

Chap 14 Tool for Auditing :
CobiT, ITIL and ISO17799
How to use them in conjunction

Dr. Ir. Yeffry Handoko Putra M.T, CISA
Magister Sistem Informasi
Universitas Komputer Indonesia

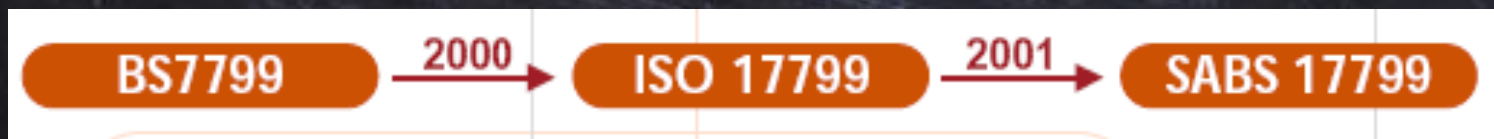
Overview

- Overview ISO 17799
- Overview CobiT
- Overview ITIL
- How to use them in conjunction
- Conclusion

Overview ISO 17799

BS 7799

- Provides guidelines and recommendations for security management.
- Part 1 - Standard; and
- Part 2 - Certification.

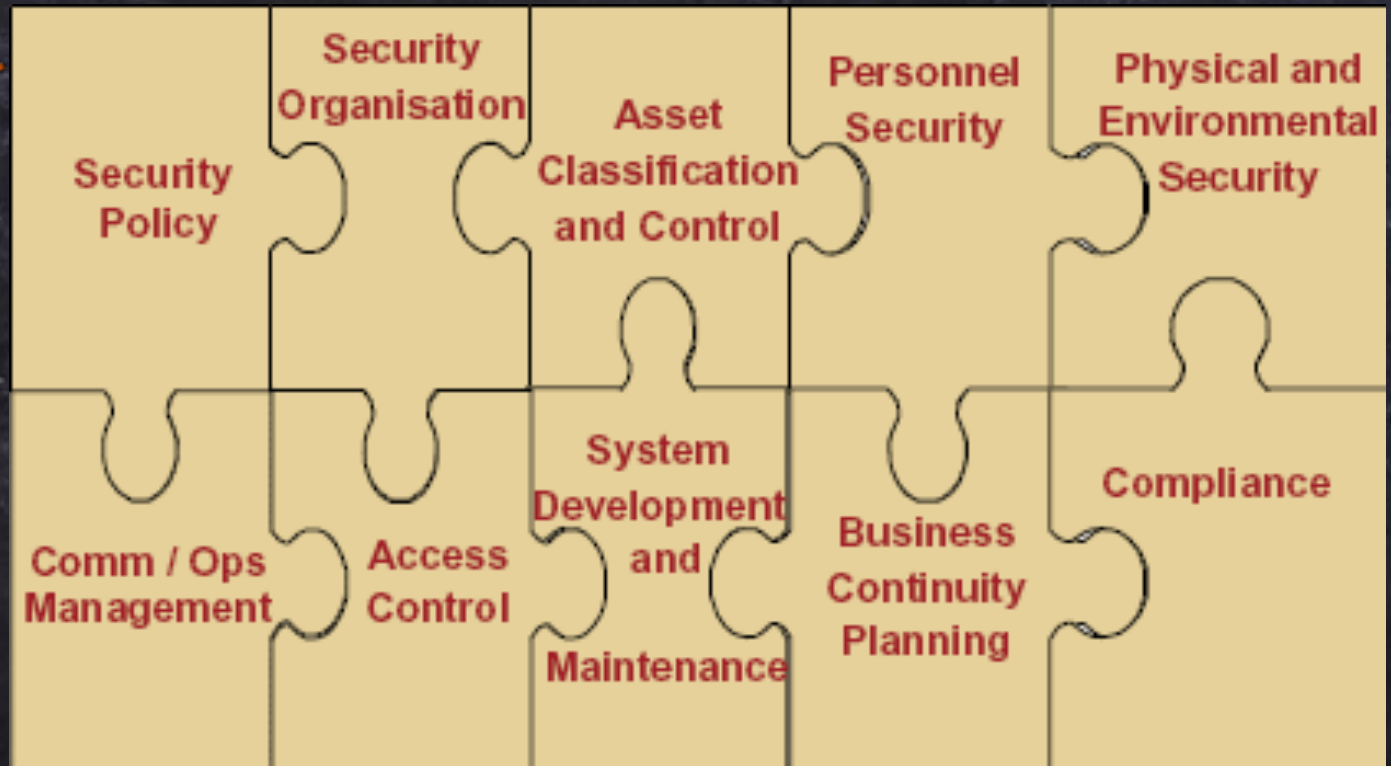


ISO 17799

- Part 1 accepted as International Standard;
- Part 2 to be accepted end of 2002.

ISO 17799 Modules

Organisational Risks



ISO 17799 Controls



Security Policy

Documented & communicate IS policy
Regularly reviewed



Security Organisation


Allocation of roles & responsibilities
3rd-party access risks / controls
Outsourcing



Asset Classification and Control


Inventory of Assets
Classification based on sensitivity/business impact

ISO 17799 Controls

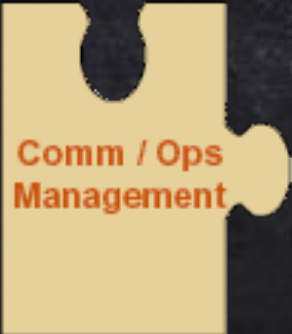


Personnel Security

- Recruitment screening
- Awareness & training
- Reporting of incidents
- Physical security perimeters
- Equipment siting
- Clear desk & clear screen



Physical and Environmental Security



Comm / Ops Management

- Incident procedures
- Segregation of duties
- System planning & acceptance
- Malicious software protection
- E-mail controls

ISO 17799 Controls



Managing Access

- Application Level
- Operating Level
- Network Level

Change control procedures

Segregation of environments

Security requirements



Business continuity plans

BCP framework and team roles & responsibilities

Testing continuity plans

Maintaining and updating continuity plans

ISO 17799 Controls



Copyright controls

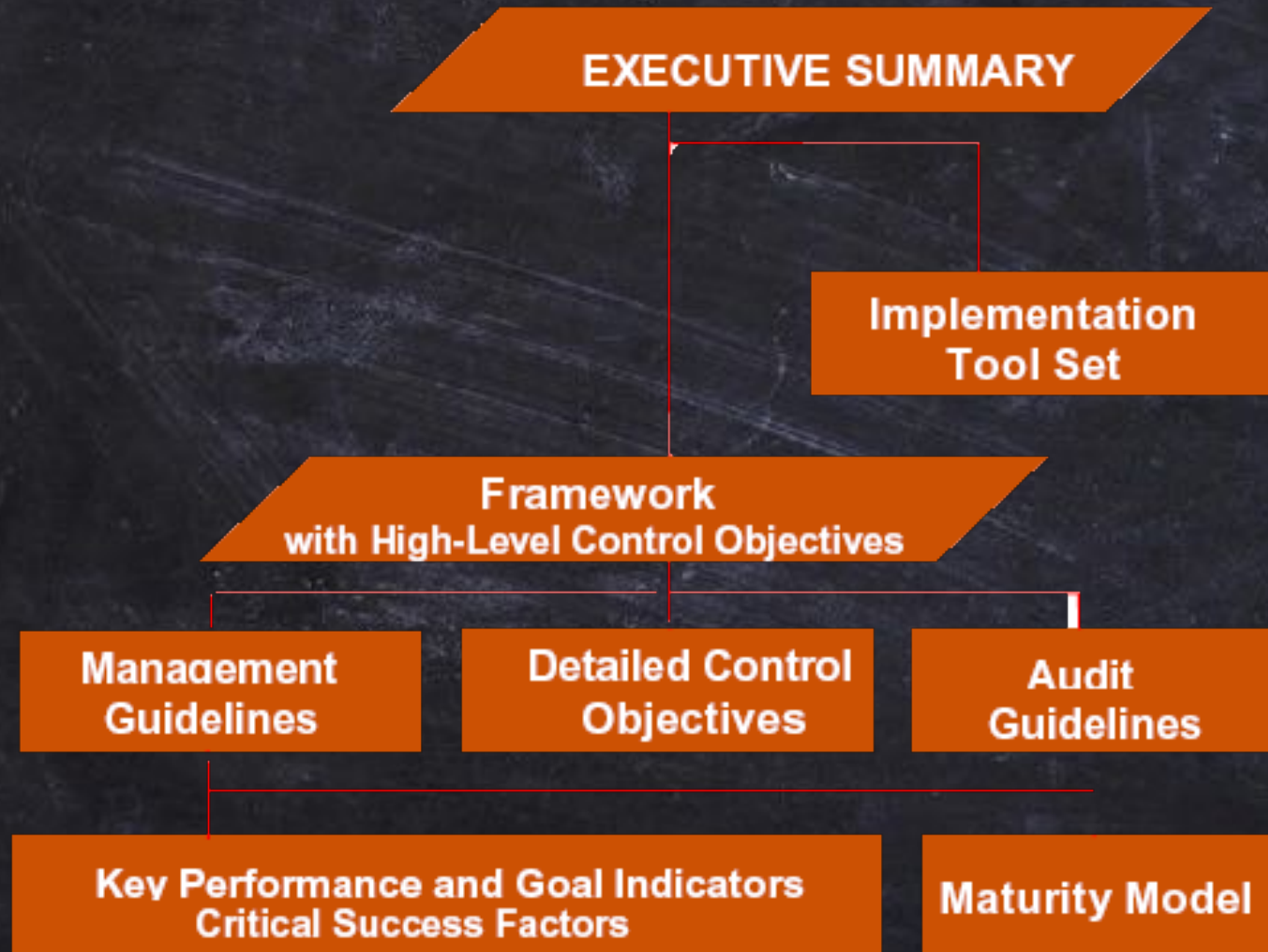
Retention of records and information

Compliance with legislation - Data protection

Compliance with company policy

Overview CobiT

CobiT Product Family



CoBiT Principles



CobiT

Domains



Processes



Acquisition & Implementation

- AI 1: Identify automated solutions
- AI 2: Acquire and maintain application software
- AI 3: Acquire and maintain technology infrastructure
- AI 4: Develop and maintain procedures
- AI 5: Install and accredit systems
- AI 6: Manage Changes

- AI 6: Manage Changes: Control objectives**
- 6.1: Change request initiation and control
 - 6.2: Impact assessment
 - 6.3: Control of changes
 - 6.4: Emergency changes
 - 6.5: Documentation and procedures
 - 6.6: Authorised maintenance
 - 6.7: Software release policy
 - 6.8: Distribution of software

Per process:

- Control objectives
- KPI's: measure of performance
- CSF's: what do you need to do
- KGI's: measure of outcome
- Maturity model

CobiT

Key Goal Indicators: Manage Change

- •Reduced number# of errors introduced into systems due to changes
- •Reduced number# of disruptions (loss of availability) caused by poorly managed change
- •Reduced impact of disruptions caused by change
- •Reduced level of resources and time required as a ratio to number# of changes
- •Number# of emergency fixes/time
- •....

Key Performance Indicators: Manage Change

- •Number# of different versions installed at the same time
- •Number# of software release/and distribution methods per platform
- •Number# of deviations from the standard configuration
- •Number# of emergency fixes for which the normal change management process was not applied retro-actively
- •Time lag between availability of fix and implementation of it. .
- •ratio of accepted vs refused change implementation requests.

Critical Success Factors: Manage Change

- •Expedient and comprehensive acceptance test procedures are applied prior to making the change.
- •There is a reliable hardware and software inventory.
- •There is segregation of duties between production and development

Overview ITIL

what service the business requires of the provider in order to provide adequate support to the business users

ensuring that the customer has access to the appropriate services to support the business functions



understanding and improving IT service provision, as an integral part of an overall business requirement for high quality IS management

Business Continuity Management

partnerships and outsourcing

surviving change

transformation of business practice through radical change.

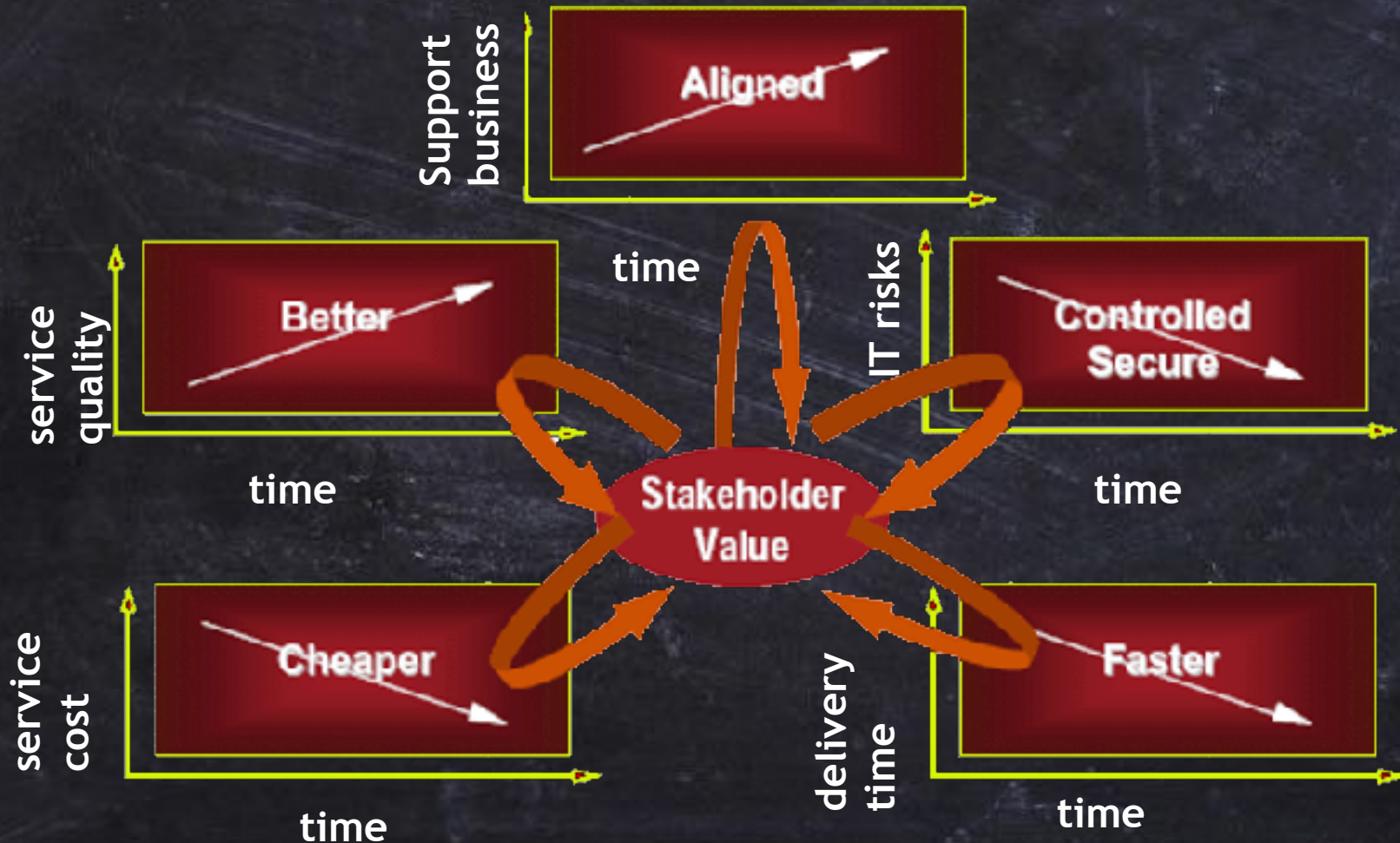
Network Service Management
Operations Management
Management of Local Processors
Computer Installation and Acceptance
Systems Management

ITIL service support & service delivery processes

- Service support:
 - Service desk
 - Incident management
 - Problem management
 - Configuration management
 - Change management
 - Release management
- Service delivery
 - capacity management
 - availability management
 - financial management of IT services
 - service level management
 - IT service continuity management

How can they be used in
conjunction?

What do we want to achieve with IT?

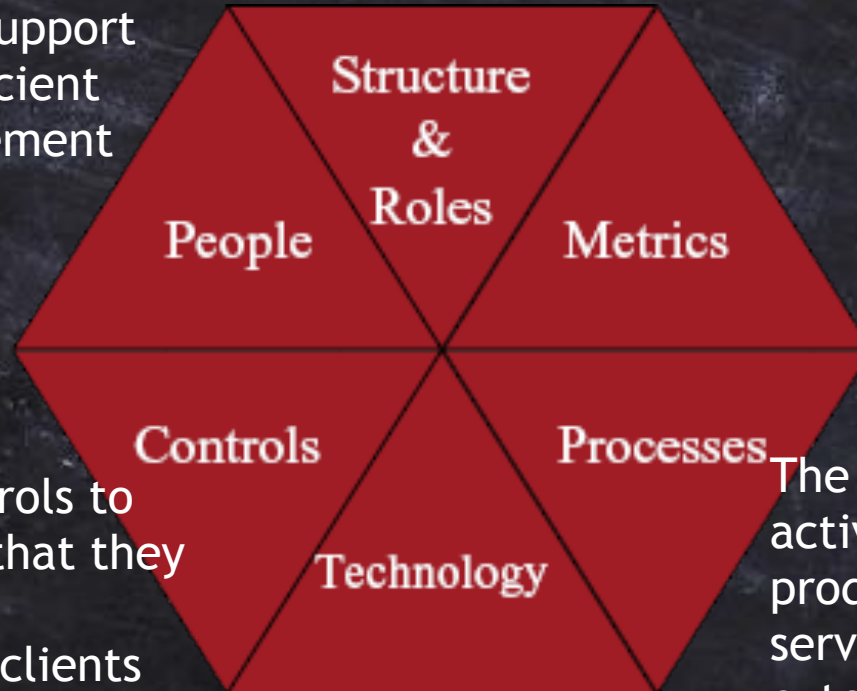


How we can achieve these IT goals

The assignment of responsibility for performing specified activities to specific groups or individuals

The people that support effective and efficient IT service management

The assignment of measurements to people processes, technology and controls to ensure they comply to what they are intended for

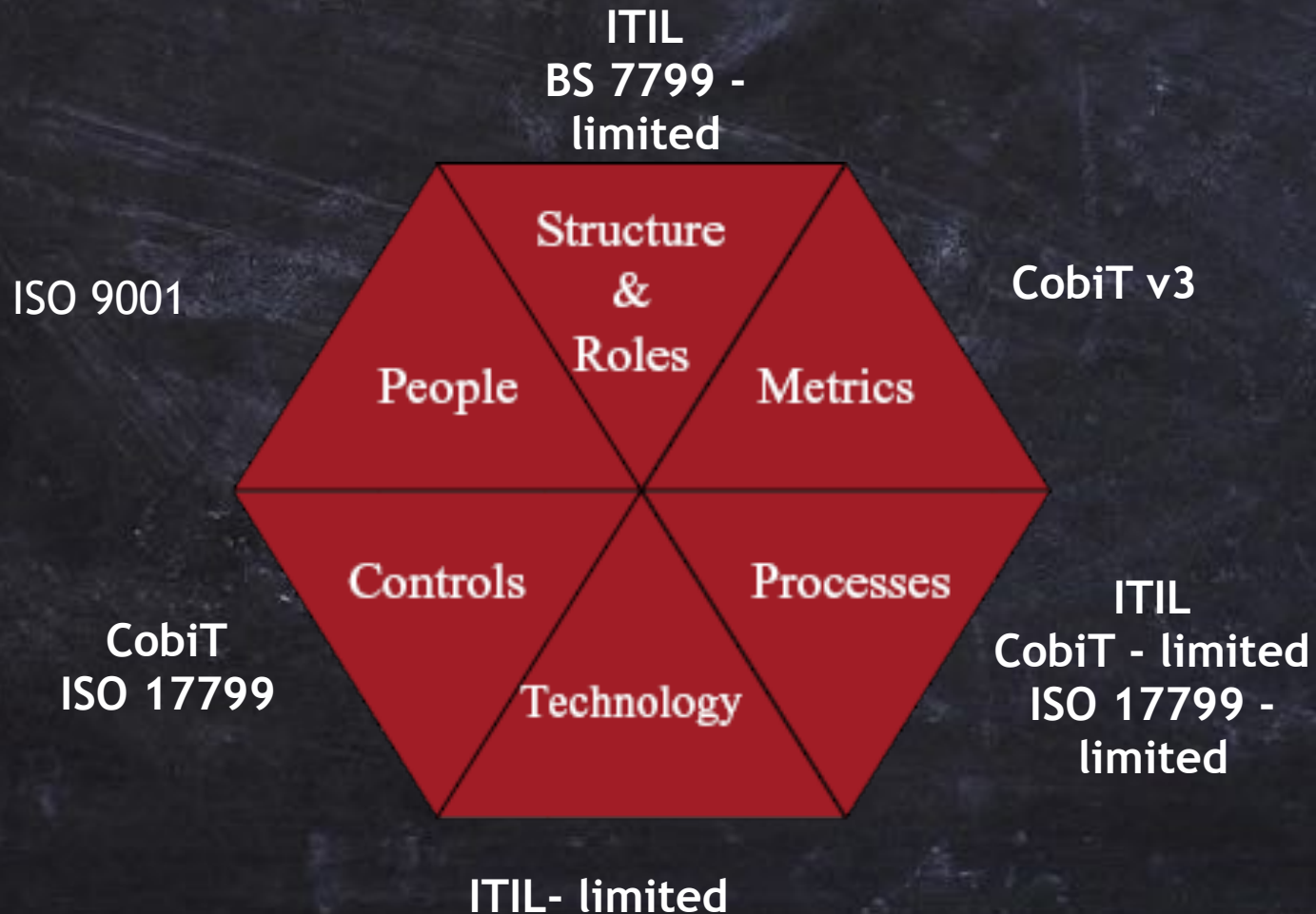


The interrelated series of activities that combine to produce products or services for internal & external clients

The technology that is supporting the IT delivery

The assignment of controls to IT processes to ensure that they deliver efficiently and effectively in line with clients requirements

How we can achieve these IT goals

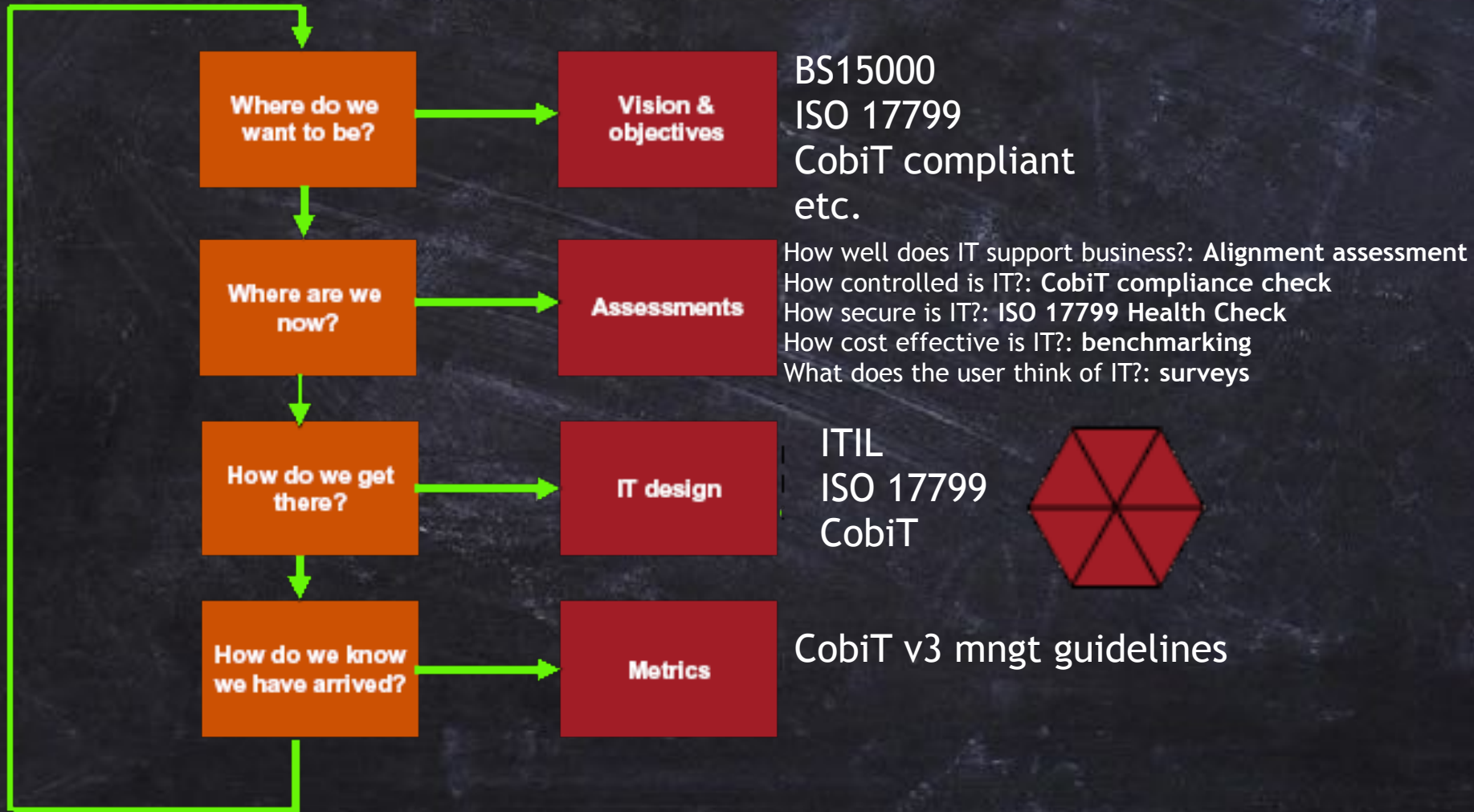


How we can achieve these IT goals:

Where are the methods strong in?

- **ITIL** strong in IT processes , but limited in security and system development
- **CobiT** strong in IT controls and IT metrics , but does not say how (i.e. process flows) and not that strong in security
- **ISO 17799** strong in security controls , but does not say how (i.e. process flows)
- Conclusion:
 - No contradictions or real overlaps
 - None identify people requirements
 - Not strong on organisational side (structure & roles)
 - – Not strong on technology side

How can we achieve these IT goals: continuous IT improvement



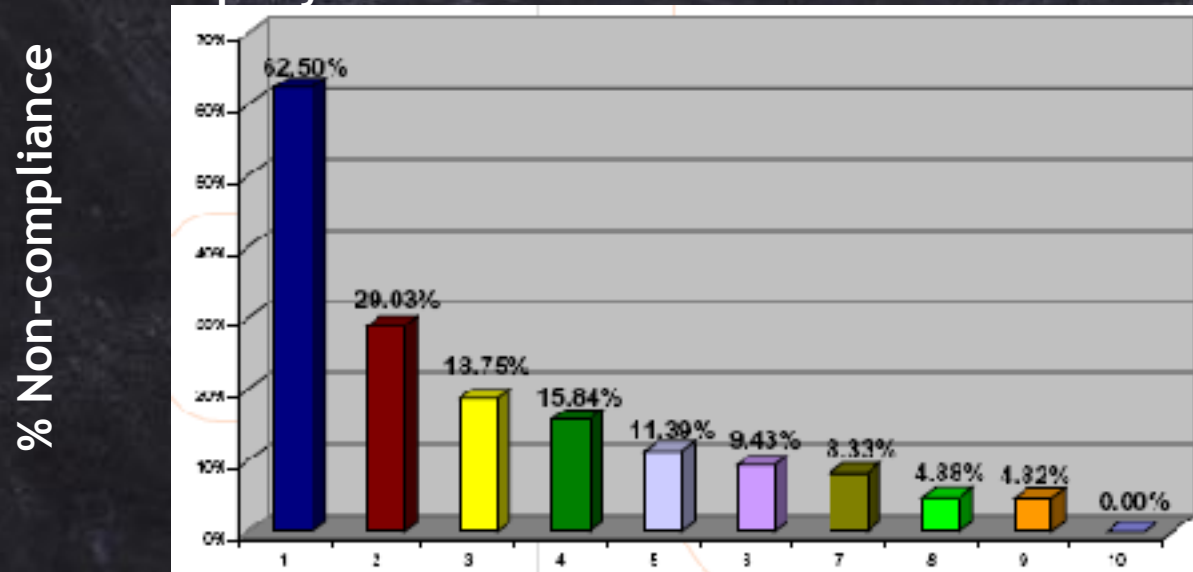
| Control Risk | | Control Evaluation | Effectiveness | Efficiency | Confidentiality | Integrity | Availability | Compliance | Reliability |
|--------------------------------|--|--------------------|---------------|------------|-----------------|-----------|--------------|------------|-------------|
| Materiality | | | 4 | 4 | 4 | 1.5 | 1.5 | 1.5 | 1.5 |
| Planning and organisation | | | | | | | | | |
| PO 1 | Define a strategic IT plan | 2 | C | H | | | | | |
| PO 2 | Define the information architecture | 1 | E | C | C | O | | | |
| PO 3 | Determine the technological direction | 2 | C | H | | | | | |
| PO 4 | Define organisation and relationships | 2 | C | H | | | | | |
| PO 5 | Manage the investment | 2 | C | C | | | | | O |
| PO 6 | Communicate management aims and direction | 1 | E | | | | | O | |
| PO 7 | Manage human resources | 1 | E | E | | | | | |
| PO 8 | Ensure compliance with external requirements | 1 | E | | | | | C | O |
| PO 9 | Assess risk | 1 | C | C | E | C | C | O | O |
| PO 10 | Manage projects | 1 | E | E | | | | | |
| PO 11 | Manage quality | 1 | E | E | | C | | | O |
| Acquisition and Implementation | | | | | | | | | |
| AI 1 | Identify automated solutions | 1 | E | C | | | | | |
| AI 2 | Acquire and maintain application software | 1 | E | E | | O | | O | O |
| AI 3 | Acquire and maintain technology architecture | 1 | E | E | | O | | | |
| AI 4 | Develop and maintain procedures | 1 | E | E | | O | | O | O |
| AI 5 | Install and accept systems | 1 | E | | | O | O | | |
| AI 6 | Managing changes | 2 | C | C | | C | C | | O |
| Delivery and support | | | | | | | | | |
| DS 1 | Define service levels | 1 | E | E | C | O | O | O | O |
| DS 2 | Manage third-party services | 1 | E | E | C | O | O | O | O |
| DS 3 | Manage performance and capacity | 1 | E | E | | | O | | |
| DS 4 | Ensure continuous service | 2 | C | H | | | C | | |
| DS 5 | Ensure systems security | 2 | | | C | C | O | O | O |
| DS 6 | Identify and allocate costs | 1 | | E | | | | | C |
| DS 7 | Educate and train users | 1 | E | C | | | | | |
| DS 8 | Assist and advise customers | 1 | E | | | | | | |
| DS 9 | Manage the configuration | 1 | E | | | | O | | O |
| DS 10 | Manage problems and incidents | 1 | E | E | | | O | | |
| DS 11 | Manage data | 2 | | | | C | | | |
| DS 12 | Manage facilities | 2 | | | | C | C | | |
| DS 13 | Manage operations | 1 | E | E | | O | O | | |
| Monitoring | | | | | | | | | |
| M 1 | Monitor the process | 1 | E | C | C | O | O | O | O |
| M 2 | Assess internal control adequacy | 1 | E | E | C | O | O | O | O |
| M 3 | Obtain independent assurance | 1 | E | E | C | O | O | O | O |
| M 4 | Provide for Independent Audit | 1 | E | E | C | O | O | O | O |
| Legend | | | E | C | H | O | C | | |
| | | | Exposure | Concern | Housekeeping | OK | concern + | | |

CobiT compliance check

How can we achieve these IT goals:
continuous IT improvement

ISO 17799 Health Check

Graph depicting the level of non-compliance of company XYZ



ISO 17799 Modules

Conclusion

- Use CobiT and ISO 17799 health check to determine current status
- Identify weaknesses in processes and controls
- Use ITIL to improve IT processes & controls, use ISO 17799 to improve
- security processes & controls (although not strong on process side)
- Use ITIL to determine technology, although not complete
- Use CobiT to define metrics
- Query ITIL on possible structures