Trust In, and Value From, Information Systems

What Does It Mean?

Ken Vander Wal, CISA, CPA

ISACA International President

vandeke@gmail.com

2011-2012 Board of Directors

International President
Kenneth Vander Wal
Chicago Chapter

Past International President
Emil D'Angelo
NY Metropolitan Chapter

Past International President
Lynn Lawton
Moscow Chapter

Vice Presidents

Christos Dimitriadis
Athens Chapter

Tony Hayes
Brisbane Chapter

Greg Grocholski
Member at Large

Niraj Kapasi
Hyderabad Chapter

Jo Stewart-Rattray
Adelaide Chapter

Jeff Spivey
Charlotte Chapter

Appointed directors: Marc Vael, Belgium Chapter; Allan Boardman, London Chapter

A Test

Pace of Change of Digital Infrastructure

Digital power =

Computing		Communication		Storage		Content
↓		↓		↓		↓
Moore's law		Fiber law		Disk law		Community law
↓		↓		↓		↓
Doubles every 18 months	x	Doubles every 9 months	x	Doubles every 12 months	x	2^n, where n is number of people

Source: John Seely Brown

Technology Spending Trends

Global spending on all IT (including computing hardware, enterprise software, IT services and telecom) is expected to total US $3.67 trillion in 2011, a 7.1% increase over 2010.

Spending on global IT services is forecast to reach US $846 billion in 2011, a 6.6% increase over 2010.

The computing and hardware segment is poised for the strongest growth among the IT categories with spending expected to grow 11.7% from 2010, to US $419 billion in 2011.

Source: Gartner 2Q 2011 Technology Spending Forecast, July 2011

Business Technology Trends for 2012

1. The high-IQ network effect
2. The enterprise cloud
3. Large data sets
4. Social enterprise
5. Emerging video
6. Personalization
7. IT departments increasingly influenced by users
8. Machine-to-machine-to-people communications
9. Compliance with security standards
10. Energy-efficient business practices

Source: Verizon

Top Ten Technology Trends for 2012

1. **Media tablets and beyond** (bring your own technology)
2. **Mobile-centric applications and interfaces**
3. **Social and contextual user experience**
4. **Application stores and marketplace**
5. **The Internet of everything**
6. **Next-generation analytics**
7. **Big data**
8. **In-memory computing**
9. **Extreme low-energy servers**
10. **Cloud computing** (number 1 on the list for 2011)

Source: Gartner

Speaking of Big Data

We no longer speak using terms like bytes or kilobyte (KB) or gigabytes (GB)

How many bytes in a Terabyte (TB)?

10^{12} (or 2^{40})

Equivalent to roughly 1,610 CDs worth of data

Anyone heard of a Petabyte ?

Or an Exabyte?

1 Petabyte (PB) is 1,024TB
1 Exabyte (EB) is 1,024PB
1 Zettabyte (ZB) is 1,024EB
1 Yottabyte (YB) is 1,024ZB

Top 10 CIO Priorities

10. Improve collaboration
9. Explore cloud computing
8. Get your arms around the consumerization of IT
7. Leverage social media
6. Find the right people
5. Prep for the post-PC era
4. Harness big data
3. Break out of the 80/20 spending trap
2. Make IT one with the business

And the number 1 priority: IT is too darn slow (and needs to get faster)

Source: *InformationWeek*

ISACA Then and Now

THEN	NOW
EDPAA	ISACA
IT auditors…	… and risk managers, privacy officers, compliance professionals, information security experts, IT control and IT governance professionals
CISA…	… and CISM, CGEIT and CRISC
IS Auditing Standards…	… and IS Control Standards
ISACF	IT Governance Institute
COBIT	COBIT 5
7,504 members (y-e 1992)	103,043 members (y-e 2011)

North Texas Chapter Then and Now

# members	1,680 (as of 31 January 2012) Member Growth (as of 31 January each year): 2012 = 1,680 2011 = 1,614 2010 = 1,611 2009 = 1,602 2008 = 1,503 Renewal Percentages (as of 31 January each year) (regional % for comparison): 2012 = 70% (68%) 2011 = 72% (71%) 2010 = 67% (66%) 2009 = 67% (65%) 2008 = 65% (66%)
Year formed	December 1975 (12th ISACA chapter charter)
% members certified	74% Number of Certifieds (Member Certifieds) CISA = 1,172 (1,020) CISM = 260 (234) CGEIT = 81 (81) CRISC = 315 (296)
Awards won	2008 – K. Wayne Snipes Award for Best Very Large Chapter in North America 2009 – K. Wayne Snipes Award for Best Very Large Chapter in North America 2009 – K. Wayne Snipes Award for Best Very Large Chapter Worldwide 2010 – K. Wayne Snipes Award for Best Very Large Chapter in North America

Who We Are, What We Do, and For Whom We Do It

Advocacy for the profession, influence on regulation/ legislation, subject matter expertise

Frameworks & guidance to help enterprises achieve business objectives

Products & services to increase professional value (credibility & capability)

3
Tertiary beneficiary
Indirect benefit
Influencers

2
Secondary beneficiary
Indirect benefit
Organizations

1
Core constituency
Direct benefit
Individuals

Support, endorsement, adoption, recognition, engagement

ISACA

As an independent, nonprofit, global membership association, ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. ISACA helps its members achieve individual and organizational success, resulting in greater trust in, and value from, information systems. Its members and certification holders are qualified and skilled professionals who make a difference.

Vision and Mission

ISACA's vision *(to aspire to as an organization)*

"Trust in, and value from, information systems"

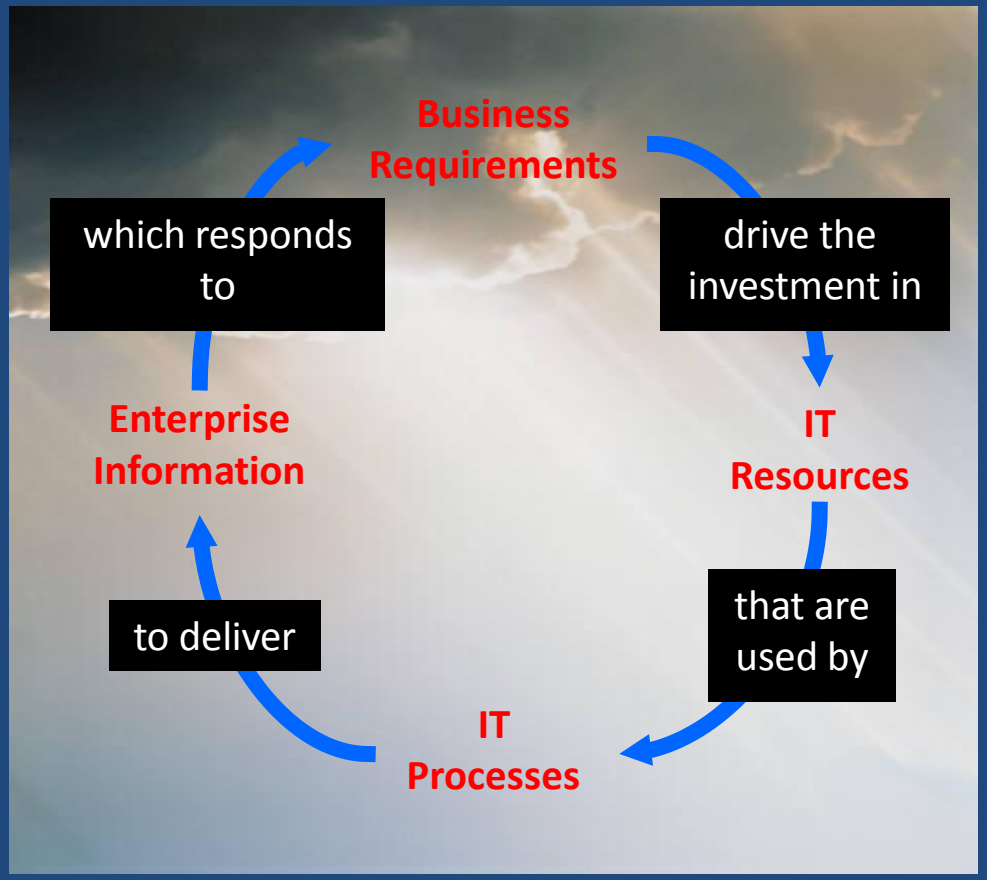
ISACA's mission *(to guide decision making and investments)*

"For professionals and organizations be the leading global provider of knowledge, certifications, community, advocacy and education on information systems assurance and security, enterprise governance of IT, and IT-related risk and compliance"

IT Value Factors

Alignment
- IT and business processes
- Organization structure
- Organization strategy

Integration
- Enterprise architecture
- Business architecture
- Process design
- Organization design
- Performance metrics



Value Defined (Val IT)

- IT is not an end to itself but a means of enabling business outcomes. IT is not about implementing technology. It is about unlocking value through IT-enabled organizational change.
- Value is the total life-cycle benefits net of related costs, adjusted for risk and (in the case of financial value) for the time value of money.
- The concept of value relies on the relationship between meeting the expectations of stakeholders and the resources used to do so.

Trust Defined

***Definition 1*:** Trust is the ability to predict what a system will do in various situations.

***Definition 2*:** Trust is using an information system without having full knowledge about it.

***Definition 3*:** Trust is giving something now (credit card) with an expectation of some future return or benefit (on line purchase).

***Definition 4*:** Trust is being vulnerable (entering private and sensitive information) while expecting that the vulnerabilities will not be exploited (identity theft).

Trust that:

*Private and sensitive information will remain **confidential***

*Process **integrity** is maintained*

*Essential business processes are **available** or recoverable*

Trust in an Information Society

- Systems should give minimum and, as much as possible, measurable guarantees and information on related risks concerning quality of service, security and resilience, transparency of actions and the protection of users' data and users' privacy, in accordance with predefined, acknowledged policies.
- Systems should provide tools and mechanisms (or allow third-party service providers to do so) that enable the user to assess the risks and audit the qualities it is claimed to possess.
- A *bona fide* trustworthy system must also entail quantifiable and auditable technical and organizational aspects of delivery (policies, architectures, service level agreements, etc.), as well as the user's perceptions on its operation.

Trustworthy Computing

Security

Investment in expertise & technology
Responsible leadership and partnering
Guidance and engagement through best practices & education

Privacy

Design, development and testing
Standards and policies
User sense of control over personal information

Reliability

Resilient – continues in the face of internal or external disruption
Recoverable – restorable to a previously known state
Controlled – accurate and timely service
Undisruptable – changes and upgrades do not disrupt service
Production ready – minimal bugs or fixes
Predictable - works as expected or promised

Integrity

Acceptance or responsibility for problems and takes action to correct them

Trust and Value Relationship

Trust creates the opportunity for **Value**
Value is based on an expectation of **Trust**
Assurance binds **Trust** and **Value** together

Certified Information Systems Auditor (CISA)

<u>CISAs</u> provide assurance by conducting audits and assessments of information systems to ensure:

- Information systems risks are measured and managed.
- Information systems and assets are protected and controlled.
- The adequacy of, and compliance with, organizational standards, policies, procedures, processes.
- Information systems controls are efficient and effective.
- Information systems are acquired, developed, implemented and maintained according to established management policies and practices.

Certified Information Security Manager (CISM)

CISMs develop, implement and manage information security activities to ensure:

- Information security risks are identified and managed.
- Information security requirements are integrated into, and maintained throughout, the organization's information systems processes.
- Information security controls are monitored and tested for efficiency and effectiveness.
- Information security roles and responsibilities are defined throughout the organization.
- Information security incidents are managed efficiently and effectively.

Certified in the Governance of Enterprise IT (CGEIT)

CGEITs define, establish, maintain and manage a framework of governance to ensure:

- Business value is achieved from the implementation of information systems.
- Risk management is integrated into business and planning.
- Appropriate management structures, roles, responsibilities and accountabilities are established and strategically aligned.
- Information system processes and controls are comprehensive and repeatable and optimized.
- Investments in information systems and resources are appropriate, measurable and managed.

Survey Results

Top Business/Technology Issues 2011

Top Seven Business Issues Overall

1. Regulatory compliance
2. Enterprise-based IT management and IT governance
3. Information security management
4. Disaster recovery/business continuity
5. Challenges of managing IT risks
6. Vulnerability management
7. Continuous process improvement and business agility

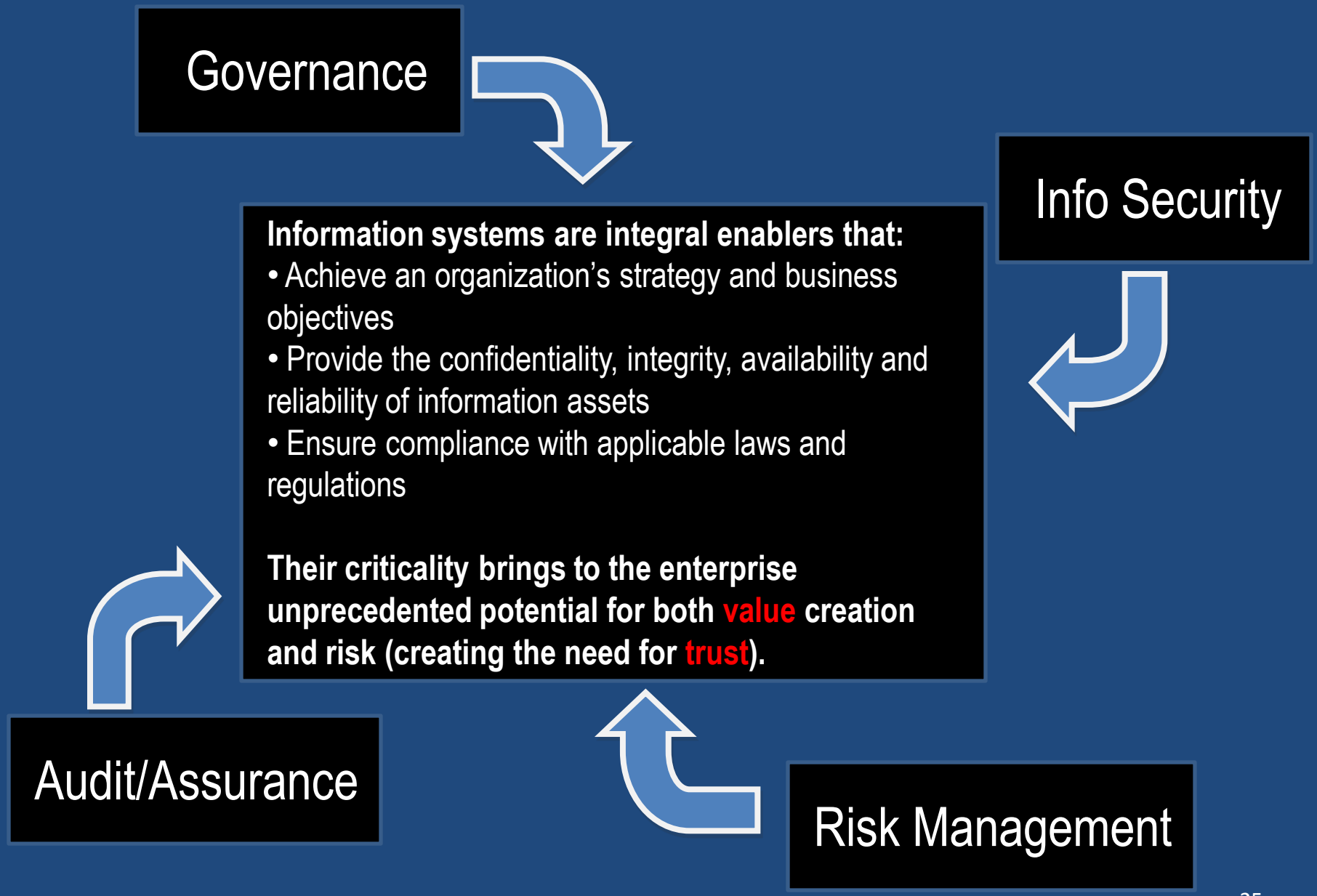
Global Status Report on GEIT

- IT is important in delivering on the business strategy, but there are challenges, notably increasing cost of IT and insufficient IT staff.
- IT is more effective when it can be proactive; it tends to be proactive where it has a seat at the senior executive table.
- Governing IT is a priority and most organizations are making an effort, with the primary results being mitigation of IT-related risk and better communication between IT and the business.
- There is concern about jumping on board with new technologies, particularly in areas of security and privacy.

Certified in Risk and Information Systems Control (CRISC)

<u>CRISCs</u> identify, evaluate and manage risk through the development, implementation and maintenance of information systems controls to ensure:

- Organizational management and stakeholders are aware of risks and how they are being addressed.
- Information systems controls are aligned with business process objectives and risk tolerance levels.
- Information systems controls mitigate risk.
- Information systems control deficiencies are corrected.
- Information systems controls are efficient and effective.


Governance
Info Security
Information systems are integral enablers that:
• Achieve an organization's strategy and business objectives
• Provide the confidentiality, integrity, availability and reliability of information assets
• Ensure compliance with applicable laws and regulations
Their criticality brings to the enterprise unprecedented potential for both value creation and risk (creating the need for trust).
Audit/Assurance
Risk Management

What does all this mean for ISACA members?

Learn Faster

- White papers
- IT audit/assurance programs
- Survey results
- COBIT 5
  - COBIT Process Assessment Model
- Other research
- *Journal* articles

Share Knowledge

- Networking at chapter, regional and international levels
- Knowledge Center on ISACA's web site
- Communicate

Engage

- Volunteer
- Share knowledge
- Attend
- Get a certification
- Comment on exposure drafts

ISACA

Trust in, and value from, information systems

Thank you!

Ken Vander Wal
vandeke@gmail.com

ISACA
info@isaca.org