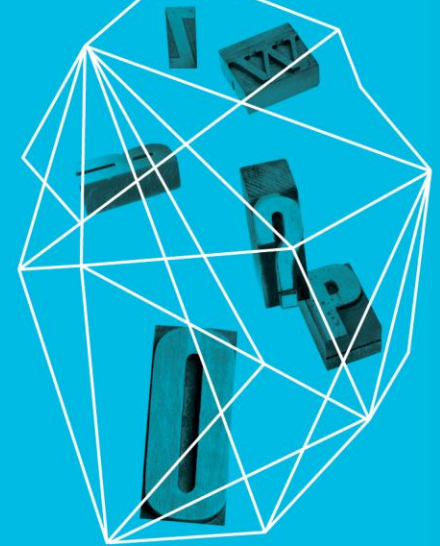


MANAGING RISK WHEN EVERYTHING IS CHANGING

Ron Hale Ph.D., CISM
ISACA

Ed Moyle, CISSP
ISACA

Security in
knowledge



Observations

- ▶ Technology change is accelerating
- ▶ Change is impacting expectations about information, communications, information services, and how organizations deploy and benefit from technology
- ▶ Change is causing users and IT to reform how they work
- ▶ Change creates great opportunity as well as great risk
- ▶ Not being able to manage risk and to create value will cause some enterprises to fail
- ▶ Some best performing organizations are adapting to change
- ▶ These organizations could serve as a model

**The Challenge -
Everything seems
to be changing so
rapidly that
expectations
about risk and
value and how to
manage these is
no longer clear.**



Change is Driven by the Combined Force of Computing, Communications, and Storage Advancements and the Resulting Growth in Content



Computing X Communications X Storage X Content

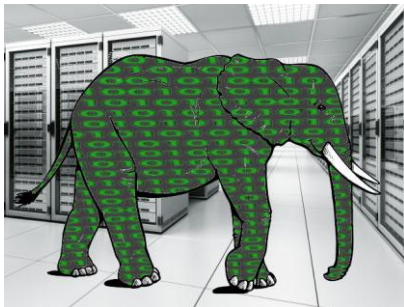
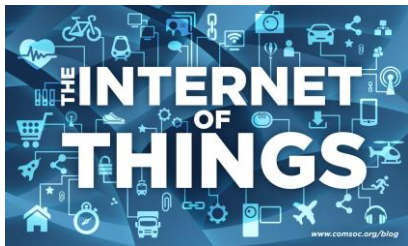
Doubles
Every
18
Months

Doubles
Every
9
Months

Doubles
Every
12
Months

Doubles
Every
 2^n
 $n = \# \text{ people}$

Hyper Exponential Pace of Change

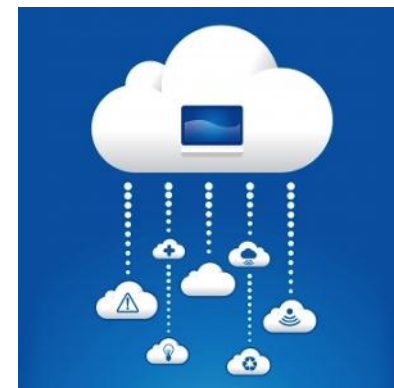


Big Data



Analytics

New technologies bring both opportunities and new risks for enterprises and individuals



Cloud



Social Media



Consumerization



Gamification

Access to new technologies is encouraging a change in how individuals view technology and information in their private and work lives.



**Smart Phone
Tablet
Mobile Apps
Augmented Reality Glasses
Etc.**

“Risk is a function of how poorly a strategy will perform if the ‘wrong’ scenario occurs.”

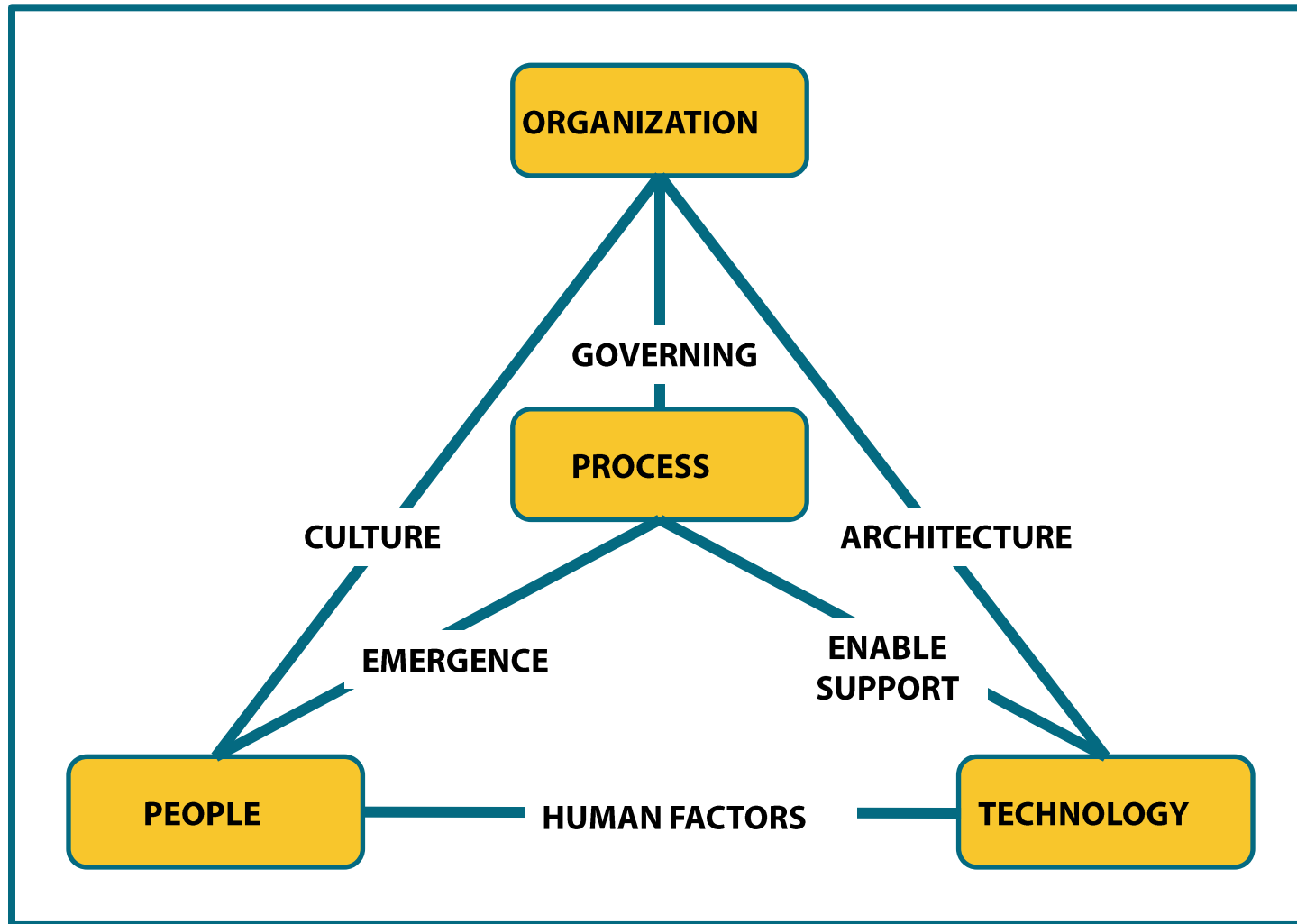
– Michael Porter, Competitive Advantage

Risk Failures

- ▶ Potential interaction of multiple risks are underestimated or disregarded
- ▶ Shortcuts are taken; scenario planning underutilized
- ▶ Risk managers isolated in silos
- ▶ Warnings are ignored; those who deliver warning are seen as not being team players
- ▶ Short-term perspective and single-minded focus
- ▶ Lack of comprehensive enterprise-wide risk management program
- ▶ Risk focused on compliance rather than performance

Deloitte

Creating a strategy to manage change, to capture value, and reduce risk, requires a holistic view



ISACA Business Model for Information Security

Learning From Best Performing Enterprises



How High Performance Enterprises Manage Technology Related Risks

Best Performers drive more value and less risk from the use of IT

- Use simple approaches to manage more value and less risk from IT
- Implement specific practices to transform data-driven decision-making into compelling competitive advantage

As a result they

- Post higher revenues and profit
- Achieve greater customer attraction and retention levels
- Experience lowest rates of business disruption and problems from IT
- Have the fewest problems with regulatory audits

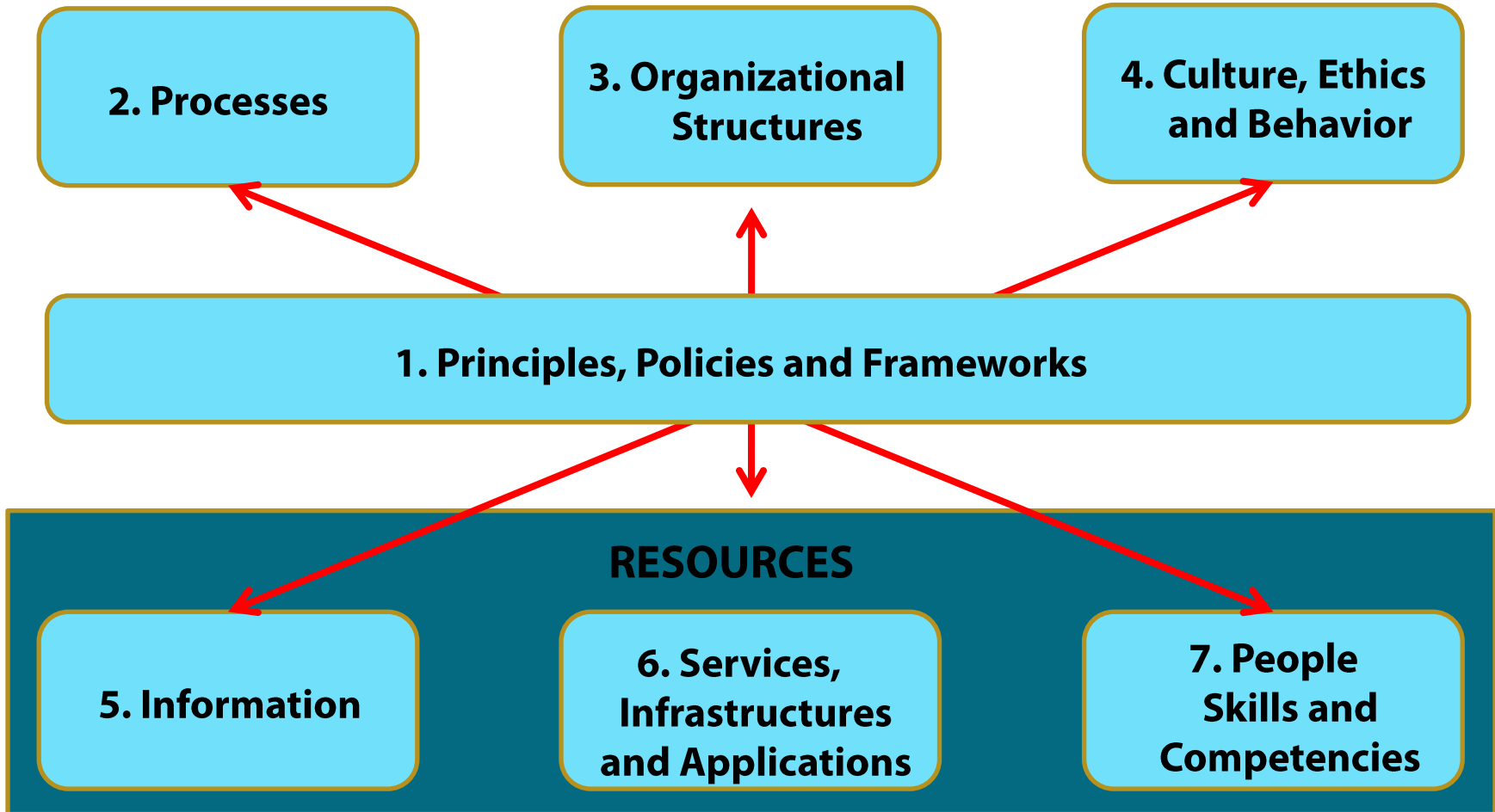
IT Policy Compliance Group 2011

Different Views of Risk Management: Trust Professionals vs. Business Lines



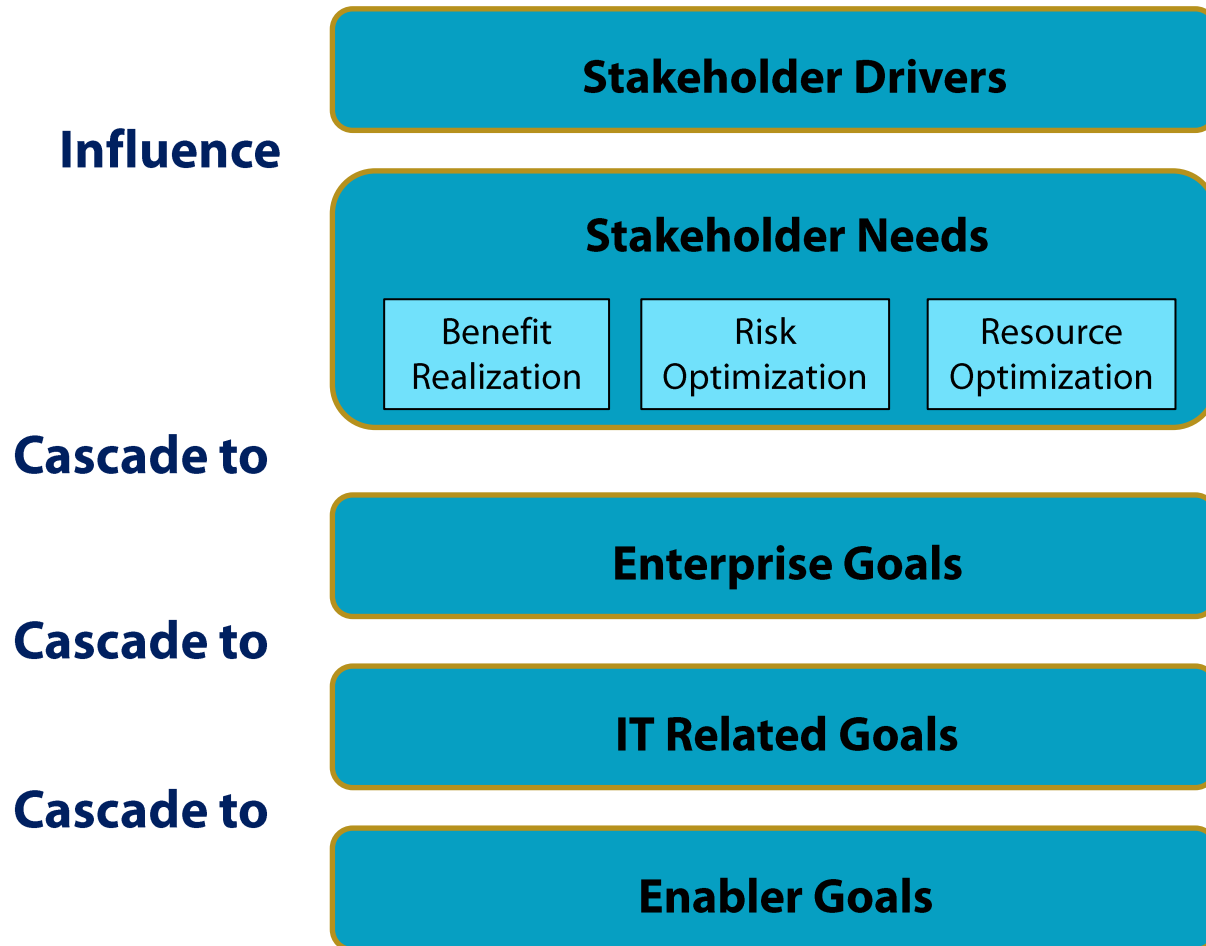
**IT
Information Security
Risk Management
Assurance**

Enterprise Enablers: Core Components for Managing Change



ISACA COBIT 5

Defining the 'business strategy' to avoid risk and optimize value requires an understanding of stakeholder needs and related goals.



Best Practices - Policy, Assessment and Response Planning

External Fraud

Losses from external thefts and fraud
 Losses from external system activities, hacking, theft of information

Policy
 Procedure
 Process

Risk
 Assmt

Response
 Plans



Internal Fraud

Losses from internal fraud and unauthorized transactions
 Losses from internal thefts, credit card fraud, embezzlement



Client, Product, Business Practices

Losses from breach of privacy, misuse of confidential information
 Losses from insider trading, money laundering
 Losses from product defects, system design, implementation integration



Damage to Physical Assets

Losses from natural disasters, vandalism
 Losses from business disruption



P <= 0.05 P > 0.05

Best Practices - Risk Management Activities

	Identify Risks	ID Product Risks	Profile Risks	Inform Mgt of Risks	Tech & Op Controls
External Fraud					
Losses from external thefts and fraud	█	█	█	█	█
Losses from external system activities, hacking, theft of information	█	█	█	█	█
Internal Fraud					
Losses from internal fraud and unauthorized transactions	█	█	█	█	█
Losses from internal thefts, credit card fraud, embezzlement	█	█	█	█	█
Client, Product, Business Practices					
Losses from breach of privacy, misuse of confidential information	█	█	█	█	█
Losses from insider trading, money laundering	█	█	█	█	█
Losses from product defects, system design, implementation integration	█	█	█	█	█
Damage to Physical Assets					
Losses from natural disasters, vandalism	█	█	█	█	█
Losses from business disruption	█	█	█	█	█

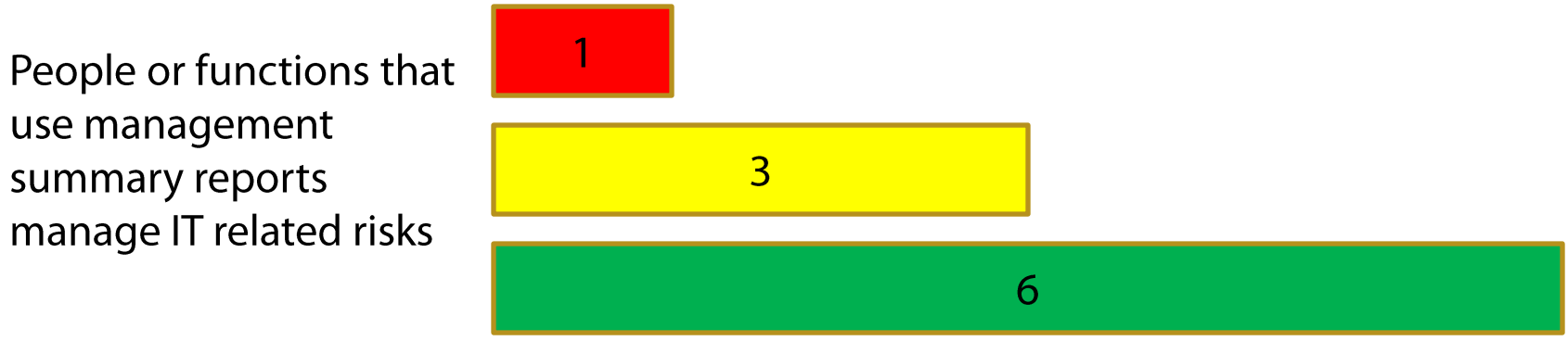
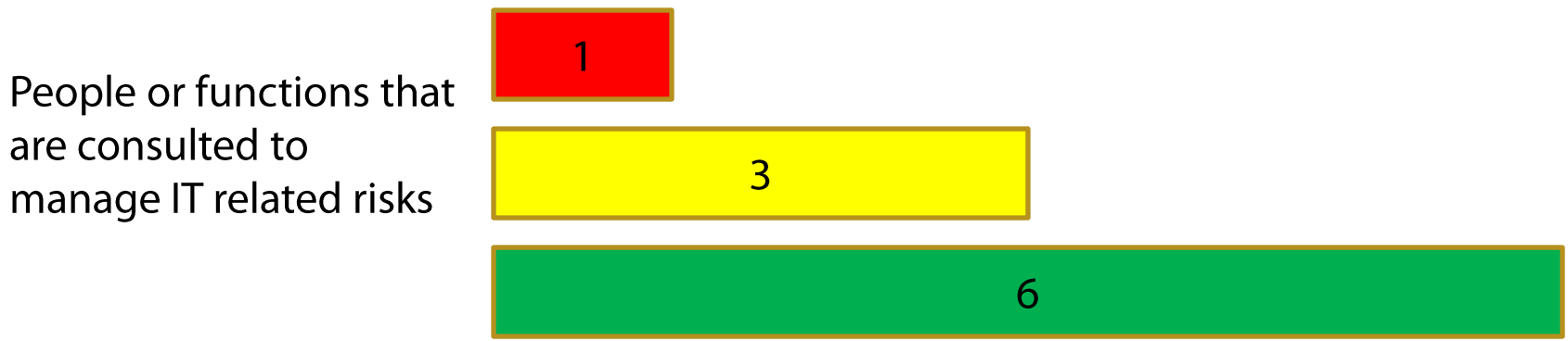
█ P ≤ 0.05
 █ P > 0.05

Best Practices – Involvement in Managing Business Risks

Outcomes	People or functions consulted to manage IT related risks	People or functions that use management summary reports to manage IT related risks
Worst Outcomes	Business unit managers	Senior managers
Average Outcomes	Senior IT managers Legal and financial managers Business unit managers	Senior managers IT operations managers Information security managers
Best Outcomes	IT operations managers Internal auditors Business unit managers Legal and financial managers Risk and compliance managers Information security managers	Senior managers IT operations managers Information security managers Risk managers Internal auditors Legal and compliance managers

IT Policy Compliance Group 2010

Best Practices - Involvement in Managing Business Risks



- Worst Outcomes
- Average Outcomes
- Best Outcomes

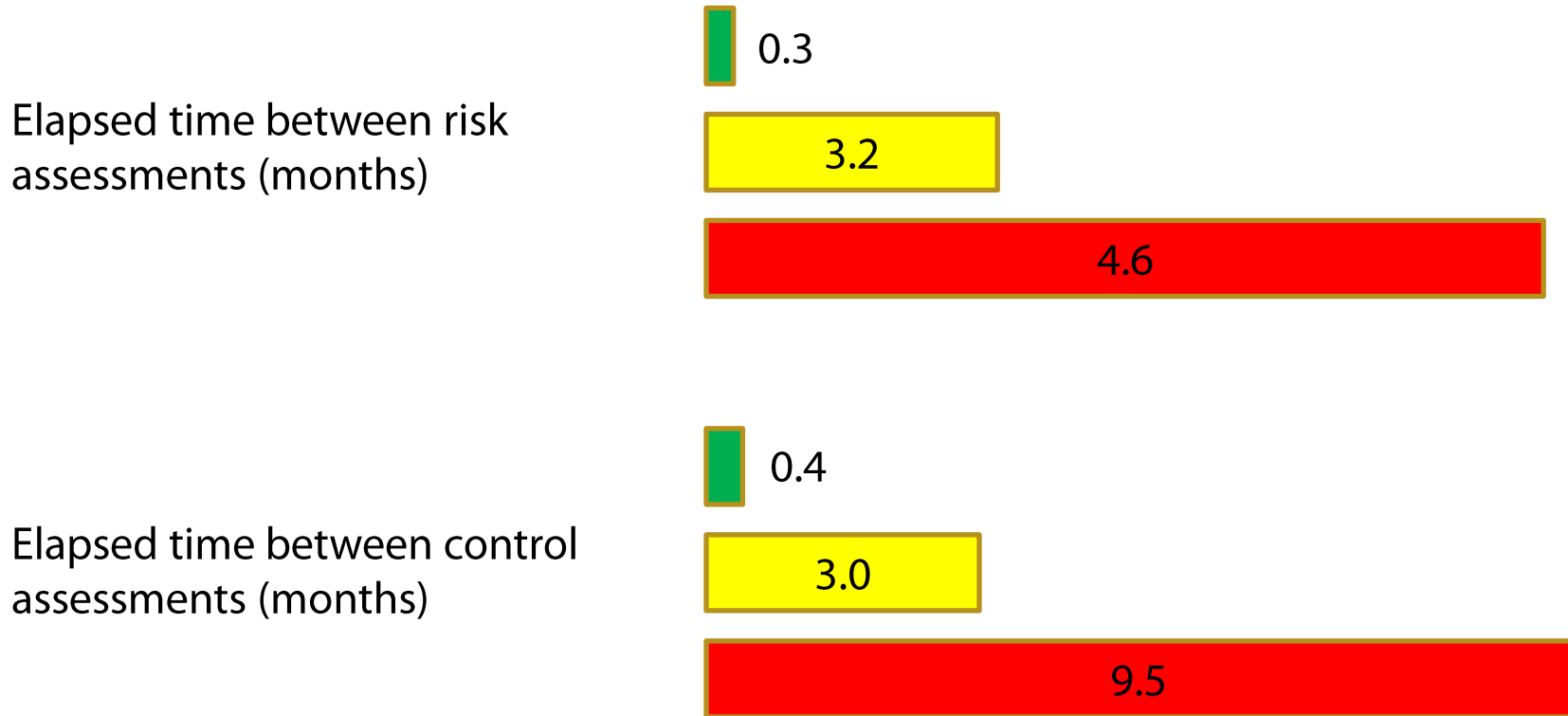
IT Policy Compliance Group 2010

Best Practices - IT Effectiveness Metrics in Management Summary Reports

Metric	Worst 2 in 10	Average 7 in 10	Best 1 in 10
Availability of IT service levels	45%	23%	84%
Integrity of IT assets and information	11%	27%	80%
Integrity of financial systems and data	11%	37%	80%
Integrity of customer data	8%	41%	75%
Integrity of sensitive corporate data	8%	41%	75%
Integrity of audit data and security controls	7%	30%	75%

IT Policy Compliance Group 2010

Best Practices - Frequency of Risk and Control Assessments



- Worst Outcomes
- Average Outcomes
- Best Outcomes

IT Policy Compliance Group 2010

Best Practices - IT Vulnerabilities and Related Threats Covered in Risk Reports

Vulnerabilities / Threats	Worst 2 in 10	Average 7 in 10	Best 1 in 10
Internet security threats	22%	39%	77%
IT vulnerabilities, threats, exploits	10%	31%	65%
Unauthorized use of software / devices	12%	27%	65%
Outstanding fixes for IT vulnerabilities	7%	14%	62%
Outstanding IT change orders	7%	22%	62%
Unauthorized user accounts or changes in entitlements	10%	26%	46%

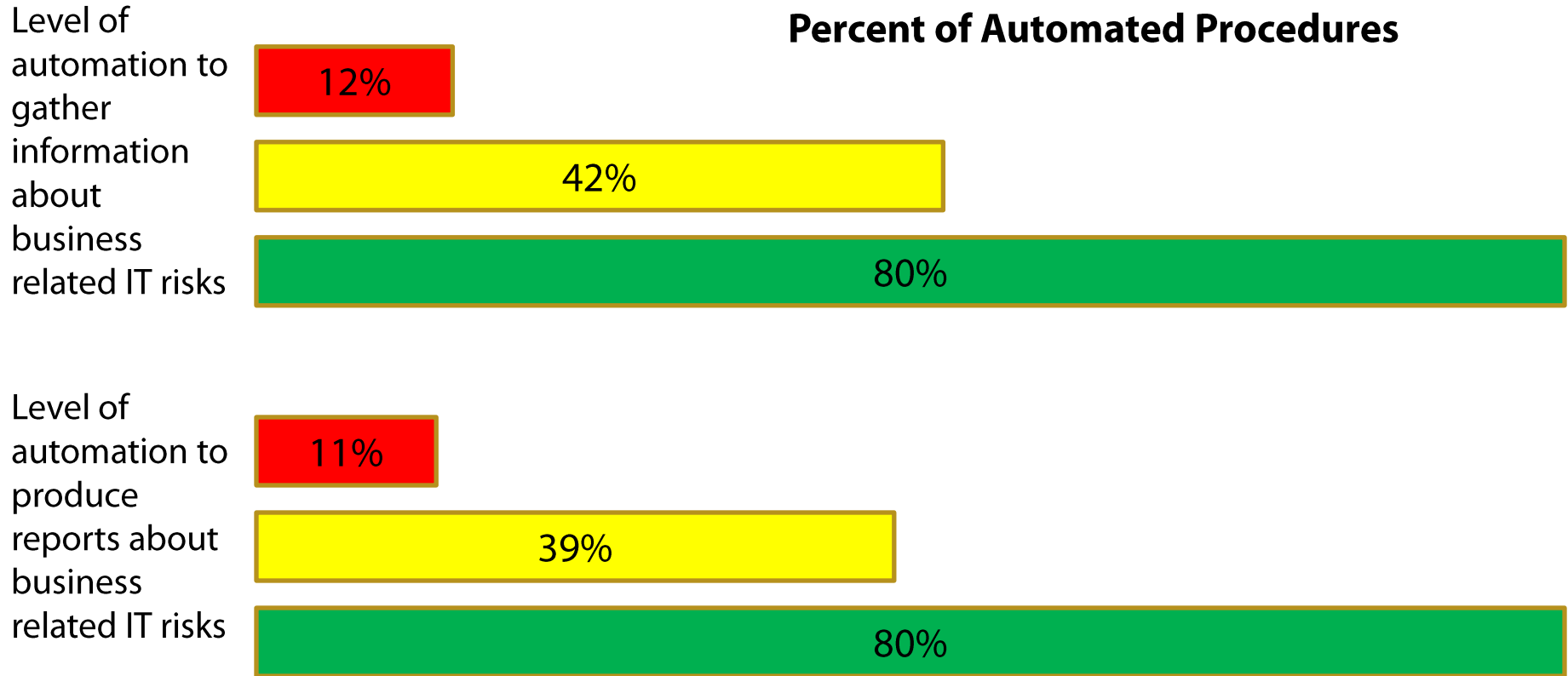
IT Policy Compliance Group 2010




Best Practices - Trends Covered in Management Summary Reports

Trend (Changes Reported)	Worst 2 in 10	Average 7 in 10	Best 1 in 10
In internet security threats	27%	32%	73%
In risks and priorities	7%	30%	69%
In data loss, misuse, theft	17%	27%	69%
In IT vulnerabilities and exploits	22%	20%	69%
In IT control failures	12%	27%	65%
In exceptions to policy	7%	20%	50%

IT Policy Compliance Group 2010

Best Practices - Automation to Gather Information and Produce Risk Reports



-  Worst Outcomes
-  Average Outcomes
-  Best Outcomes

IT Policy Compliance Group 2010

Best Practices - Reports Used to Manage IT Related Business Risk

Reports Used	Worst 2 in 10	Average 7 in 10	Best 1 in 10
Business impact summary reports	8%	29%	68%
Email and phone notifications	36%	34%	68%
Written reports	28%	26%	68%
Exception reports	14%	29%	55%
Risk priority reports	11%	29%	46%
Web-based dashboard reports	8%	22%	41%

IT Policy Compliance Group 2010

Best Practices - Human Behaviors Covered in Reports

Human Behavior	Worst 2 in 10	Average 7 in 10	Best 1 in 10
Training delivered to employees	49%	62%	76%
Employees surveyed on policies and ethics	24%	50%	71%
Employees are surveyed on procedures and practices	43%	58%	59%
Process controls are mapped against policy, regulatory and legal requirements	19%	60%	74%
Gaps in process controls are identified and remediated	17%	49%	88%
Conformance with policy is documented and reported	46%	68%	73%

IT Policy Compliance Group 2010

Leading Enterprise Results - Financial Outcomes

Outcomes	Worst 2 in 10	Average 7 in 10	Best 1 in 10
Business downtime due to IT failures / . disruptions	10% of revenue	1% of revenue	0.2% of revenue
Loss or theft of sensitive data including customer data	9.6% of revenue	6.4% of revenue	0.4% of revenue
Relative spend in time spent in TI and money spent on regulatory audit	\$0.60	\$1.00	\$0.30

IT Policy Compliance Group 2010

Leading Enterprise Results - Operational Outcomes

Outcomes	Worst 2 in 10	Average 7 in 10	Best 1 in 10
Business downtime due to IT failures / disruptions	More than 60 hours	4 to 59 hours	Less than 4 hours
Loss or theft of sensitive data including customer data	16 or more events	3 to 15 events	Less than 3 events
Deficiencies in IT that had to be corrected to pass audits	16 or more deficiencies	3 to 5 deficiencies	Less than 3 deficiencies

IT Policy Compliance Group 2010

Best Performer Practices

- ❑ Easy to follow risk-reward practice involving identification, response, measurement, communications and refinement to manage results
- ❑ Simple – effective approach to quantify business risk and reward
- ❑ Highly automated procedures to gather information and report on change impacting both business value and risk
- ❑ Simple but effective approach to funding improvements
- ❑ Short reporting cycles focused on managing change
- ❑ Simple but effective contextual scorecards
- ❑ Prescriptive scorecards containing information relevant to stakeholders
- ❑ Prescriptive scorecards containing comparisons against objectives and requirements
- ❑ Credible information in drill-downs
- ❑ Refinement through the use of value, risk, performance, composite indicators and benchmarks

Best Performer Profile

- ❑ Revenue and profits 5% higher than average
- ❑ Customer attraction and retention 5% higher than industry average
- ❑ Business disruptions 90% lower than average
- ❑ Audit deficiencies 90% lower than industry average
- ❑ Spending on IT for top line growth that is 70% higher than average
- ❑ Spending on information security to manage risk that is 100% higher than average

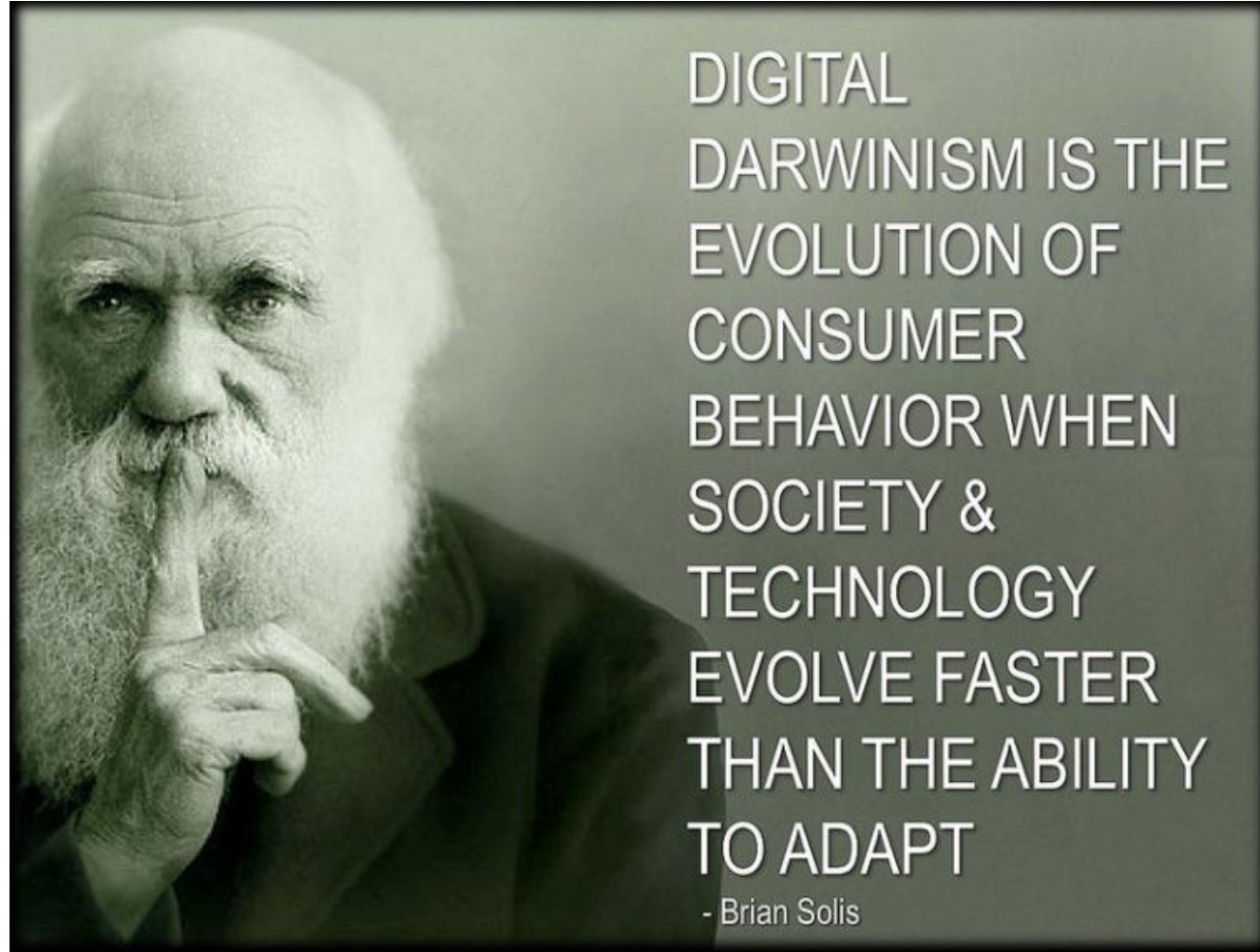
IT Focus

- ✓ Customer attraction
- ✓ Customer retention
- ✓ Financial opportunity
- ✓ Competitive advantage

Security Focus

- ✓ Manage unacceptable / uncontrolled risk
- ✓ Manage change
- ✓ Frequent assessment of value, risk, controls
- ✓ Context based communication using scorecards

Digital Darwinism – some organizations will fail, some will thrive, and all will have to evolve.



DIGITAL
DARWINISM IS THE
EVOLUTION OF
CONSUMER
BEHAVIOR WHEN
SOCIETY &
TECHNOLOGY
EVOLVE FASTER
THAN THE ABILITY
TO ADAPT

- Brian Solis

QUESTIONS?



References

COBIT Resources

COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, ISACA, 2012,

www.isaca.org/COBIT

COBIT5: Implementation, ISACA, 2012, www.isaca.org/COBIT

COBIT 5: Enabling Processes, ISACA, 2012, www.isaca.org/COBIT

COBIT 5 for Information Security, ISACA, 2012, www.isaca.org/COBIT

COBIT 5 Assessment Programme, ISACA, 2012, www.isaca.org/COBIT

COBIT 5 for Assurance, ISACA, 2013, www.isaca.org/COBIT (available summer 2013)

COBIT 5 for Risk, ISACA, 2013, www.isaca.org/COBIT (available summer 2013)

COBIT 5: Enabling Information, ISACA 2013, www.isaca.org/COBIT (available summer 2013)

Other Resources

Managing and Communicating the Business Risk of IT, IT Policy Compliance Group, 2012,
www.ITPolicyCompliance.com

How High Performance Organizations Manage IT, IT Policy Compliance Group, 2011,
www.ITPolicyCompliance.com

What Color is Your Information Risk – Today?, IT Policy Compliance Group, 2010,
www.ITPolicyCompliance.com