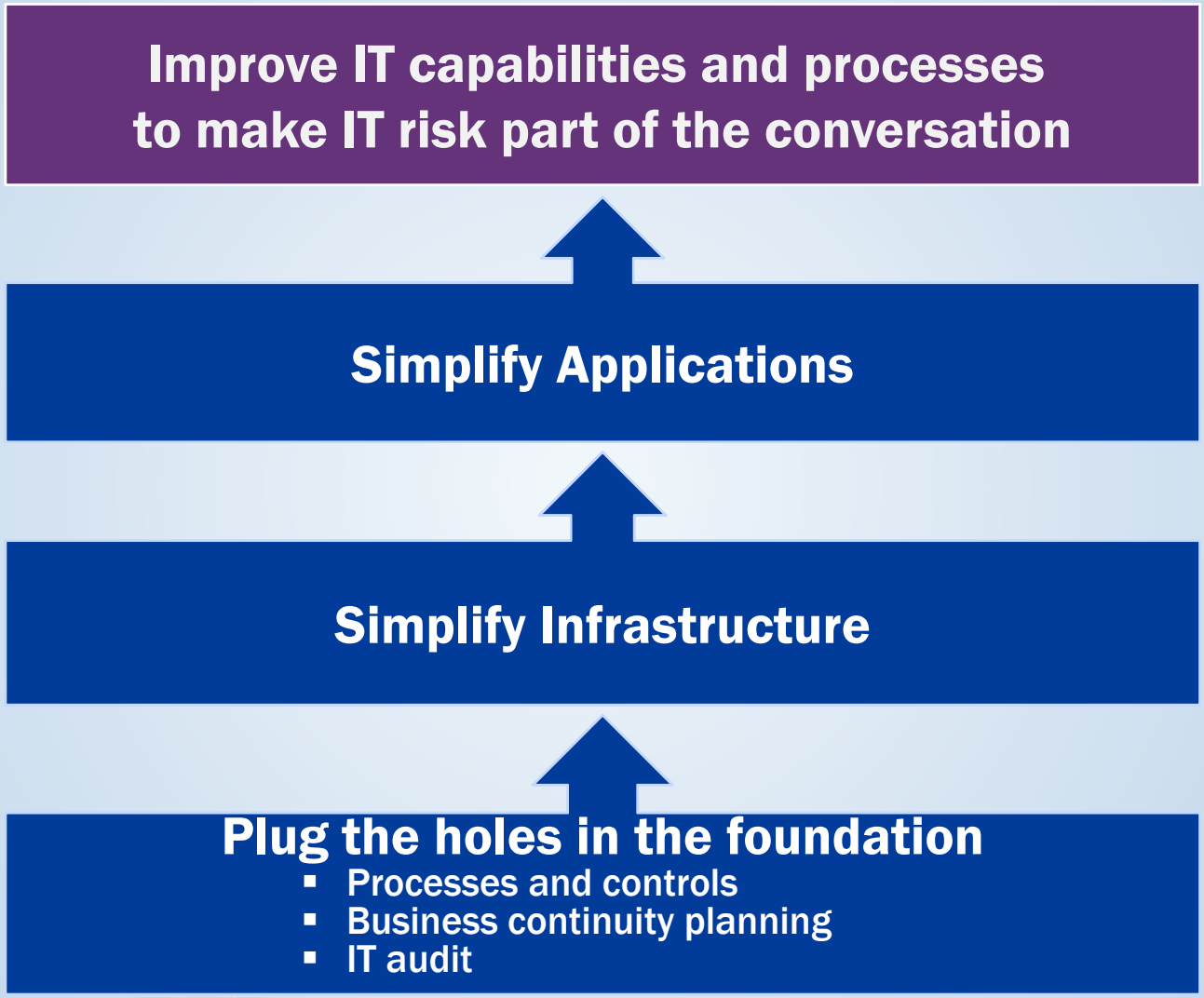
The IT Risk Pyramid



Analysis of 134 surveys shows that risk factors for a given enterprise IT risk (level of the pyramid) are statistically significantly correlated with amount of that risk, and also one or more risks above it in the pyramid.

Source: Westerman, G. & Hunter, R., *IT Risk: Turning Business Threats into Competitive Advantage,* Harvard Business School Press, 2007.

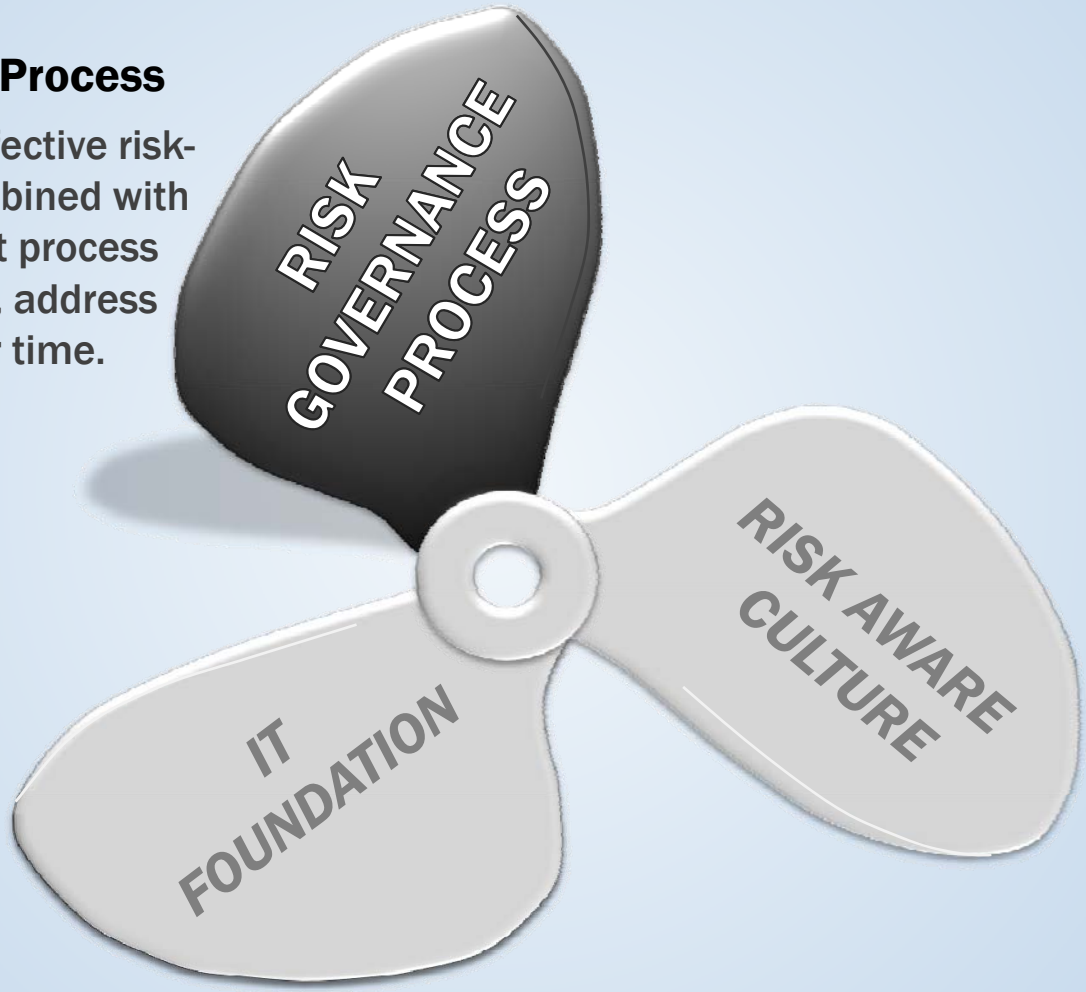
Fixing the Foundation: First Things First



Three Core Disciplines of IT Risk Management

Risk Governance Process

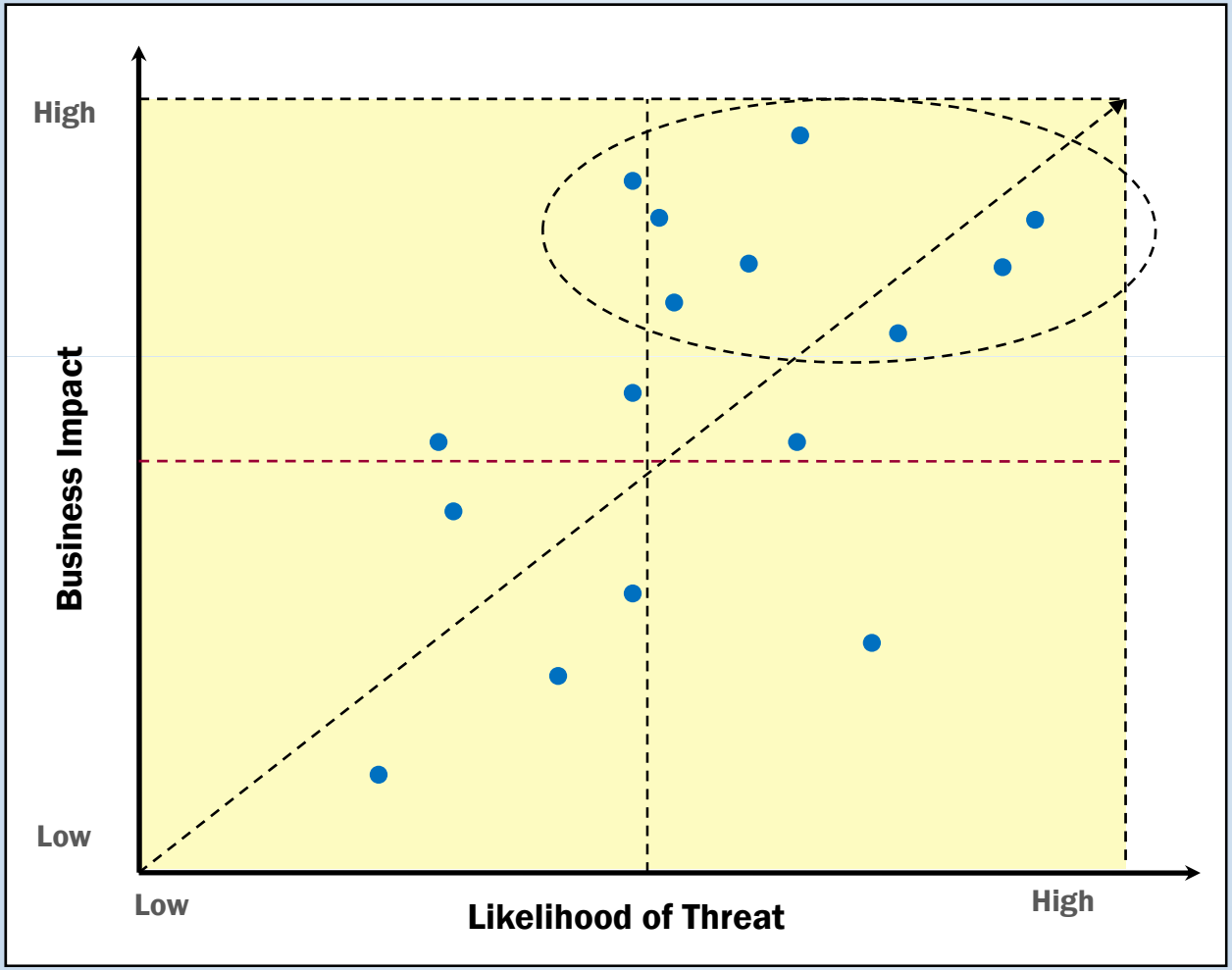
Organization has effective risk-related policies combined with a mature, consistent process to identify, prioritize, address & monitor risks over time.



What Every Parent Knows About IT Risk Management

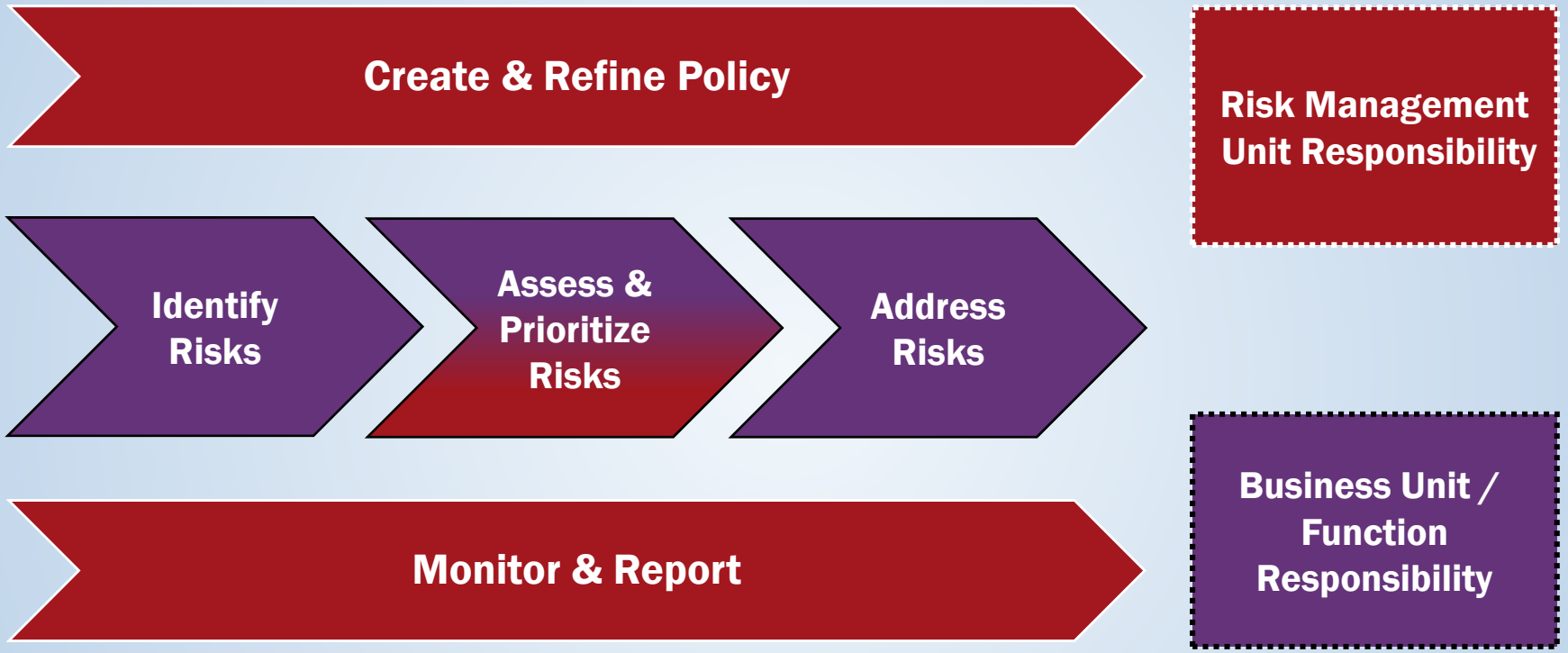
“The Clare Factor”

The Goal of the IT Risk Governance Process: Complete Picture of Risks Across the Enterprise



Source: Westerman, G. & Hunter, R., *IT Risk: Turning Business Threats Into Competitive Advantage*, HBS Press, 2007.

The IT Risk Officer Manages the Risk Process, Not the Risks Themselves



Key Elements for the IT Risk Governance Process

Provide the right resources

- ☑ **Single person in charge of process**
- ☑ **Risk committee**

> ***"My biggest IT risk was not knowing what my risks were."***
>
> —CIO of a global financial services firm

Create the environment for IT risk management

- ☑ **Risk policies**
- ☑ **Best practice frameworks**

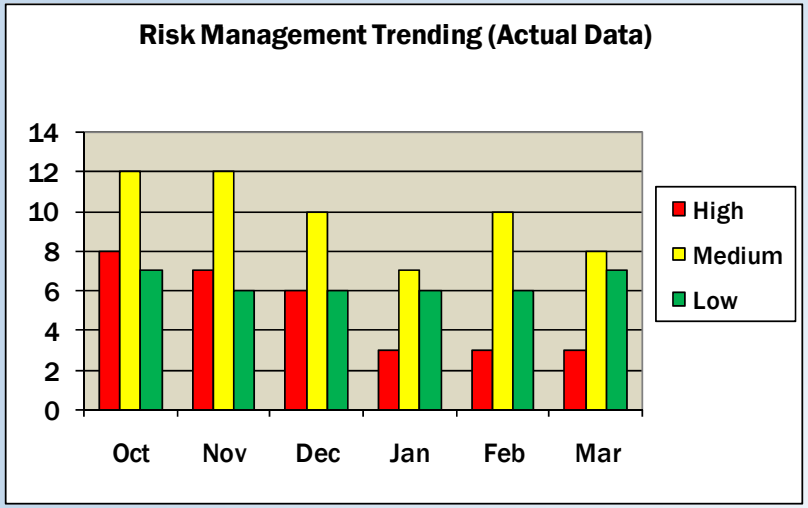
Ensure a consistent view across multiple units and functions

- ☑ **Formal risk categories**
- ☑ **Quantified risk assessments**
- ☑ **Central risk register**

Enterprises using these process elements had statistically significantly mitigated higher levels of *three or more* IT Risks: Availability, Access, Accuracy, and Agility in a global survey of 134 firms.

Source: Westerman, G. & Hunter, R., *IT Risk: Turning Business Threats into Competitive Advantage*, Harvard Business School Press, 2007

PFPC IT Risk Dashboard



RISKS BY RATING

# of Open Issues	Total	Rating: High	Rating: Medium	Rating: Low
Beginning of month	19	3	10	6
New Risks	3	1	0	2
Closed Risks	4	1	2	1
Improved Risk Rating	0	0	0	0
Declined Risk Rating	0	0	0	0
End of Month	18	3	8	7

RISK AGING

Risk Category	Owner	Total	(months) Under 1	1–2	2–3	3–6	6–9	9–12	Over 12
Architecture	Parker	2					1	1	
Financial	O'Reilly	2		1			1		
HR	Johnson	1				1			
Operations	Jacobs	6		2			1	3	
PMO	Amoroso	1		1					
Security	Brown	6	2	1			1	2	
Strategy	Chin	0							
Total		18	2	5	0	1	4	6	0

Source: Adapted from Westerman, G. and Walpole, R., "PFPC: Building an IT Risk Management Competency," MIT CISR Working Paper #352, and Westerman, G. & Hunter, R., *IT Risk: Turning Business Threats into Competitive Advantage*, Harvard Business School Press, 2007.

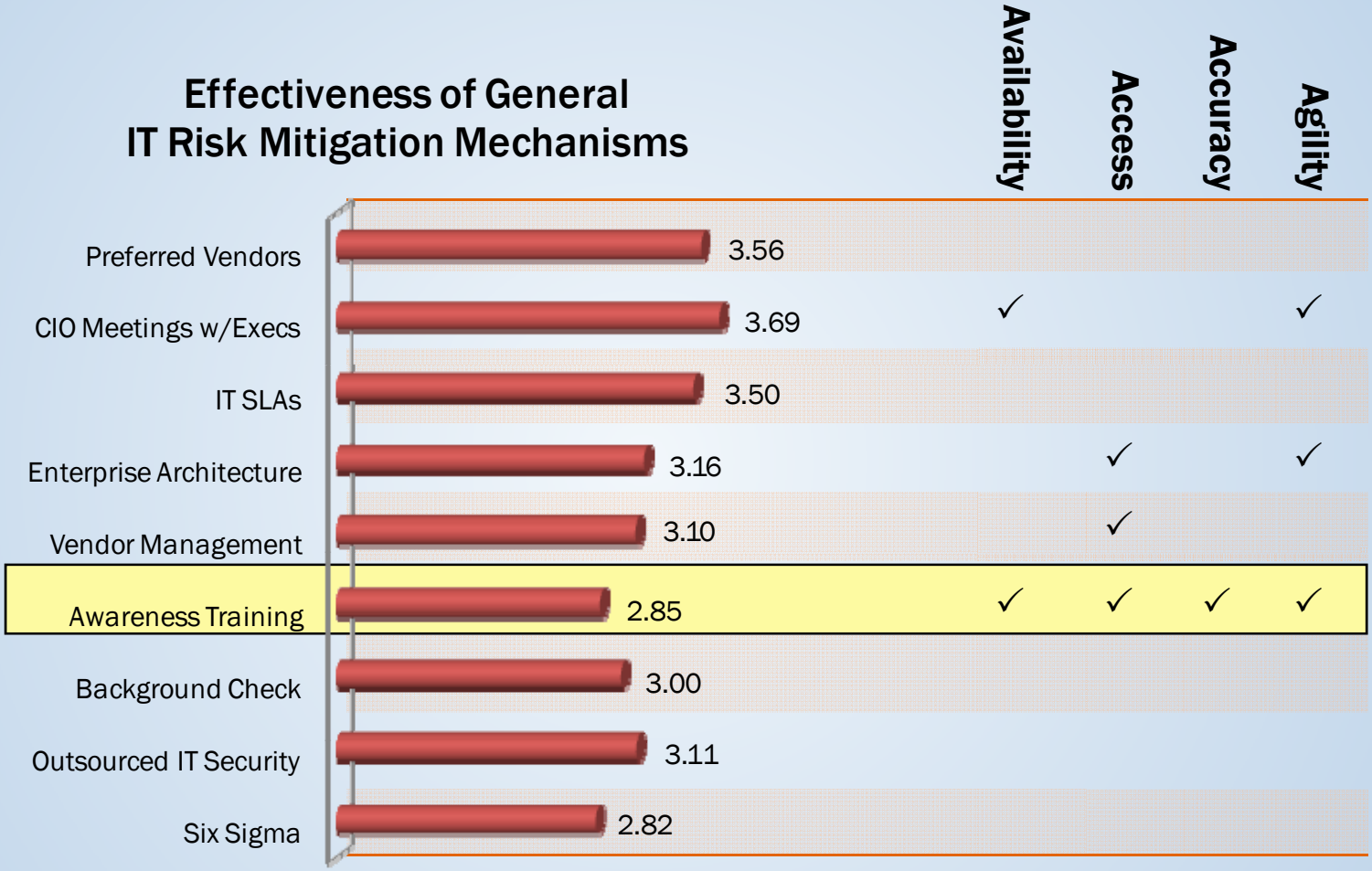
Three Core Disciplines of IT Risk Management

Risk Aware Culture

IT and Business staff are appropriately aware of threats and risk management methods and have a culture that encourages discussion of risk.

Source: Westerman, G. & R. Hunter, *IT Risk: Turning Business Threats into Competitive Advantage*, Harvard Business School Press, 2007.

Awareness Training Is Very Effective
(But a Risk Aware Culture Needs More than Formal Training)



Note: Average Effectiveness scores are on a scale of 1 (Ineffective) to 5 (Highly Effective) as rated by 119 survey respondents. The checkmarks indicate that using the mechanism was associated with statistically significantly more risk mitigation for Availability, Access, Accuracy, or Agility respectively.

Source: Westerman, G. & Hunter, R., *IT Risk: Turning Business Threats into Competitive Advantage*, Harvard Business School Press, 2007.

"Teachable Moments:" Opportunities to Make IT Risk Part of the Conversation

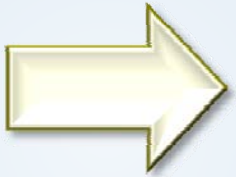
- Project manager under-communicates risks
- Business unit wants to buy cool new software-as-a-service
- Debate over acquisition integration
- Different units (or vendors) use different software development methodologies or standards
- Internal auditor identifies many tiny risks
- Salespeople independently start "IM-ing" with clients

… and many more.

Changing the Risk Culture at Celanese

Risk Averse Culture

- Avoids risk
- Padded budgets, extended timelines
- Managers assign blame
- Managers do not share risk
- Enterprise unable to take on important risks

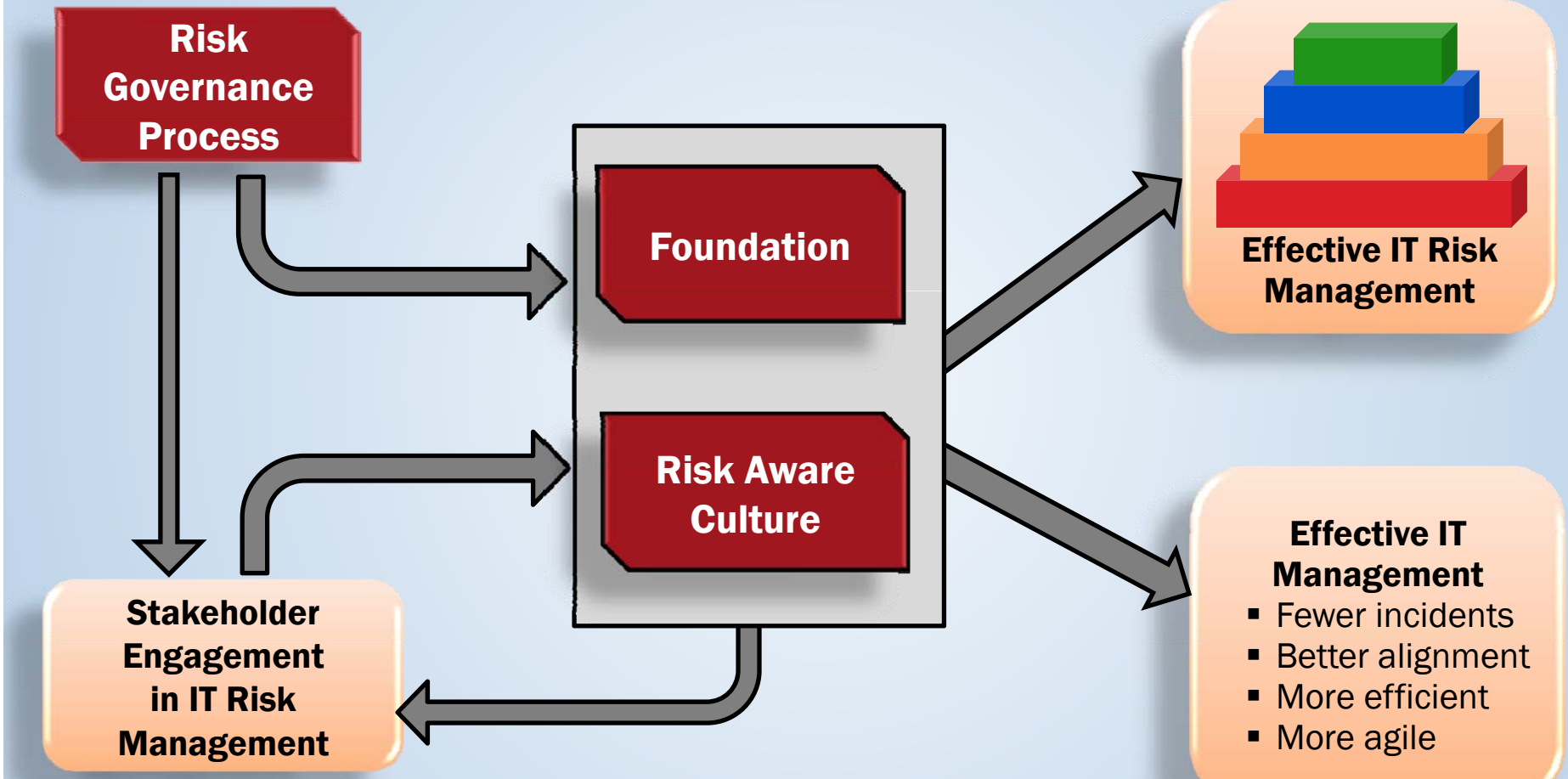


Risk Aware Culture

- OK to talk about risk
- OK to take risks
- OK to fail (if managing appropriately)
- Managers actively share risks and risk management
- Enterprise able to take on bigger risks

Source: Westerman, G. & Hunter, R., *IT Risk: Turning Business Threats into Competitive Advantage*, Harvard Business School Press, 2007.

IT Risk Management and Business Value



Arrows represent statistically significant correlations between IT risk discipline maturity and value outcomes in a joint MIT CISR / IBM global survey of 258 senior IT and non-IT executives.

Turning IT Risk Management Into Business Value

- **Change the mindset about IT risk management**
  - Discuss IT risk in business terms (the four As)
  - Integrate silos of risk management
  - IT risk as opportunity to improve capability, not avoid failure
- **Use risk governance process to improve the foundation**
  - Business continuity or IT Audit to get started
  - Incorporate risks into project initiation discussions
  - Focus on improving foundation, not just bolting on protections
- **Promote risk aware culture**
  - Lead by example
  - Achieving greatness, not just staying safe
- **Use your risk-enabled IT capability for business advantage**