

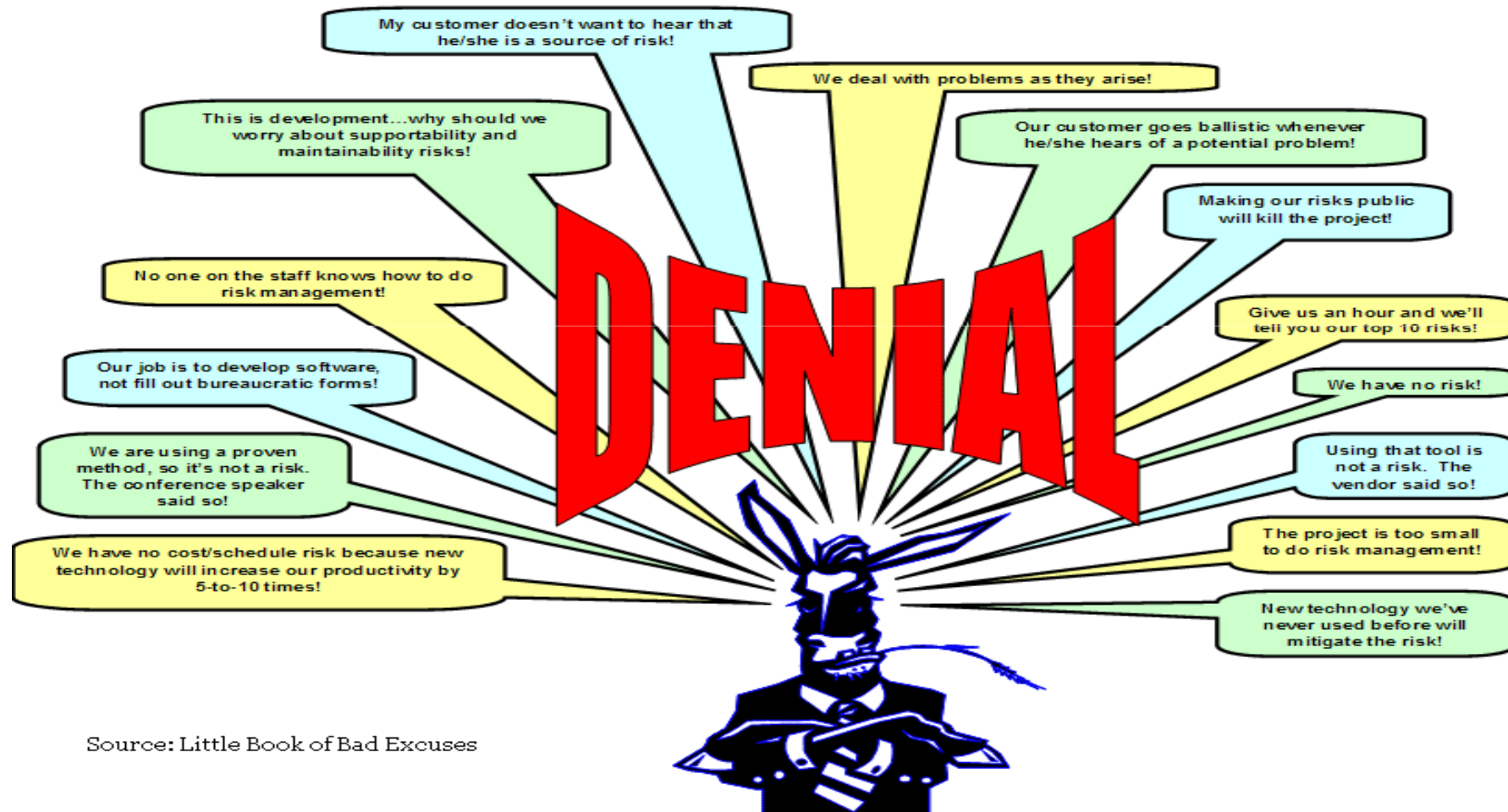
Optimizing your security and business continuity process through integration.



John A. DiMaria; Six Sigma BB, HISP
Director of Professional Services
eFortresses GRC



Excuses!



Source: Little Book of Bad Excuses



eFortresses

Security & Compliance Solutions

Are we comfortably numb?



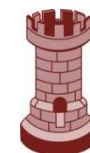
“Hello.

Is there anybody in there?
Just nod if you can hear me.
Is there anyone home? “

Key Implications of Inaction

- Unclear assignment of accountability
- Unclear delegated responsibilities
- Denial of access to information assets
- Denial of customer service
- Assets under or over protected

= Financial cost

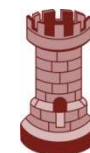
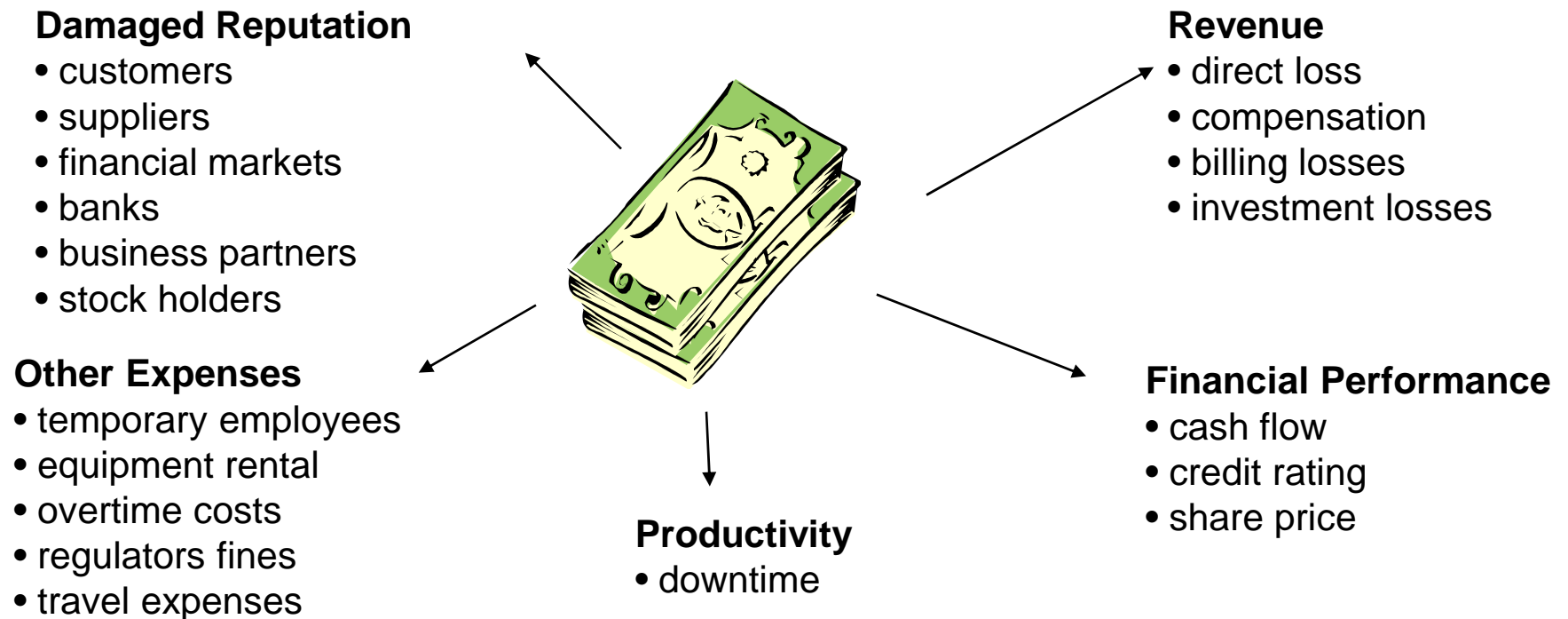


eFortresses

Security & Compliance Solutions

Impact of an Incident

Financial Loss



eFortresses

Security & Compliance Solutions

Don't just stand there!



eFortresses

Security & Compliance Solutions

What are “Standards” ?



Standards set out what are widely accepted as good principles, practices, or guidelines in a given area.

Standards are statements that outline what level of service you can expect to be provided, and how it will be provided.

What standards and guidelines are available

- There are actually a number of different standards and guidelines.
- They are different in the following ways:
 - Country-specific or international
 - Industry-specific
 - Focus (operational risk vs. BCM vs. DR)
 - Depth (are they prescriptive or dictate minimum requirements)
 - Certifiable/Auditable

Why formal standards based programs are used

- Provide a common framework, based on generally accepted best practices for implementing and managing business continuity
- Provide a framework for organizations of any type, size and location
- Improve operational effectiveness of an organization
- Allow for the proactive management of business risks
- Help demonstrate applicable laws, regulations and contractual requirements are being observed
- Bring a common understanding to the marketplace
- Facilitates Integration and complying with other required regulatory requirements

Why formal standards based programs are used

- Growing consensus on what is best practice
- Better understanding of business benefits among increasing numbers of organizations
- Seen as part of overall Risk Management profile
- Help reduce business interruptions, and
- Add value to the business by identifying opportunities for improvement

Consistency of Process

Why a formal standard

- Civil Contingencies / Homeland Security and similar obligations. For the US this means issues related to:
 - **Title IX DHS requirement to protect critical infrastructure**
 - “Implementing Recommendations of the 9/11 Commission Act of 2007”. Includes “Voluntary Private Sector Preparedness Accreditation and Voluntary Certification Program”.
 - FISMA Harmonization with ISO 27001

What BCMS standards and guidelines are available

Example country and standards

- Australian Standards BCM Handbook
- British Standard 25999
- National Fire Protection Association NFPA 1600 (US)
- ASIS BCM Standard
 - US
 - Under Development

Example standards and guidelines for Financial Institutions

- FFIEC BCP Handbook
- NASD Rule 3510
- NYSE Rule 446



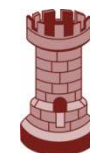
eFortresses

Security & Compliance Solutions

BS 25999

- Authored by the British Standards Institution, BS 25999 replaces PAS 56 as an “umbrella” standard providing a basis for understanding, developing and implementing business continuity within an organization, to integrate risk management disciplines and processes with business continuity, and to provide confidence in business-to-business and business-to-customer dealings.
- BS 25999 Part One, a Code of Practice, provides BCM recommendations
- BS 25999 Part Two, a Specification, provides an auditable management system framework for managing business continuity
- 40 Organizations certified globally
- 160 in pipeline

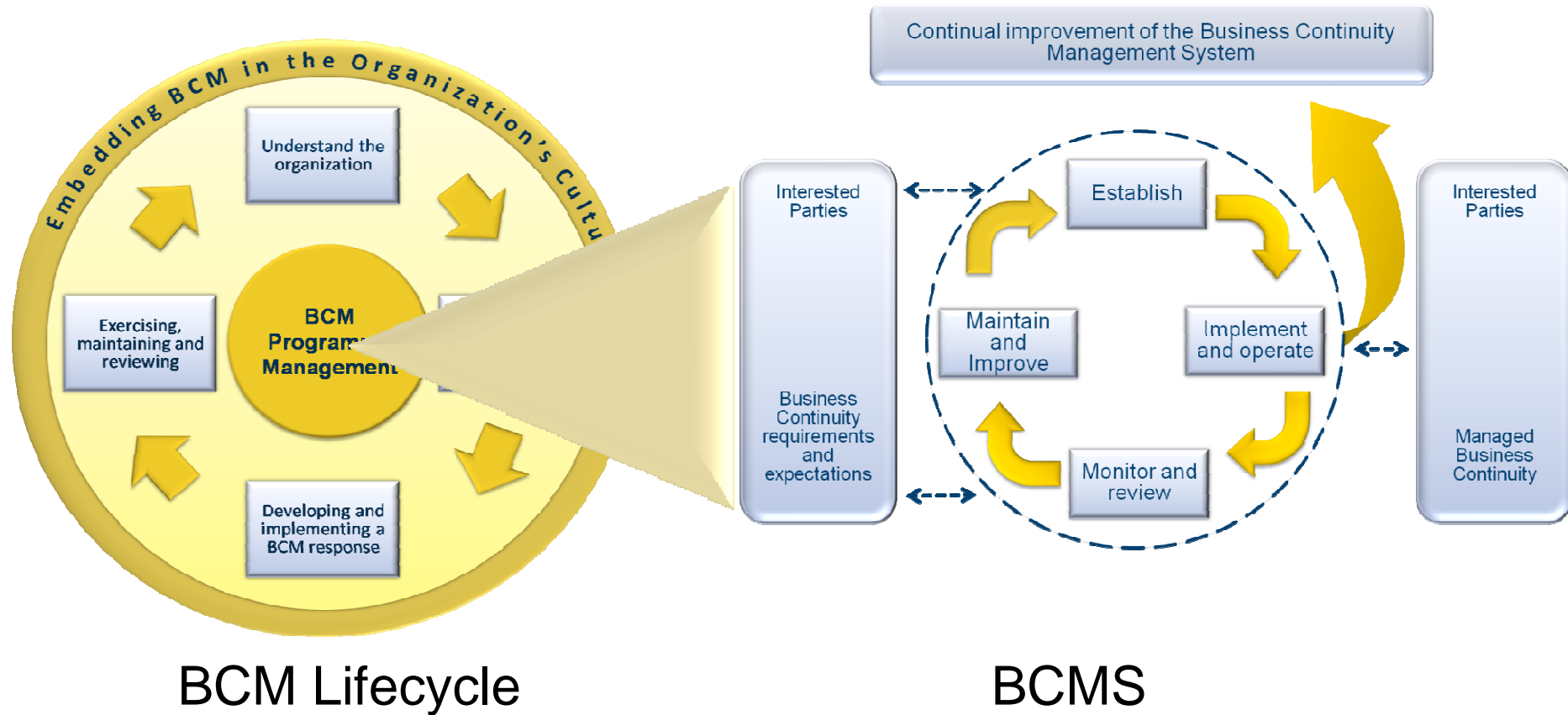
Certifiable



eFortresses

Security & Compliance Solutions

A Management System Process



ISO 20000
IT Service Management

ISO 9001/ISO
14001
Management &
Environmental

BS 25999
BCMS

NFPA
1600

ISO 27001
Information
Security
Management

ISO 9001
Quality Management System

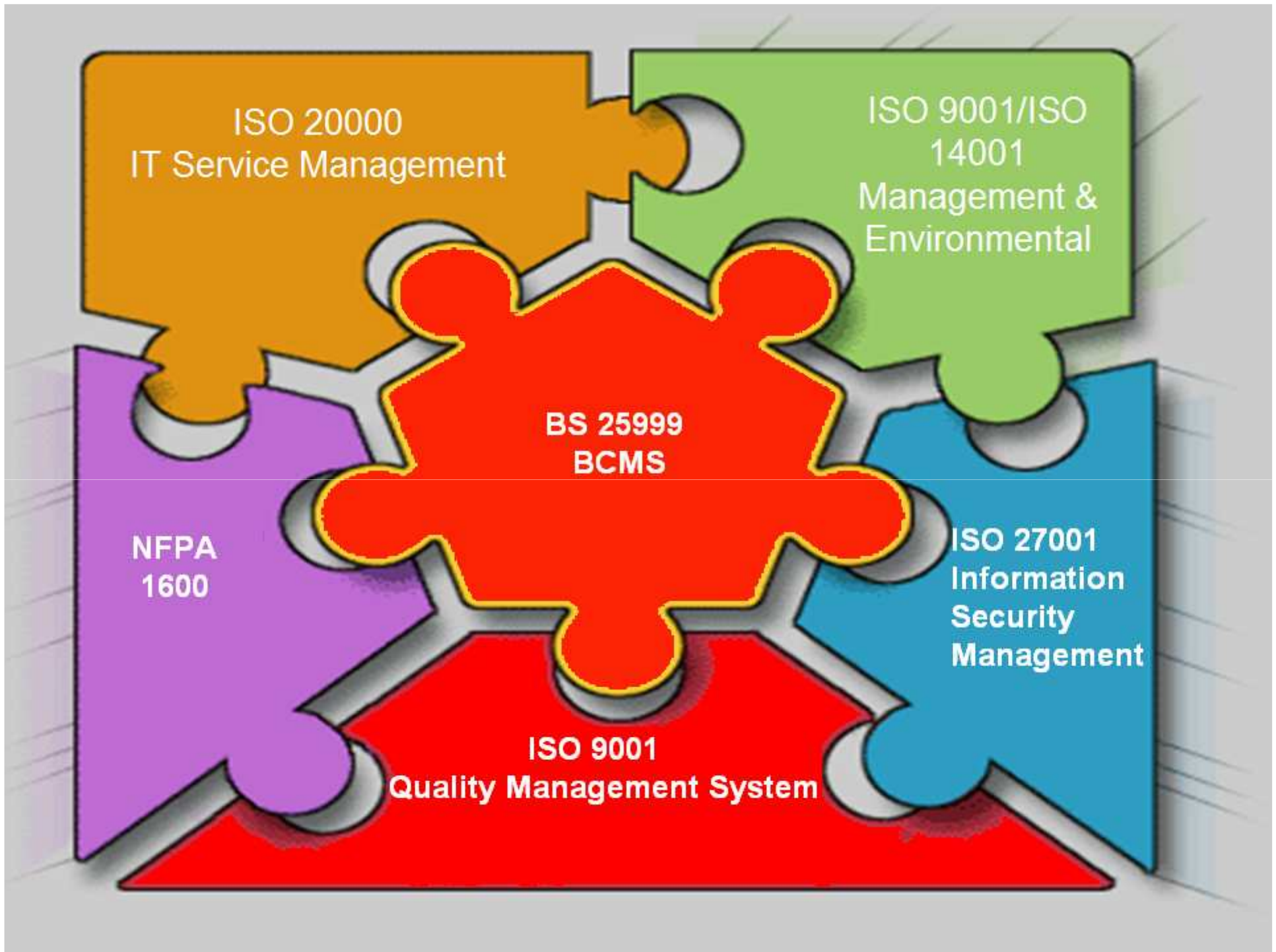


Table A.1 Correspondence of BS 25999-2 with other management systems standards

BS 25999-2:2007	BS ISO/IEC 27001:2005	BS EN ISO 9001:2000	BS EN ISO 14001: 2004
Introduction	0 Introduction 0.1 General 0.2 Process approach 0.3 Compatibility with other management systems	0 Introduction 0.1 General 0.2 Process approach 0.3 Relationship with ISO 9004 0.4 compatibility with other management systems	Introduction
1 Scope	1 Scope 1.1 General 1.2 Application	1 Scope 1.1 General 1.2 Application	1 Scope
	2 Normative references	2 Normative reference	2 Normative references
2 Terms and definitions	3 Terms and definitions	3 Terms and definitions	3 Terms and definitions
3 Planning the BCMS 3.1 General 3.2 Establishing and managing the BCMS	4 ISMS requirements 4.1 General requirements 4.2 Establishing and managing the ISMS 4.2.1 Establish the ISMS 4.2.2 Implement and operate the ISMS	4 QMS requirements 4.1 General requirements	4 EMS requirements 4.1 General requirements
4 Implementing and operating the BCMS 4.1 Understanding the organization 4.2 Determining business continuity strategy 4.3 Developing and implementing a BCM response 4.4 Exercising, maintaining and reviewing BCM	4.2.3 Maintain and improve the ISMS		4.4 Implementation and operation 4.5.1 Monitoring and measurement



Fortresses

Security & Compliance Solutions

NFPA 1600

NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs is a consensus standard, which had its origin in 1991 and as such, has matured and evolved over the past seventeen years. Since it was originally published in the United States, a number of international versions were issued.

NFPA 1600 advocates that organizations take an “all hazards approach” to prepare for any incident, including human, natural or technological events. NFPA 1600 also advocates a team-based approach to response, restoration and recovery preparation with strong senior management support and involvement.

ASIS

“BSI and ASIS are collaborating on an American Business Continuity Standard.”

“The standard will be based on the recently published British Standard, BS 25999 standard (Part 1 - Code of Practice; Part 2 - Specification), eliminating confusion in the marketplace by providing a unified approach to BCM on both sides of the Atlantic.

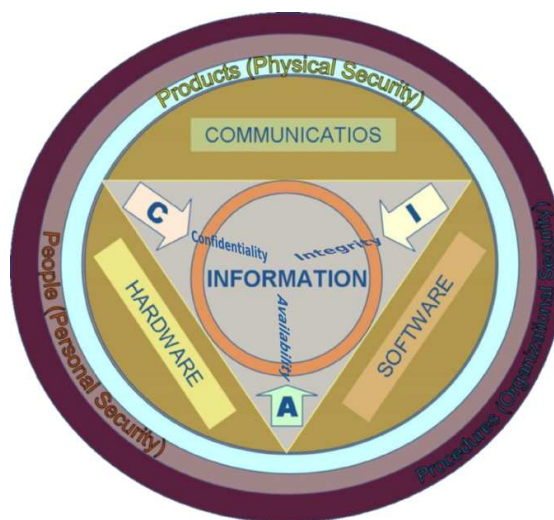
The new American National Standard will provide a clear roadmap for developing, implementing and improving the effectiveness of an organization's business continuity management plan. It will provide criteria that can be objectively audited by third parties, thereby assuring company Stakeholders

There will be reciprocation between the two standards, allowing companies to start building their BCM programs immediately, without having to wait for the new American National Standard.”

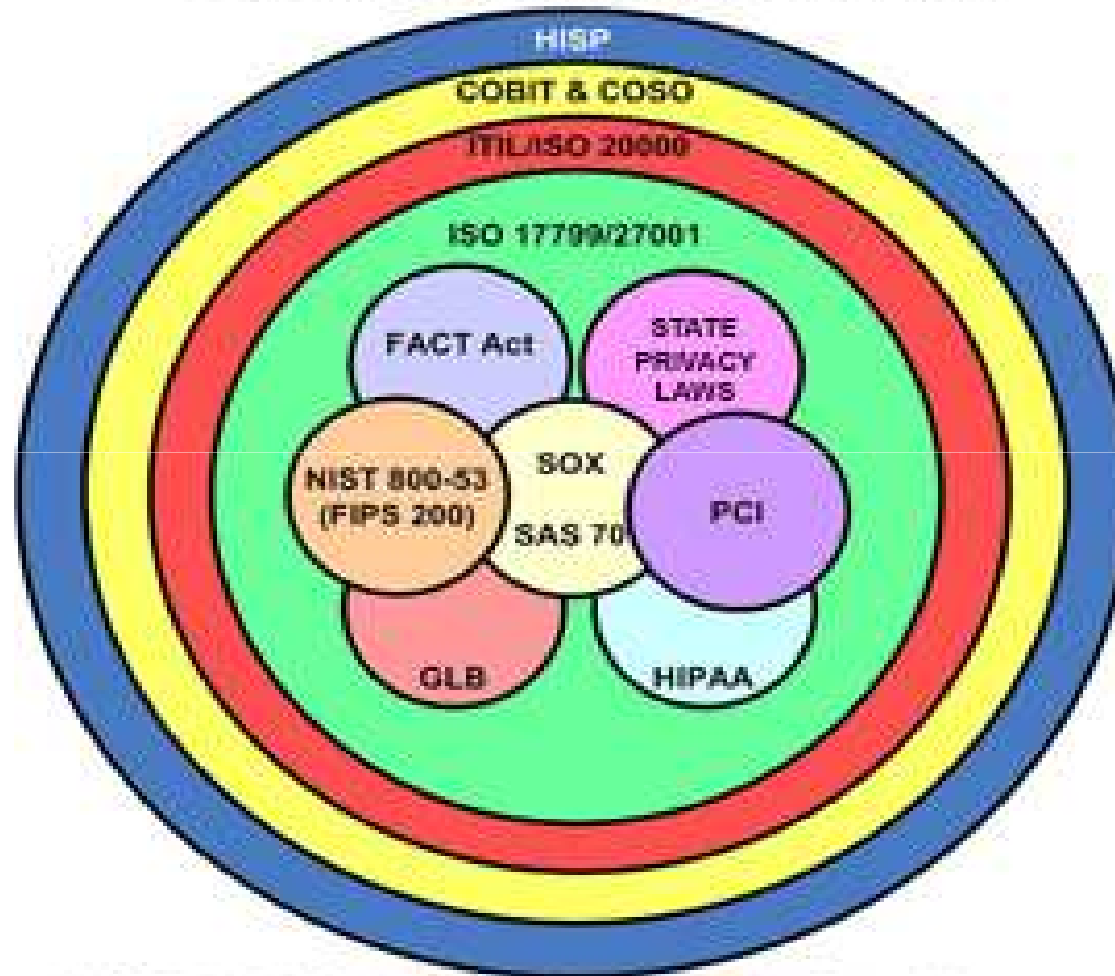
Information Security Management System



Visa CISP
ITIL SAS 70 Sarbanes Oxley
NIST GLBA ISO 20000
CobIT HIPAA



HOLISTIC APPROACH



HISP: Holistic Information Security Practitioner



eFortresses

Security & Compliance Solutions

Why the “Holistic” approach?

Are you building your plane in the sky??

IP

BC

Data Analysis

SOX

GLBA

HIPAA

COBIT

Personal Security

Basel II

NIST Harmonization

NASD

NYSE

Physical Security

Access Control

OECD Guidelines

Risk Management

System Planning

PCI

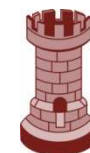
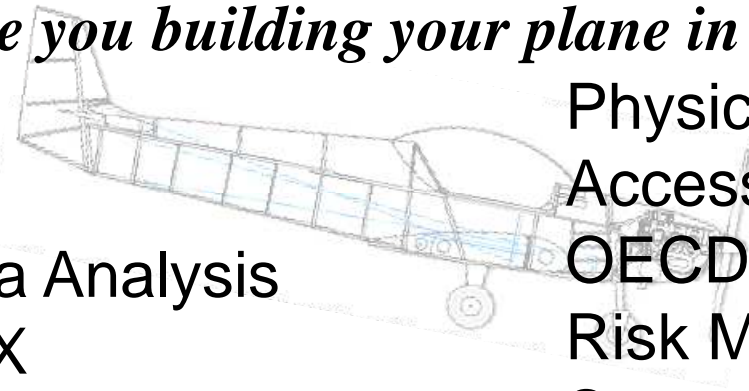
PIPEDA

BITS Shared

Assessments

BS 25999

FFIEC



eFortresses

Security & Compliance Solutions



So what are you waiting for??
You need a plan!!!



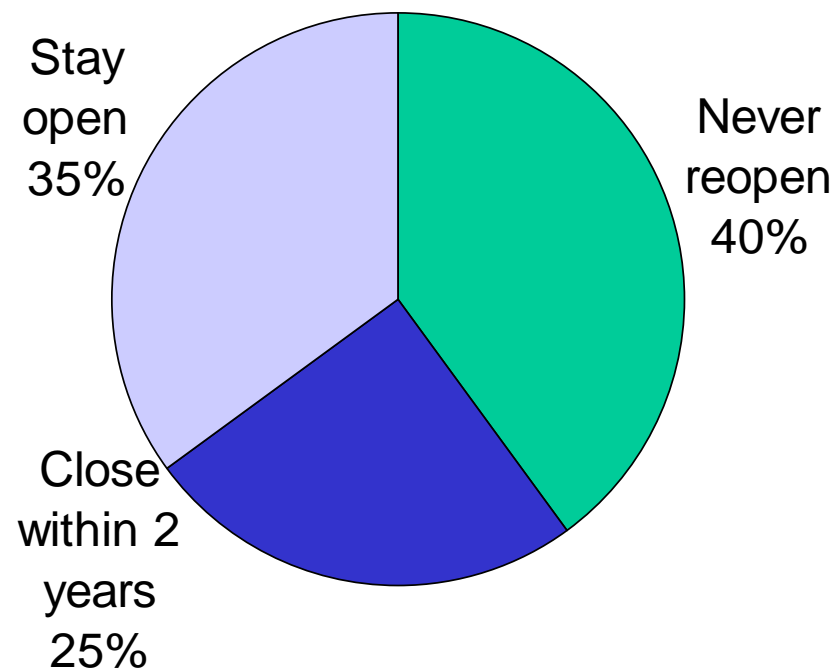
eFortresses

Security & Compliance Solutions

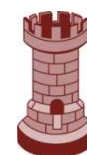
Why you need a formalized integrated process

- Cost of downtime
 - deferred or permanently lost revenue
 - employee productivity losses
 - fees
 - penalties
 - loss of discounts etc.
 - Impact to corporate reputation
- Long-term viability

Business Viability Following A Disaster



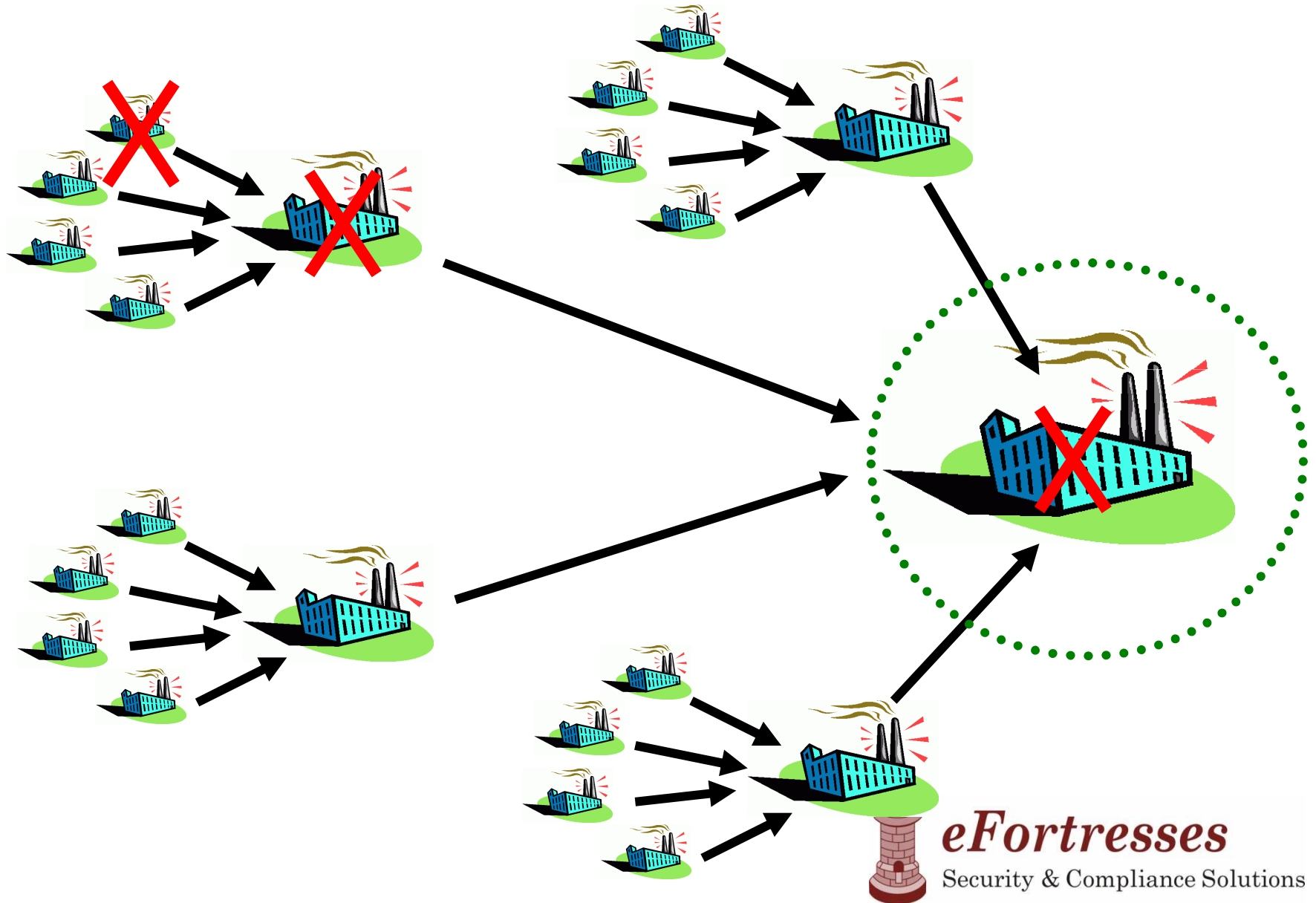
Source: The U.S. Department of Labor



eFortresses

Security & Compliance Solutions

Increasing organizational and supply chain complexity



Reacting to Failures



Prevention Systems



eFortresses

Security & Compliance Solutions

You may have to testify to the authenticity and integrity of the system



Certification VS Compliance



eFortresses

Security & Compliance Solutions

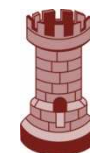
What is Compliance?

- Compliance is an informal industry term generally accepted to mean the system provides support for some or all of a given standard.
- Vendors of compliant systems are generally expected to offer documentation describing which parts of the standard are supported, and which are not.

What is certification?

- Certification on the other hand is a recognition of formal testing, to prove that a system provides 100% support for a given standard.
- Certification is awarded to an organization after an official accredited Certification Body (CB) has reviewed not only the results of formal testing, but formal conformance documentation as well as assessing their management system against the requirements of a standard and the organizations own internal requirements ***proving effectiveness.***
- This – hopefully - results in the issuing of a certificate of registration to show that the organization abides by the principles set out in the standard.
- Offers global consistency in implementation.
- Continual improvement - achieved through regular assessments of the management system.
- Supply Chain Management.

~Accountability~



eFortresses

Security & Compliance Solutions

Assessment & Stages

Pre-assessment (optional)
Documentation Assessment
(Stage I)
Certification Assessment
(Stage II)

Pre-certification

Adherence to ISO 17021

Conformity assessment requirements for bodies providing audit and certification of management systems

Continuing Assessment
Triennial Re-assessment

Post-certification



eFortresses

Security & Compliance Solutions

Conclusion

Certification, can easily show that the system has been audited and tested to the standard involved by evidence of accredited of third party approval.

But it is up to you!

Factors to consider

Mandates

Marketing

Business Plan/Value

Budget



eFortresses

Security & Compliance Solutions

Do Something!!

- You do need a formal risk based framework in place
- Don't start from scratch; evaluate and use standards to provide best practices for establishing the framework
- You can use any of the standards as the basis for your framework
- Start simple and keep it simple; establish a program that address the likeliest of risks with the most impact. You can improve over time.

Do Something!!

- If you already have a framework in place, it's worthwhile to compare your current program and practices to one or more of the standards and understand what the differences are. Use the standards to drive continuous improvement and effectiveness.
- Be aware of industry-specific standards regulations and guidelines in your industry and country.
- Involve more than the core team in your program. Involve all stakeholders and have a good cross-functional team. Make sure they get the awareness and training they need to be effective.

Questions?



eFortresses

Security & Compliance Solutions

John DiMaria; Six Sigma BB, HISP
Director of Professional Services
Cell: 678-923-3555 Office: 404-238-0588
E-mail: jdimaria@efortresses.com
solutions@efortresses.com

www.efortresses.com