THE INTERNATIONAL TAKAFUL SUMMIT 2014

GISBA

Establishing IT Governance for Takaful Organizations using Triple ISO Standards & TOGAF Framework

By: Javed A. Abbasi

GISBA

MBA Bi Major (MIS & Finance) PMP, MBCP (DRII, USA), BCMI(Singapore), ISO 27001 Lead Auditor (EP), CISA, CISM, CISSP ISO/IEC 27001 ISMS Practitioner & Auditor, IT Project Plus, ITIL, CIPA, IBM-CSE, IBM-SP, DIBI (IBII, UK), IFQ (SII, UK), CIPA-(AAIOFI), CCSA, CCSE, Six Sigma Black Belt

Javed@GISBA.NET

Agenda

- What is IT Governance?
- What are the three components?
- Why it is Important to use ISO standards?
- Integrating the Requirements of the Standards
- Discussion on Standards
  - ISO 27001:2013 for Information Security
  - ISO 20000 for Service Management
  - ISO 22301 for Business Continuity
  - TOGAF Framework
- Conclusion

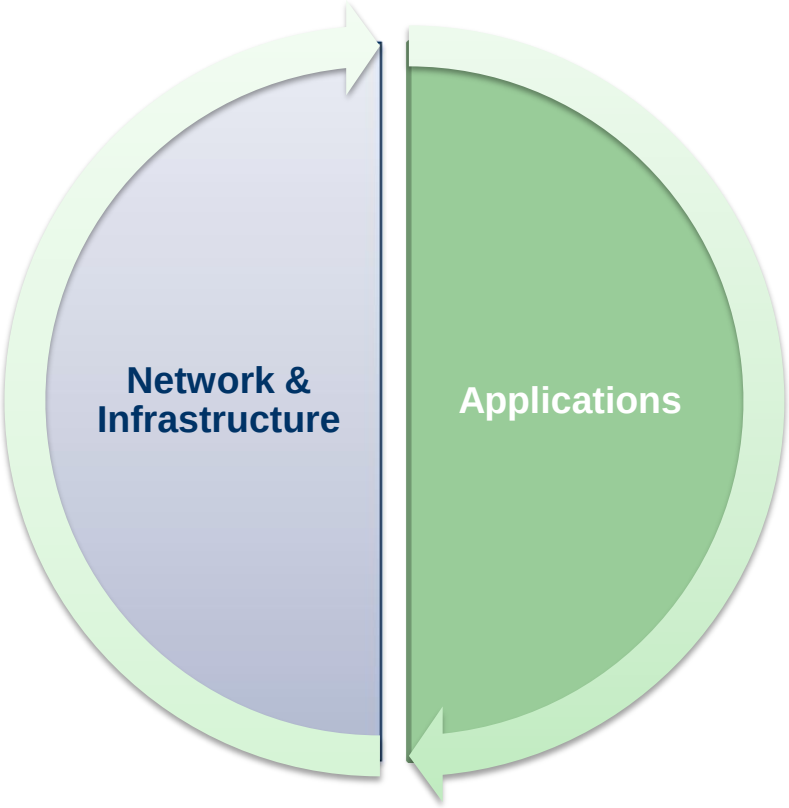
Why IT Governance?

- Takaful Organizations audited by the external auditors, regulators and others
  - Auditor and others are using different model to evaluate
  - They are always coming up with something based on certain best practice
- Better Rating by Rating Agency
- More confidence of the Stakeholders

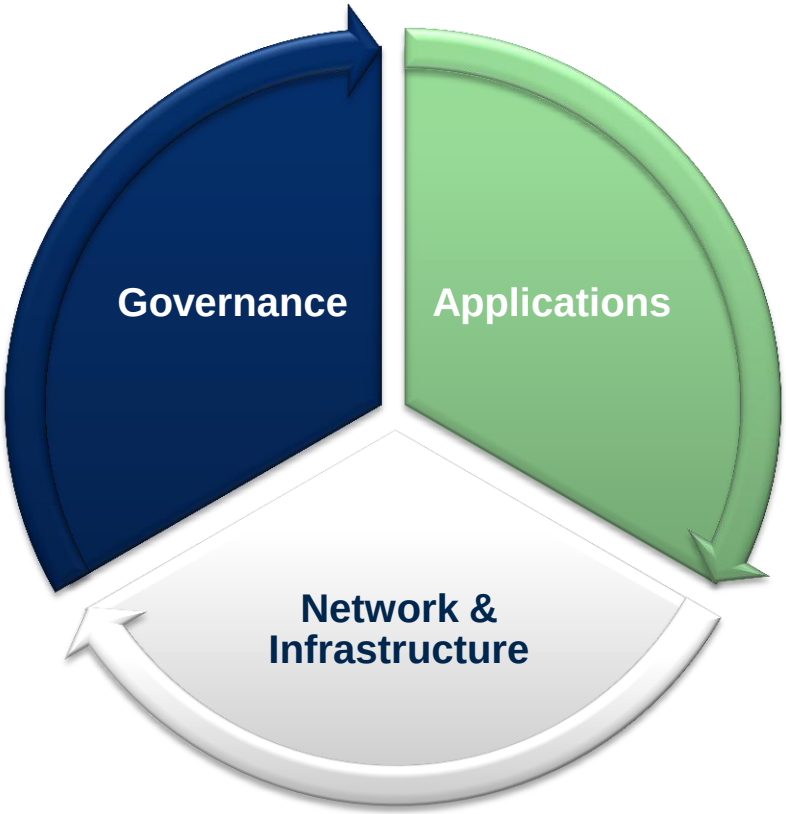
Three Important Components of IT

Three Important Components of IT

Three Important Components of IT

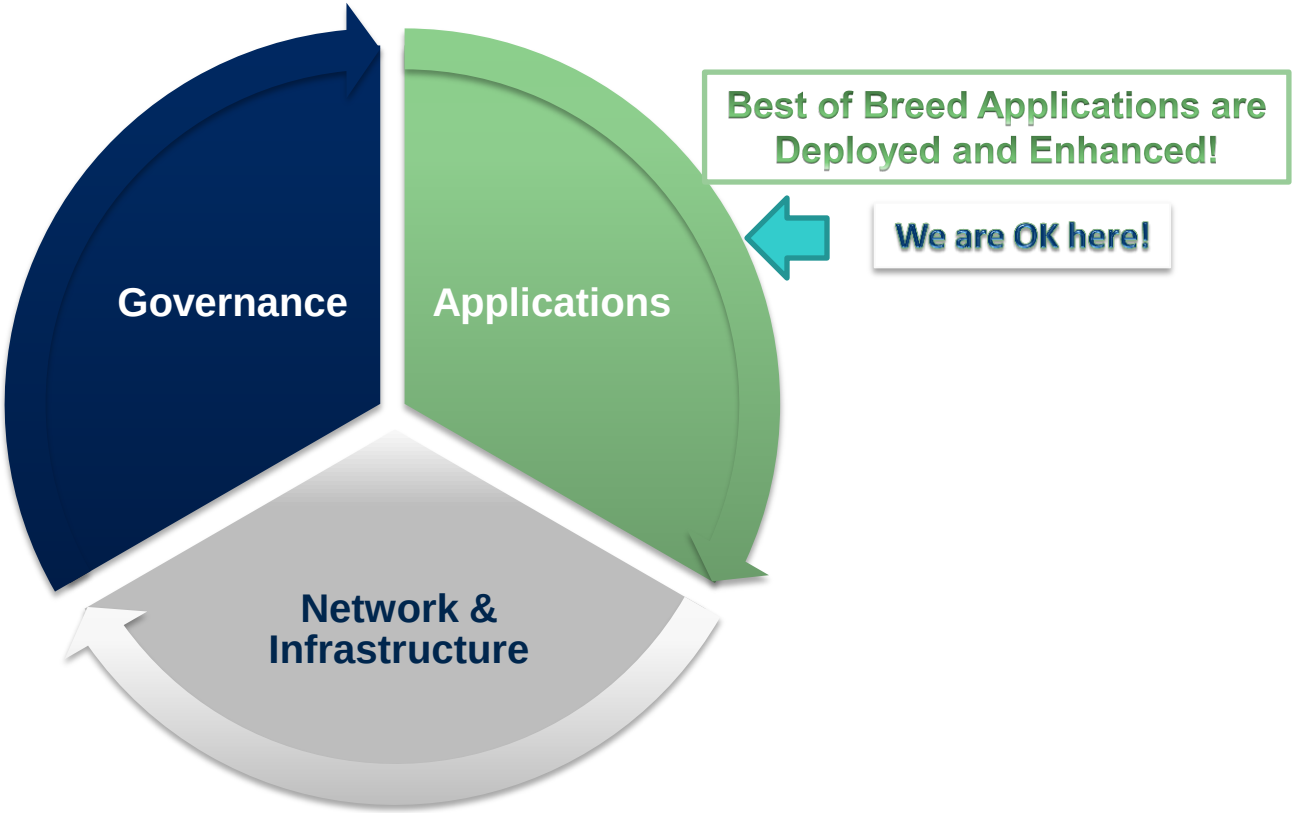


Three Important Components of IT

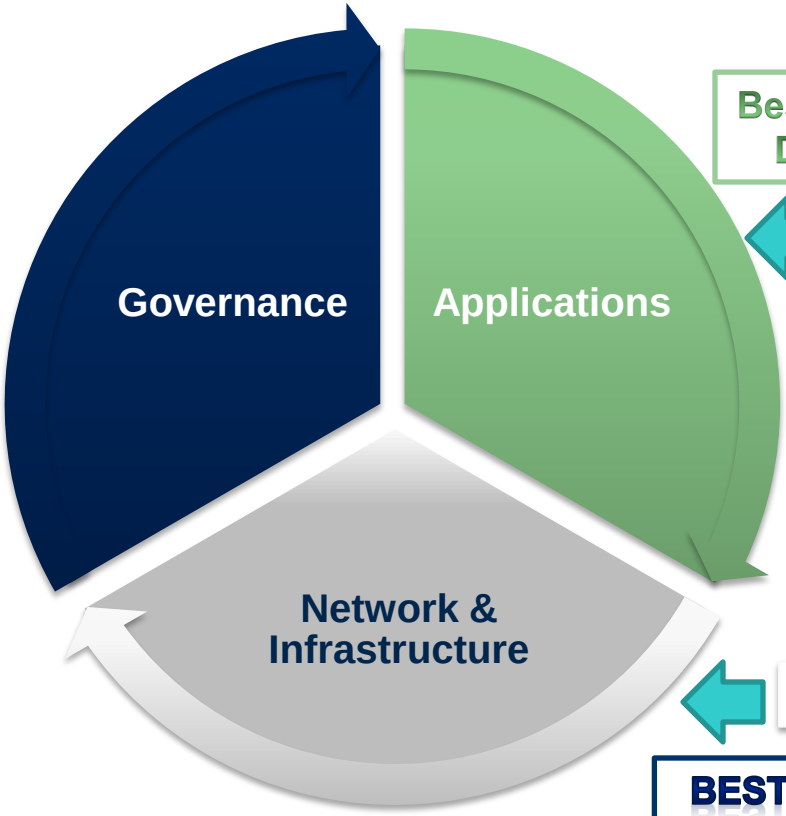


The Status of Three IT Components!

Realty Check!



Reality Check!



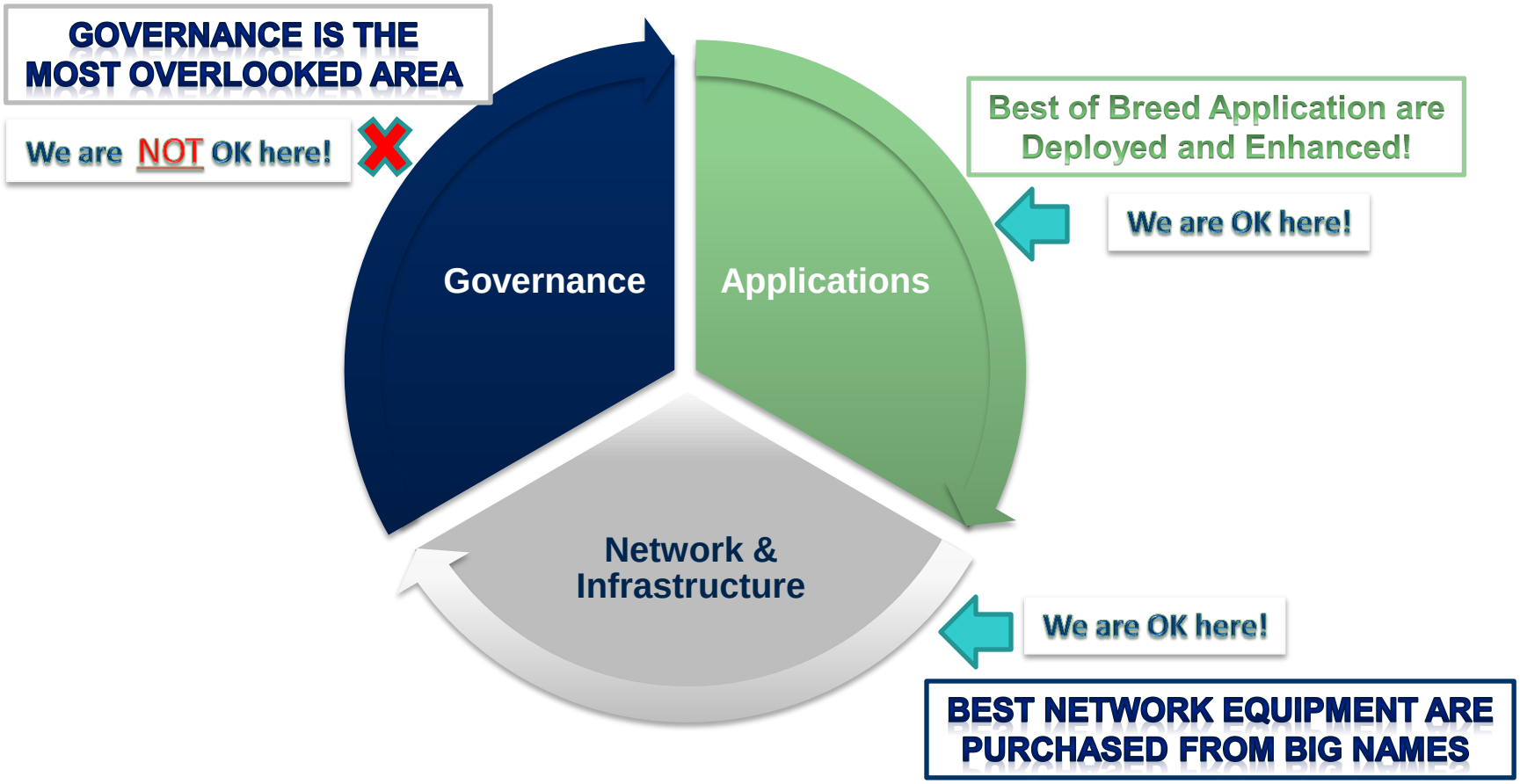
Best of Breed Application are Deployed and Enhanced!

We are OK here!

We are OK here!

BEST NETWORK EQUIPMENT ARE PURCHASED FROM BIG NAMES

The Problem Identified!



Your Achievements are Like Majestic Ship

A Torpedo of Mis-Governance!

Sinks the Ship of Majestic Achievements

People Always Complains that…

WHEN I DO SOMETHING GOOD
NO ONE REMEMBERS
BUT
WHEN I DO ANYTHING BAD
NO ONE FORGETS!

What is the Solution?

Good News!

International Standards

The Light House!

Standards
Good News & Bad News!

Standards: Good and Bad News

- Good News:
  - There is no shortage of standards
- Bad News
  - The challenge is to select and combine the right ones to generate value and avoid red tapes.
  - There is no standard which covers all areas
  - Many Standard overlap each other
  - Some standard are just the guidelines not meant to be detailed approach to IT Management

Standards: A Never Ending list!

Which one to select?

Standards: A Never Ending List

- 1. Tickit
- 2. ISO 20000
- 3. ISO 27001
- 4. CMMi
- 5. People CMMi
- 6. CGTF ISG
- 7. PMOK
- 8. Prince2
- 9. FEAF
- 10. Zachman
- 11. Corba
- 12. XML
- 13. Soap
- 14. CobiT
- 15. ITIL
- 16. SAS 70
- 17. AS 8015
- 18.etom
- 19. MOF
- 20. ISO 9000
- 21. EFQM
- 22. Lean
- 23. ISO 14000
- 24. TQM
- 25. TL 9000
- 26. King
- 27. ACC
- 28. Bakridge
- 29. Six Sigma
- 30 Coso/CoCo
- 31 Basel-II & Basel III

The list is not exhaustive…

Standards: A Never Ending List

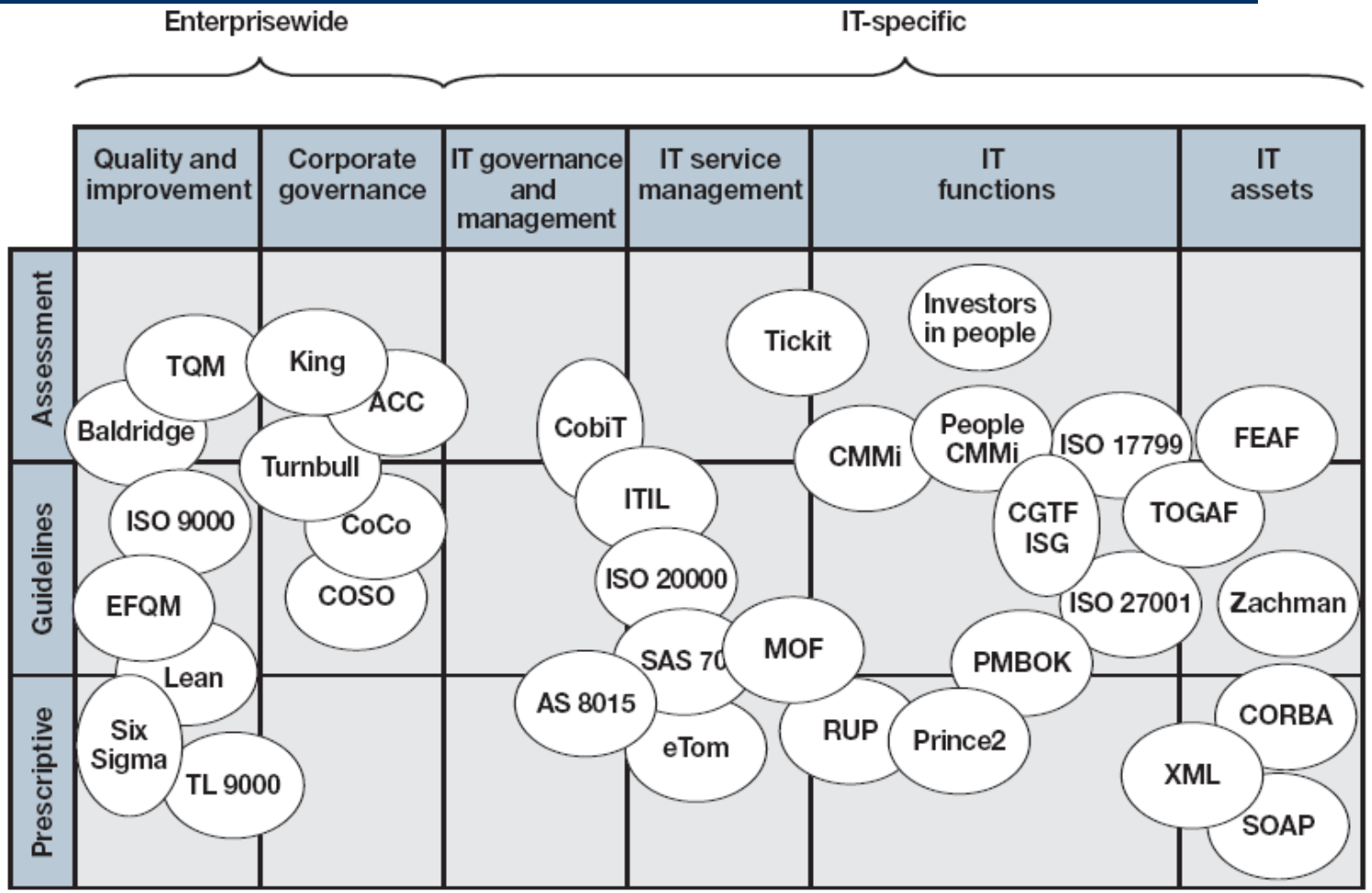
- Which Standard to choose?
- We know, 30+ standards can't be followed in any organization.
- Need to "Cherry-Pick"
- Criteria need to defined as which standards to select
  - You need to **'Select'** a set of 'Standards', not to **'choose'**
- Out of 30+ you might Select three, but which three?

Which is the Right Standard?

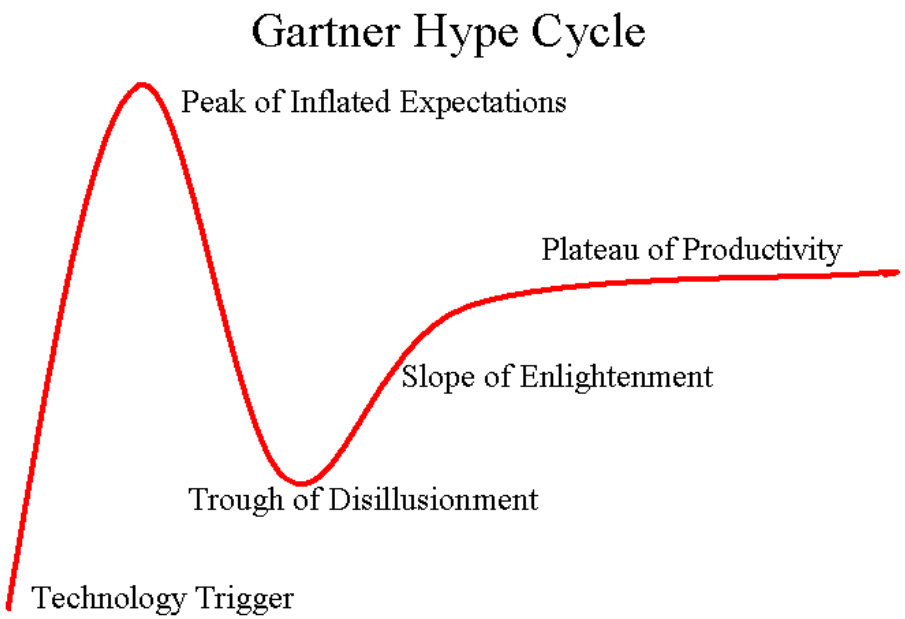
- From the list of never ending standards, how to select right one, might be a daunting task
- There are different approaches for selecting standards.
  - Some people may have their own preference
  - Most of the time the preference is based on the one of the following:
    - Organizational Policy
    - Expertise in one of the standard
    - Availability of Trained Resources/Training
    - Special Requirements
- The recommended approach is to with 4-Question Approach
- Four Key Questions:
  - It will make your journey faster and more reliable, while navigating in the jungle of standards…

Cross-Mapping the Standards against the Requirements

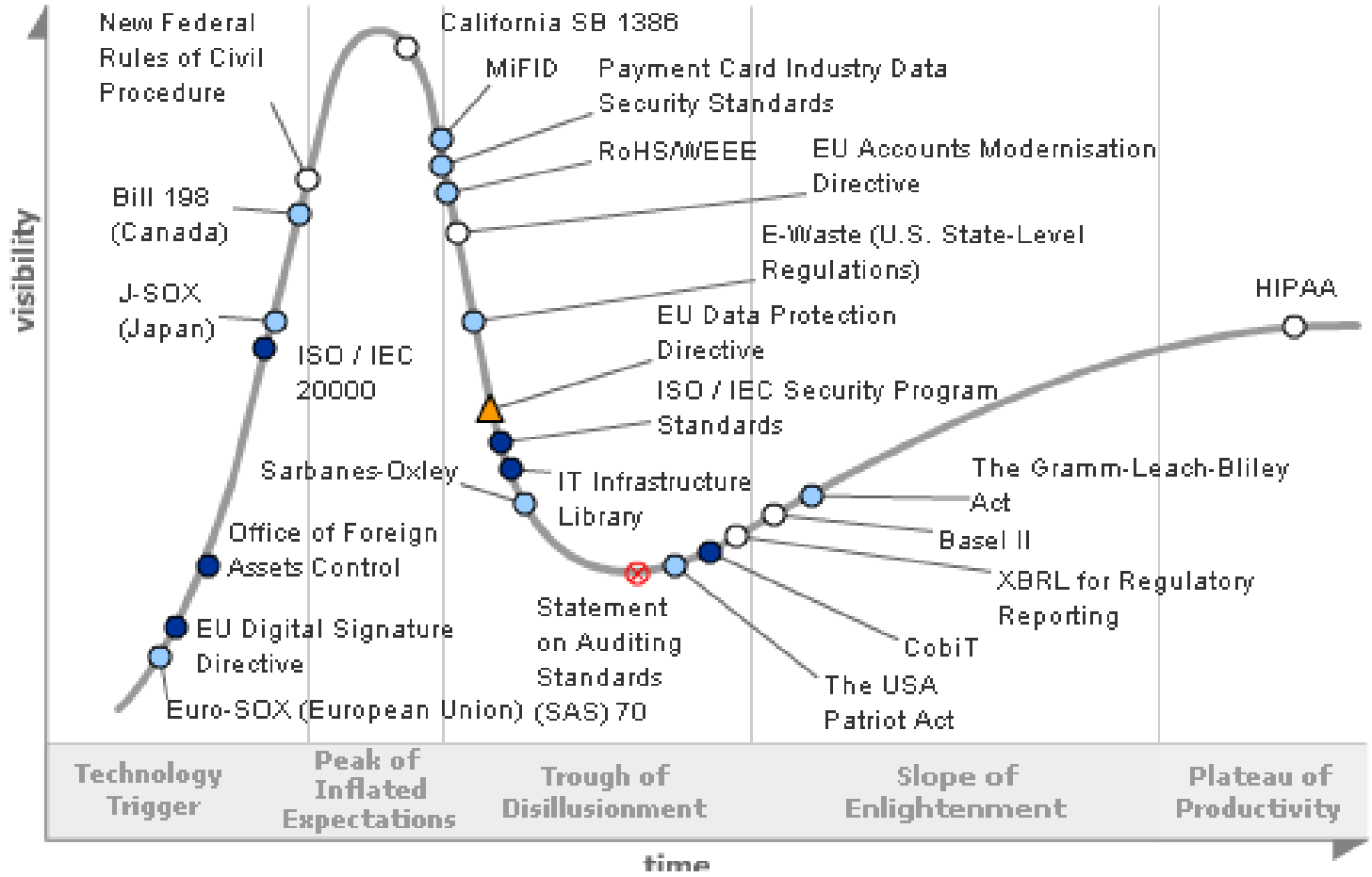
Gartner Cross-Mapping…



Managing the Expectations



Gartner's View

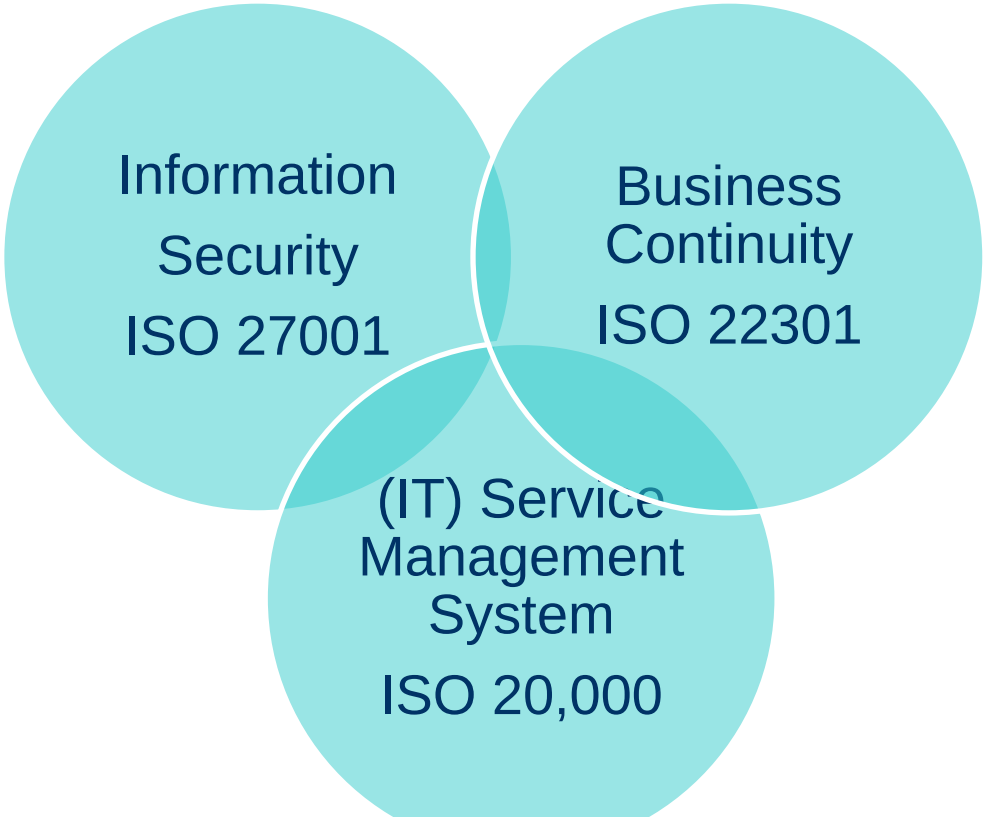


What is the Solution?

The Solution

Comprehensive Governance Coverage

TOGAF Framework +



What is TOGAF?

What is TOGAF?

- **The Open Group Architecture Framework** (**TOGAF**) is a framework for enterprise architecture
- TOGAF is a high level and holistic approach to design, which is typically modeled at four levels:
  - Business,
  - Application,
  - Data,
  - Technology.
- Give a well-tested overall blueprint
- It relies heavily on modularization, standardization, and already existing, proven technologies and products.

IT Service Management
ISO 20,000

ISO 20,000

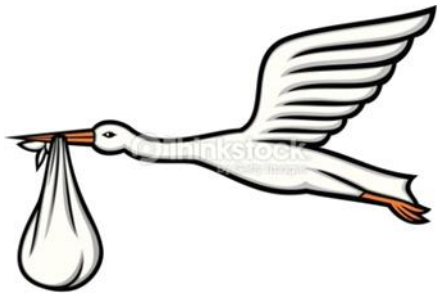
- **ISO/IEC 20000 (20K)** is the first international standard for IT Service Management.
  - **IT Service Management** (**ITSM**) is a discipline for managing information technology (IT) systems,
  - Centered on the *customer's perspective of IT's contribution to the business.*
  - ITSM stands in contrast to technology-centered approaches to IT management and business interaction. The following represents a characteristic statement from the ITSM literature:
    - *Providers of IT services can no longer afford to focus on technology and their internal organization, they now have to consider the quality of the services they provide and* ***focus on the relationship with customers.***[1]
  - ITSM is process-focused and relay on common Frameworks like ITIL

Information Security Management System
ISO 27,001

Why ISO 27001 & Information Security Management System?

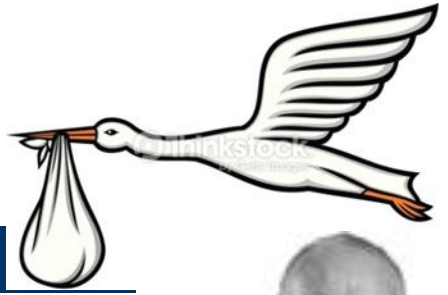
- The critical information of the organization is secure
- The information of the customers are protected
- Company sensitive information is under ISMS (Information Security Management Systems)
- Users are aware of their roles and responsibilities regarding information security
- Proper governance is in place for the information security of IT and non-IT assets
- Security is being monitored, new threats are being traced and immediate corrective action is taken
- Stake holders have more confidence.

ISO 27001: Information Security Standards



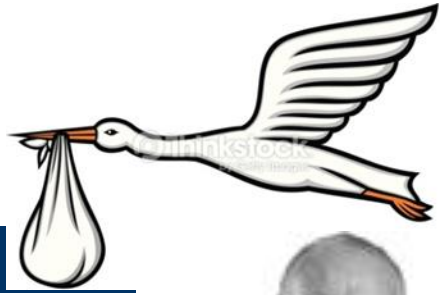
What's New

ISO 27001:2013



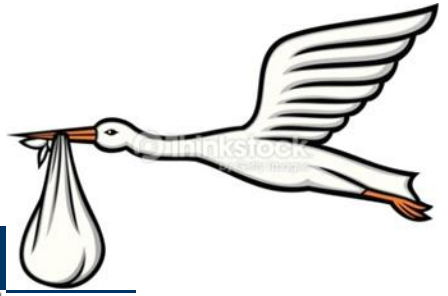
- No Deming's Plan-Do-Check-Act in this version
- Concept of Documents & Records merged as Documented Information
- Objectives for information security need to be defined, measureable and account for requirements, and risks and results communicated, updated and documented.

ISO 27001:2013



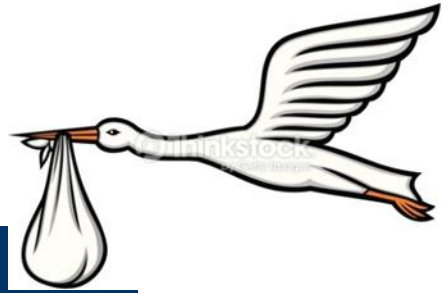
- Risk Assessment
  - Risk assessment using an asset's value, vulnerabilities and threats has been removed in the new standard.
  - Risks are now associated with the confidentiality, integrity and availability of information, and risks are assessed using the level of risk based on their consequences and the likelihood they will materialize. Risk ownership is also required.
  - Concept of Risk Owner is added.

ISO 27001:2013



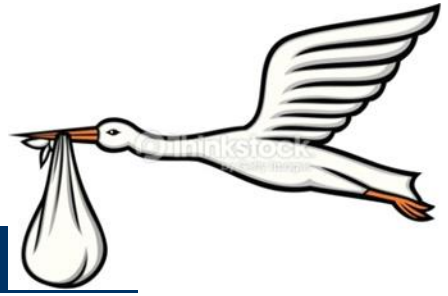
ISO Ref	Section Description	New ISO 2013		Old ISO 2005	
		Section Ref 2013	Controls Count	Section Ref 2005	Controls Count
1	Security Policies	5	2	5	2
2	Organization of Information Security	6	7	6	11
3	Human Resource Security	7	6	8	5
4	Asset Management	8	10	7	9
5	Access Control	9	14	11	25
6	Cryptography	10	2	N/A	N/A
7	Physical and Environment Security	11	15	9	13
8	Operations Security	12	14	10	32
9	Communication Security	13	7	N/A	N/A
10	System Acquisition, Development and Maintenance	14	13	12	16
11	Supplier Relationships	15	5	N/A	N/A
12	Information Security Incident Management	16	7	13	5
13	Information Security Aspects of Business Continuity	17	4	14	5
14	Compliance	18	8	15	10
	Total		**114**		**133**

New Controls



- **14.2.1: Secure development policy** – Standards for the development of software and systems shall be established.
- **14.2.5: System development procedures** – Principles for developing secure systems shall established, documented, maintained and applied to any information system.
- **14.2.6: Secure development environment** Organizations shall establish and appropriately protect secure development environments for system development and integration.

New Controls



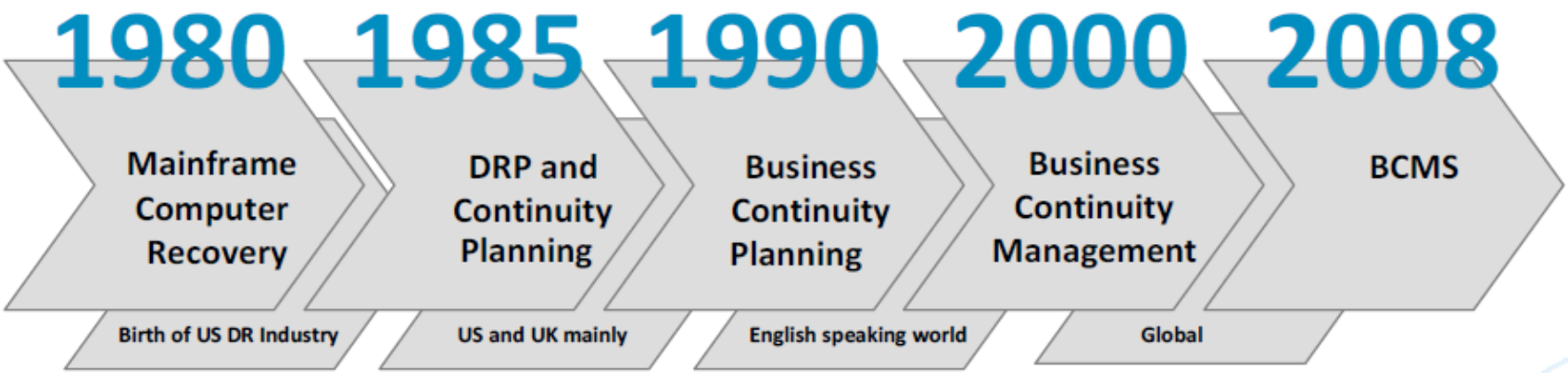
- **14.2.8: System security testing** – Testing of security functionality shall be carried out during development.
- **16.1.4: Assessment and classification of information security events** – Information security events shall be assessed, and it shall be decided if they are to be classified as information security incidents.
- **17.2.1: Availability of information processing facilities** – Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

Business Continuity Management System & ISO 22301

The Evolution

BCI View: Till the Birth of BCMS

BCM History and Background



BCMS = Business Continuity Management System

What is Business Continuity?

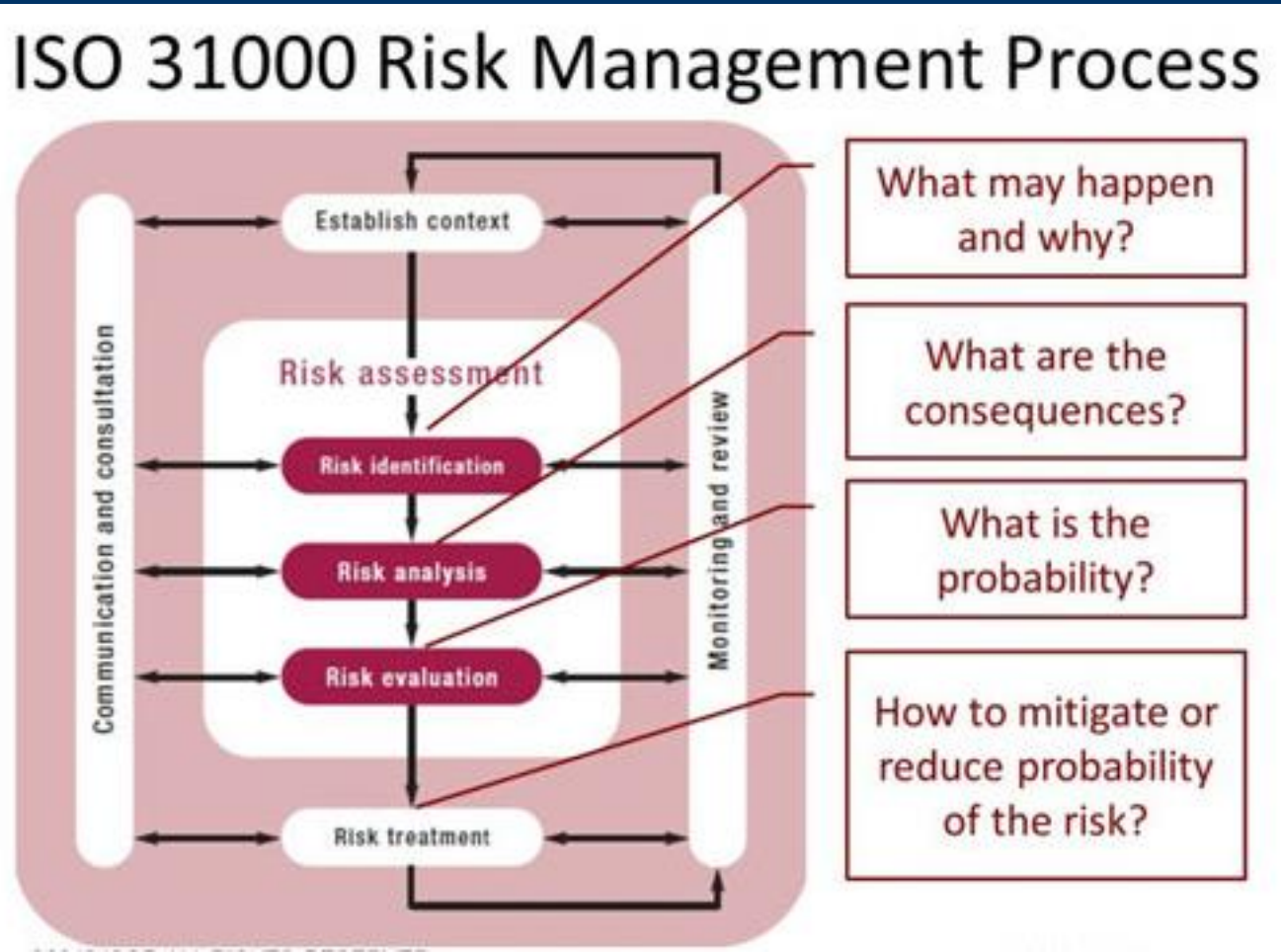
- “Business continuity management is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response which safeguards the interests of its key stakeholders, reputation, brand and value creating activities”

ISO 22301 for BCMS

ISO22301

ISO22301 Business Continuity Programme Elements

ISO 22301 and ISO 31000



Integrated Management System

TAKAFUL-IN-A-BOX

+ Can be Integrated with Industry Tutorial Solution like **Takaful-in-a-Box**
+ **Takaful-in-a-Box** is Browser Based tutorial solution with Open Interface

Take Away…

- Don’t wait for Disaster to Happen to implement Governance
- Be Proactive
- Look for Integrated Approach
  - Integrate at least three standards and focus on
    - ISO 27001 for Information Security
    - ISO 20000 for IT Service Management
    - ISO 22301 for Business Continuity Management System
  - TOFAG Framework
- Help your organization to get better rating and confidence by customers, regulators and other stakeholders.

If you are interested for more detailed information, please give me your Business Card.
Or drop me email on:
Javed_Abbasi@GISBA.net

Q&A

The End!

There is end to a race and journey,
But
There is no end to learning, you only move to the next level!