



The ERM & IT Governance Conference

CISAC 2008
Conference of Information Security
Audit & Control

Over Protection & Under Protection

Saturday, 16 February 2008

Niraj Kapasi, FCA, CISA

*Senior Manager, Systems and Process Assurance,
PriceWaterhouseCoopers*

niraj.kapasi@in.pwc.com



Learning Objectives



- Examples
- Current Scenario
- Risk based controls
- Classification of controls
- Controls optimization methodology



Over Control?



How many times do we need to show our ticket/boarding pass

Indian Airport

US Airport

Main Gate

Boarding Hall

Check-in Counter

Security

Boarding Hall

Aircraft



Under Control?



- Key findings of the 2007 Association of Finance Professional Payments Fraud Survey include:
 - Seventy-two percent of organizations experienced attempted or actual payments fraud in 2006.
 - Thirty-nine percent of survey respondents report that incidents of fraud increased over last year.
- But
 - Most organizations suffered little or no actual financial losses resulting from payments fraud.
 - Forty-two percent of organizations that experienced at least one payments fraud attempt reported no losses as a result of the attempt(s);
 - 31 percent of organizations suffered financial losses of less than \$25,000.



Actions



- Nearly half of organizations added to their internal controls and procedures during 2006 to bolster their protection against payments fraud.

Was it required?



Under Controls



- Salary increments are approved by HR Manager in hard copy
- Salary increments are input into the system by Payroll Clerk
- No review of the increments entered into the system
- Payroll Manager reviews the comparative Payroll sheet with previous month and all differences are reviewed and disposed-off
- Payroll Manager reviews the comparative payroll with all instructions from HR Team



Over Controls



- Salary increments are approved by HR Manager in hard copy
- Salary increments are input into the system by Payroll Clerk
- All changes to Payroll in the payroll application are approved by HR Manager online
- Payroll Manager reviews the comparative Payroll sheet with previous month and all differences are reviewed and disposed-off
- Payroll Manager reviews the comparative payroll with all instructions from HR Team



Current Scenario



- SoX has made companies controls conscious
- Surveys generally highlight frauds / errors / exploits
- Controls for implementing multiple standards
- Everyone wants to 'err' on the side of caution
- Technology is fast changing
- Adoption of technology is allowing Companies to implement more controls
- Local Mgmt. Controls – Top Mgmt. Controls
- Controls by IT – Controls by Business
- Short Term thinking
- No Single team looking at controls in a holistic manner



Current Scenario



But

- Controls are not being optimally implemented
- Controls do not address RISKS
- System Auditors are not able to provide comfort on the controls for the Financial Audits
- Controls and Security are as strong as the 'Weakest Link'




Outcome



Under Protection is a 'Risk'

Over Protection is a 'Cost'

Challenge is to implement optimum controls based on cost-effectiveness of the control.



How should controls be implemented?



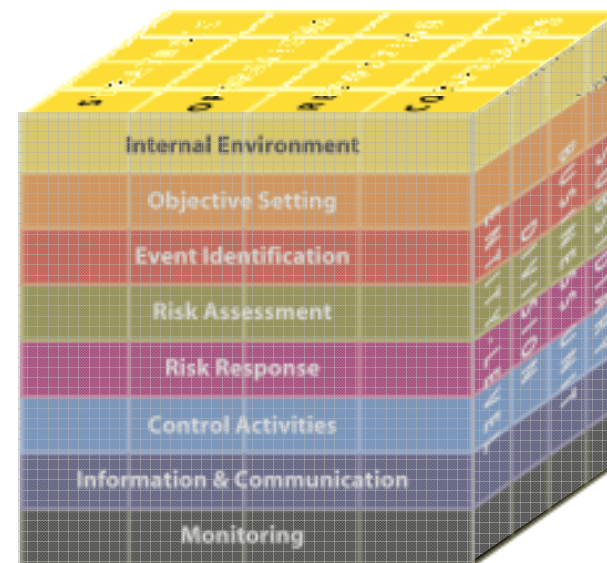
- Based on a Risk Assessment
 - Prepare a Population of Risks/threat
 - Estimate the potential loss
 - Estimate the probability of occurrence

Controls should be implemented to address risks!
Remember 'Mission Impossible' of Tom Cruise

COSO Enterprise Risk Management Framework

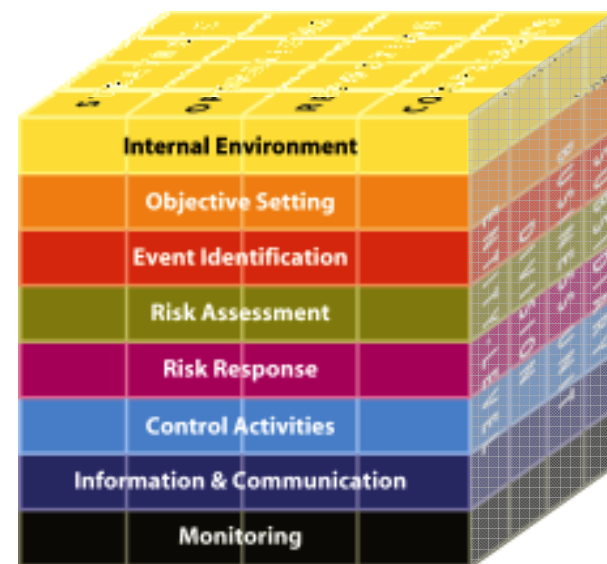


- Entity objectives can be viewed in the context of four categories:
 - Strategic
 - Operations
 - Reporting
 - Compliance



Framework overview

- Risk management components framework
 - Eight interrelated components
 - Roles & responsibilities



Framework overview



- ERM considers activities at all levels of the organization
 - Enterprise-level
 - Division or subsidiary
 - Business Unit
 - Process



Internal Environment

CISAC 2008
Conference of Information Security

The internal environment encompasses the tone of an organisation, influencing the risk consciousness of its people and is the foundation for all other components of enterprise risk management, providing discipline and structure



Internal environment factors include:

- Risk management philosophy
- Risk appetite
- Oversight by the board of directors
- The integrity, ethical values and competence of the entity's people
- The way management assigns authority and responsibility and organises and develops its people

Objective Setting



Objectives are set at the strategic level, establishing a basis for operations, reporting and compliance objectives

The establishment of objectives is a precondition to effective event identification, risk assessment and risk response

Objectives are aligned with the entity's risk appetite which drives risk tolerance levels for the entity

Event Identification

CISAC 2008
Conference of Information Security



Events with negative impact represent risks which require management's assessment and response

Events with positive impact represent opportunities which management channels back into the strategy and objective-setting processes

When identifying events, management considers a variety of internal and external factors that may give rise to risks and opportunities, in the context of the full scope of the organisation

Risk Assessment

CISAC 2008
Conference of Information Security

Risk assessment allows an entity to consider the extent to which potential events have an impact on achievement of objectives



Management assesses events from two perspectives - likelihood and impact - and normally uses a combination of qualitative and quantitative methods

The positive and negative impacts of potential events should be examined, individually or by category, across the entity

Risks are assessed on both an inherent (before risk responses) and a residual basis (after risk response)

Risk Response



Having assessed relevant risks, management determines how it will respond. Responses include:

- Risk avoidance
- Risk reduction
- Risk sharing
- Risk acceptance



In considering its response, management assesses the effect on risk likelihood and impact, as well as costs and benefits, selecting a response that brings residual risk within desired risk tolerances

Management identifies any opportunities that might be available

Take a portfolio view of risk to determine whether overall residual risk is within the entity's risk appetite

Control Activities

CISAC 2008
Conference of Information Security

Control activities are the policies and procedures that help ensure that management's risk responses are carried out



Control activities occur throughout the organisation, at all levels and in all functions

Control activities include a range of activities such as:

- Approvals
- Authorisations
- Verifications
- Reconciliations
- Reviews of operating performance
- Security of assets
- Segregation of duties

Information and Communication

CISAC 2008
Conference of Information Security

Pertinent information is identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities



Information systems use internally generated data and information about external events, providing information for managing enterprise risks and making informed decisions

Effective communication occurs, flowing down, across and up the organisation

There is also effective communication with external parties, such as customers, suppliers, regulators and shareholders

Monitoring

CISAC 2008
Conference of Information Security

The monitoring process assesses the presence and functioning of **ALL** the ERM components over time through:

- Ongoing monitoring activities
- Separate evaluations
- A combination of the two

Ongoing monitoring occurs in the normal course of management activities. The scope and frequency of separate evaluation depends on an assessment of risks and the effectiveness of ongoing monitoring procedures

Enterprise risk management deficiencies are reported upstream, with serious matters reported to senior management and the board



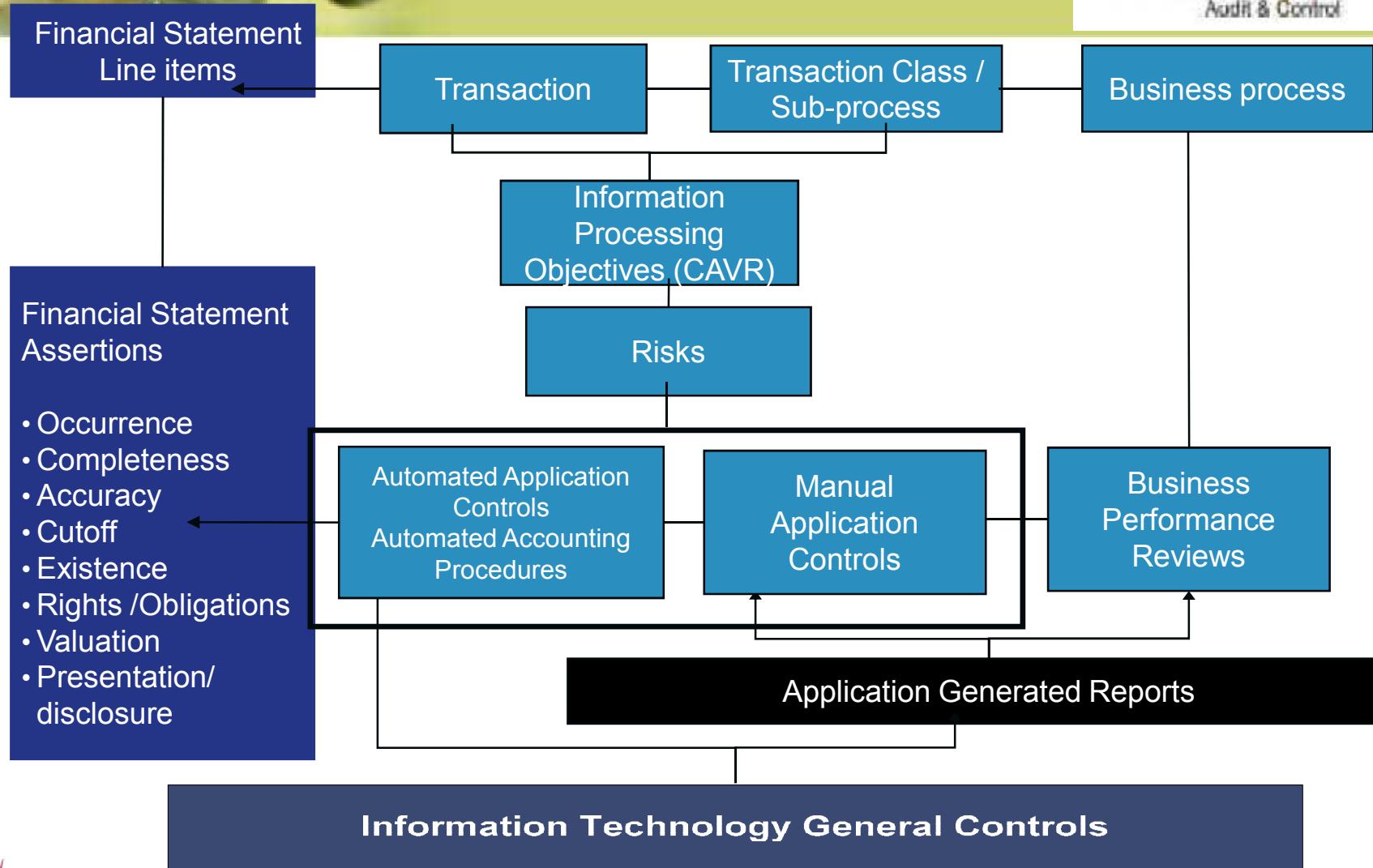
Classification of controls



- How they are applied
 - Automated
 - Manual
- Why they are applied
 - Preventive
 - Detective
 - Corrective

Classification of controls

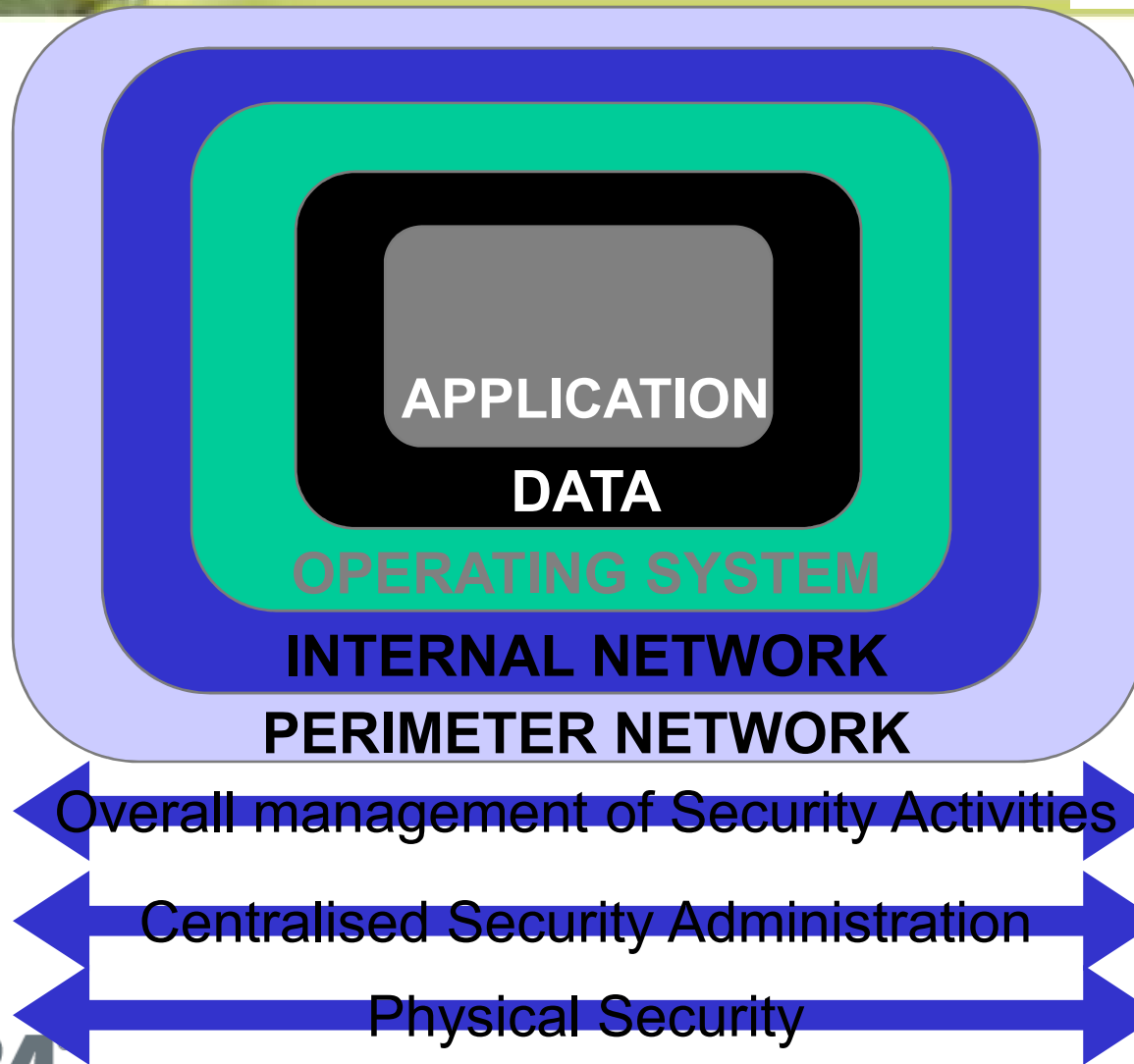
- Where they are applied
 - IT General Controls
 - Program Development and Changes
 - Security
 - Computer Operations
 - OS
 - RDBMS
 - Network/Firewall/Router
 - Application Controls
 - Manual Controls



Classification of controls

- Nature of Control
 - Authorization/Approval Controls
 - Automated Procedures
 - Configuration Controls
 - Inherent Controls
 - Segregation of duties
- Function of the Control
 - Key Control
 - Complementary Control
 - Compensating Control
 - Redundant Control

Security Components



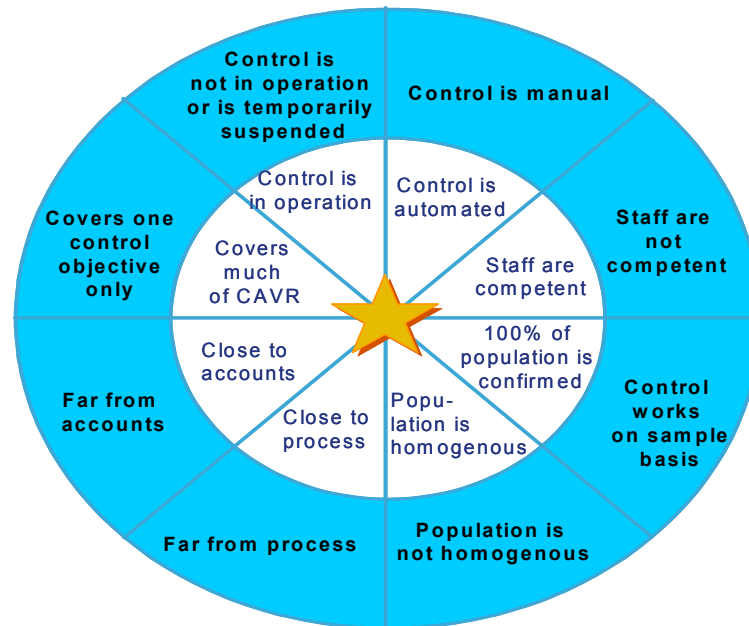
Control evaluation

When under pressure controls are the first thing to be overlooked. If a control can be suspended temporarily it is more likely to be circumvented.

Inner circle = stronger
Outer circle = weaker

If a control is manual, it will, on occasion fail – i.e. during heavy workload periods. This is an inherent risk and cannot be overlooked.

A reconciliation gives more comfort than a simple review. The more CAVR the control covers the stronger it is likely to be



For a control to work well staff need to understand the end to end process and the repercussions of not doing the control as well as being competent generally

The earlier on the control is the less impact it will likely have on the ultimate accounts. However, failure to control things early can lead to costly rework

Some exception reports are only reviewed on a sample basis, this increases the likelihood of error

The closer the control is to the process, the better it is at presenting the error. Ideally
PROCESS → CONTROL

If orders overall for say between £10 - £1000, of there is a failing of the controls an error or average £500 will occur. If the population varies widely – e.g. orders of 1p to £1m the impact of the controls failure will be greater as we cannot estimate the impact



Way forward



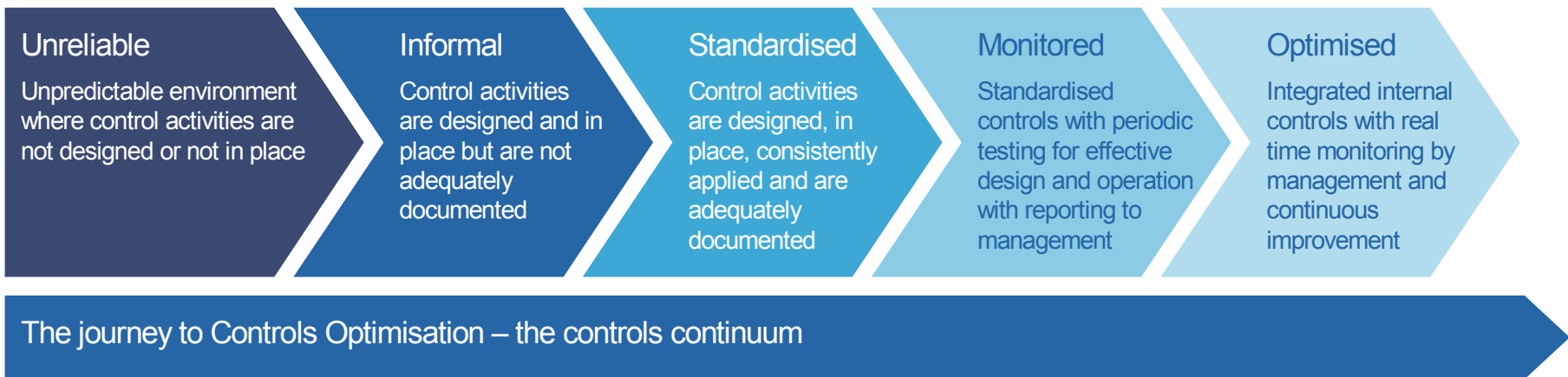
Controls Optimisation is:

A continuous process of improvement, reflecting a company's objectives and risks and the risk appetite of management by establishing effective and efficient internal controls at the right cost for the organization

Controls Continuum

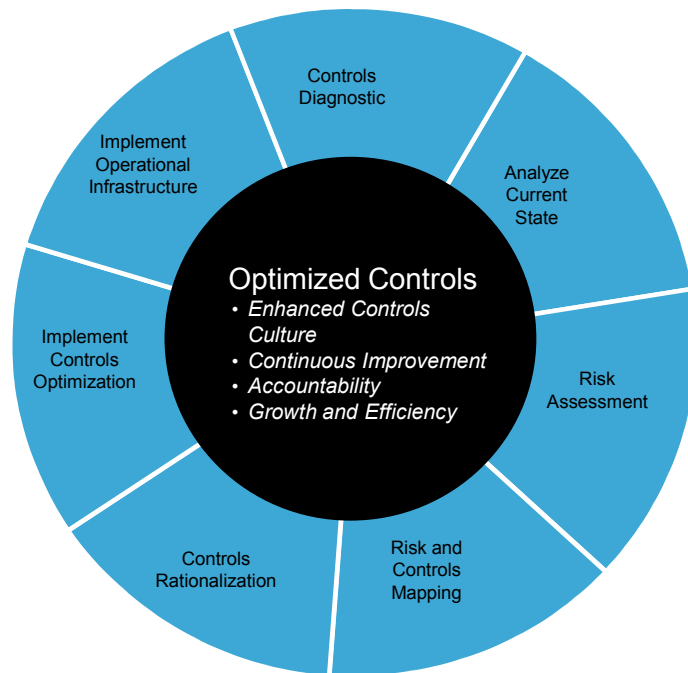


Where are *you* now and where do *you* want to be?



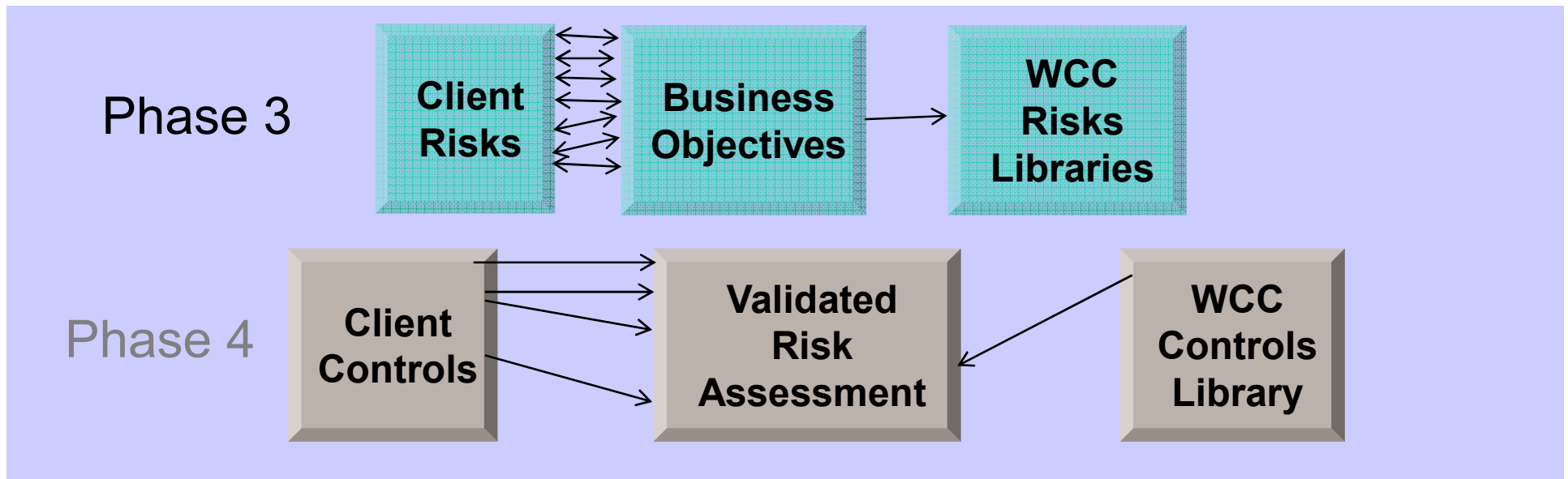
The Process

Establishing the right controls at the right cost for your organization



1. **Controls Diagnostic**
Perform diagnostic and assess needs
2. **Analyze Current State**
Evaluate to determine the landscape of controls
3. **Risk Assessment**
Conduct risk assessment.
4. **Risks and Controls Mapping**
Align risks and controls to PwC point of view
5. **Controls Rationalization Recommendations**
Provide controls optimization recommendations
6. **Implement Internal Controls Optimization**
Design and Implement the optimized controls
7. **Implement Operational Infrastructure**
Design and implement operational infrastructure for the system of controls

Risk & Control Mapping





Conclusion

- Regulatory requirements may require certain controls
- Privacy requirements may also require certain controls
- A Risk may need more than one control
- A Control may address more than one risk
- Technology provides so many options at various levels to set controls
- Use Risk-Controls Matrices for implementing controls.
- Challenge is how much is enough?



Over Protection & Under Protection

CISAC  **2008**
Conference of Information Security
Audit & Control

Questions?



Thank You

niraj.kapasi@in.pwc.com