NAI
Nouri Associates Inc.
"where experience counts"

Achieving IT Compliance

"How a Compliance Management Architecture Can Improve Your Compliance Efforts"

August 2005

Hamid Nouri
President, Nouri Associates

Client Briefing

Agenda

- Introduction
- High-Level Business Trends
- The Challenge of Regulations
- Sarbanes-Oxley Overview
- Compliance Management Architecture
  - COSO
  - COBIT
  - ITIL
  - ISO 17799
- Speaker Background

Introduction

Session Objectives

- Provide an overview of regulatory challenges faced by organizations
- Discuss an architectural approach that can be used to enhance your ability to address these challenges

High-Level Business Trends

Common Business Drivers Effecting Organizations

- Achieving profitable, predictable and consistent growth
- Competing effectively with local and global players
- Complying with, and keeping up with national and global Regulatory changes
- Improving quality while reducing costs
- Leveraging of global suppliers, services and workforce through outsourcing and offshoring.

The Challenge of Regulations

The Regulatory Storm

- **Sarbanes-Oxley** – U.S. Public Company Accounting Reform and Investor Protection Act (2002)
- **USA PATRIOT** – Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
- **FAS 150** – Financial Accounting Standards (2003)
- **21 CFR Part 11** – Title 21 Code of Federal Regulations (1997)
- **Senate Bill 1386** – CA Consumer Privacy Regulations
- **European Union Privacy Law** – Europe Privacy Regulation (1997)
- **Gramm-Leach-Bliley** – Financial Services Modernization Act of 1999
- **Basel II** – New Basel Capital Accord (1999)
- **HIPAA** – Health Insurance Portability and Accountability Act (1996)

- Many others depending on your industry ... over $15.5B to be spent on regulatory compliance in 2005 (AMR Research)!

Why The Trend Towards More Regulation?

- Some are industry specific and are intended to deal with issues within or evolution of an industry (e.g. HIPAA in Healthcare, GLBA in Financial Services). Most include provisions to protect consumer data security and privacy considerations
- Other are more broad based. Sarbanes-Oxley (SOX) is intended to restore investors' confidence in U.S. and global financial markets lost by major corporate spectacles such as:
  - Enron
  - Tyco
  - WorldCom
  - Adelphia
  - HealthSouth
  - Qwest
  - Many others ...
- 90+ Executives, Owners and Employees charged by SEC to date.
- Recent regulations have focused on correcting perceived market failures, fight terrorism, protect consumer privacy and ensure security.

Evolution of Corporate Governance in Response

From		To
Executive Decisions	→	Executive Accountability
Industry Guidance	→	Industry Oversight
Creative Accounting	→	Compliance Accounting
Secrecy	→	Transparency
Investors Seek Great Ideas	→	Investors Seek Value
Guidelines	→	Policies
Management	→	Governance

Compliance Challenges and Best Practices

- Some of the most common regulatory challenges include:
  - Consequence of non-compliance (prison, heavy fines)
  - Multiple rule sources (SEC, EU, FDA, Feds, etc.)
  - Monitoring responsibilities associated with the regulations
  - Testing is an ongoing responsibility
  - The perpetual nature of regulations.

- Some of the best practices in achieving compliance include:
  - Establish a Compliance Council and a Corporate Compliance Office
  - Establish clear communication channels and protocols
  - Manage Compliance as a Program, Not a Project
  - Leverage technology to manage content, events, tasks and approvals
  - Use Peer-Reviewed, Publicly Available Internal Control Frameworks to Improve Corporate and IT Governance
  - Identify and Use IT Solutions to Automate Process Controls Where Possible
  - Use a Logical Compliance Architecture to Reduce the Number of Controls and associated Costs Over Time.

Sarbanes-Oxley Act of 2002

The U.S. Public Company Accounting Reform and Investor Protection Act

Sarbanes

Oxley

Sarbanes-Oxley Act of 2002

- SOX Overview
  - Holds the CEO and CFO personally responsible for restatements due to misconduct
  - Imposes new obligations and responsibilities on audit committees
  - Requires process control and documentation
  - Strengthens penalties for corporate fraud
  - Requires rules to address securities analyst conflict of interest.

- Technology Implications
  - The CIO and CTO will drive risk assessments of enterprise applications
  - Systems to monitor compliance with codes of conduct will be installed
  - Internal Controls will be established in IT Operations
  - Business process modeling, analysis and management software installed
  - Will secure the confidentiality of systems and data leading to report generation
  - Records management policies and applications get increased focus.

Who is Responsible for What?

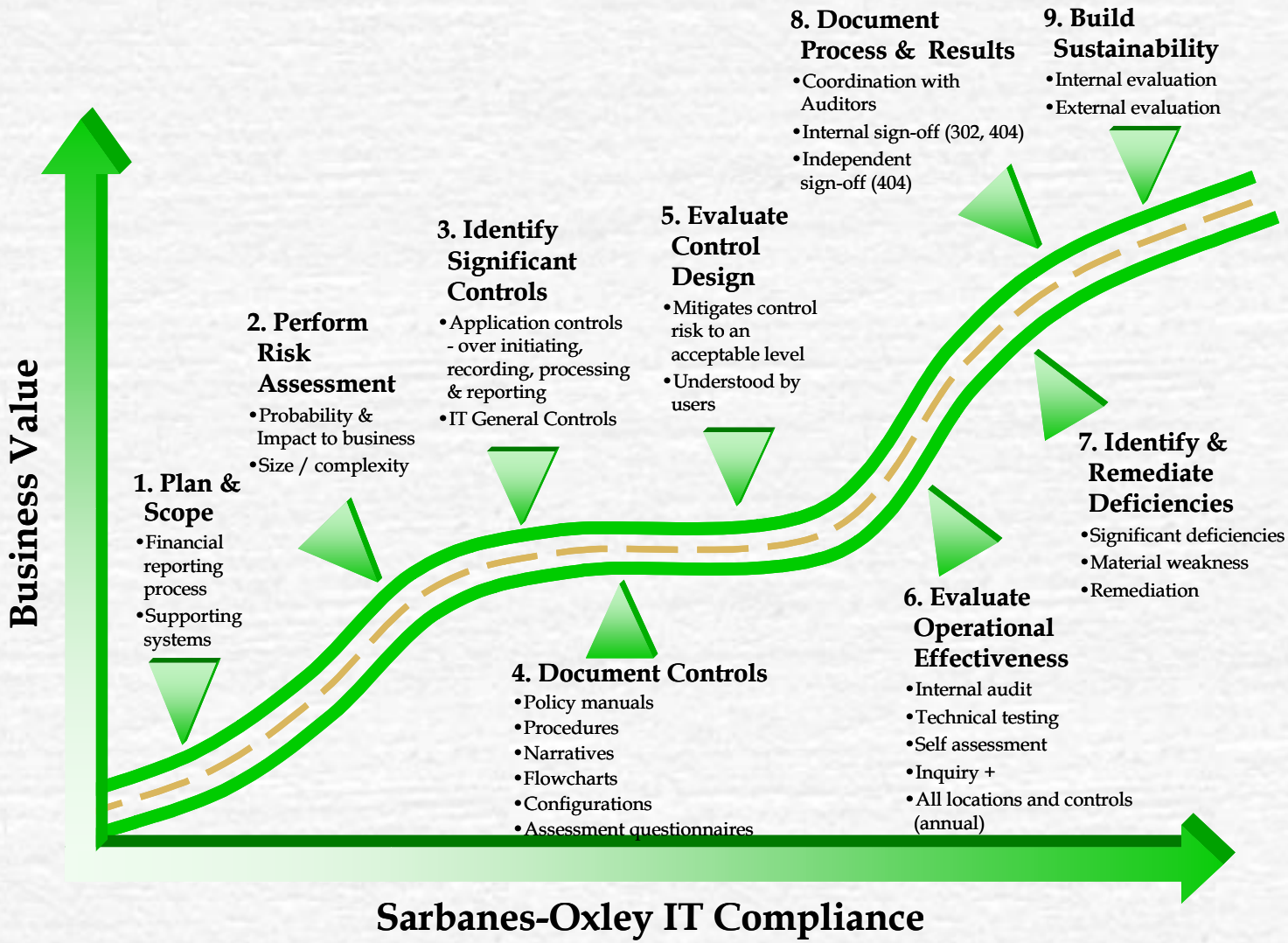
Section 302: Ultimate responsibility	*What:* Sign accounts, ensure accuracy and disclose anomalies *Who:* Board of Directors, CEO, CFO
Section 204: Penultimate responsibility	*What:* Understand controls, test and attest *Who:* External auditors and audit committee
Section 103: Standards	*What:* Demonstrate compliance with accounting standards, identify gaps and remediate *Who:* Auditors, CIO, chief counsel and compliance officer
Section 404: Report on internal controls	*What:* Process control, automation and documentation *Who:* IT managers, internal auditors, Controller, process specialists and IT systems
Section 409: Rapid disclosure	*What:* Operations, financial reporting and compliance *Who:* Accountants, controllers, records managers, security and IT managers

Internal Controls

- Sarbanes-Oxley was fashioned to protect investors by requiring accuracy, reliability, and accountability of corporate disclosures. It requires companies to put in place controls to inhibit and deter financial misconduct. And it places responsibility for all this – unambiguously – in the hands of the CEO.

- What is Internal Control?
  - Internal control is broadly defined as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
    - Effectiveness and efficiency of operations
    - Reliability of financial reporting
    - Compliance with applicable laws and regulations

SOX Readiness Roadmap



Source: Deloitte & Touche

Compliance Management Architecture

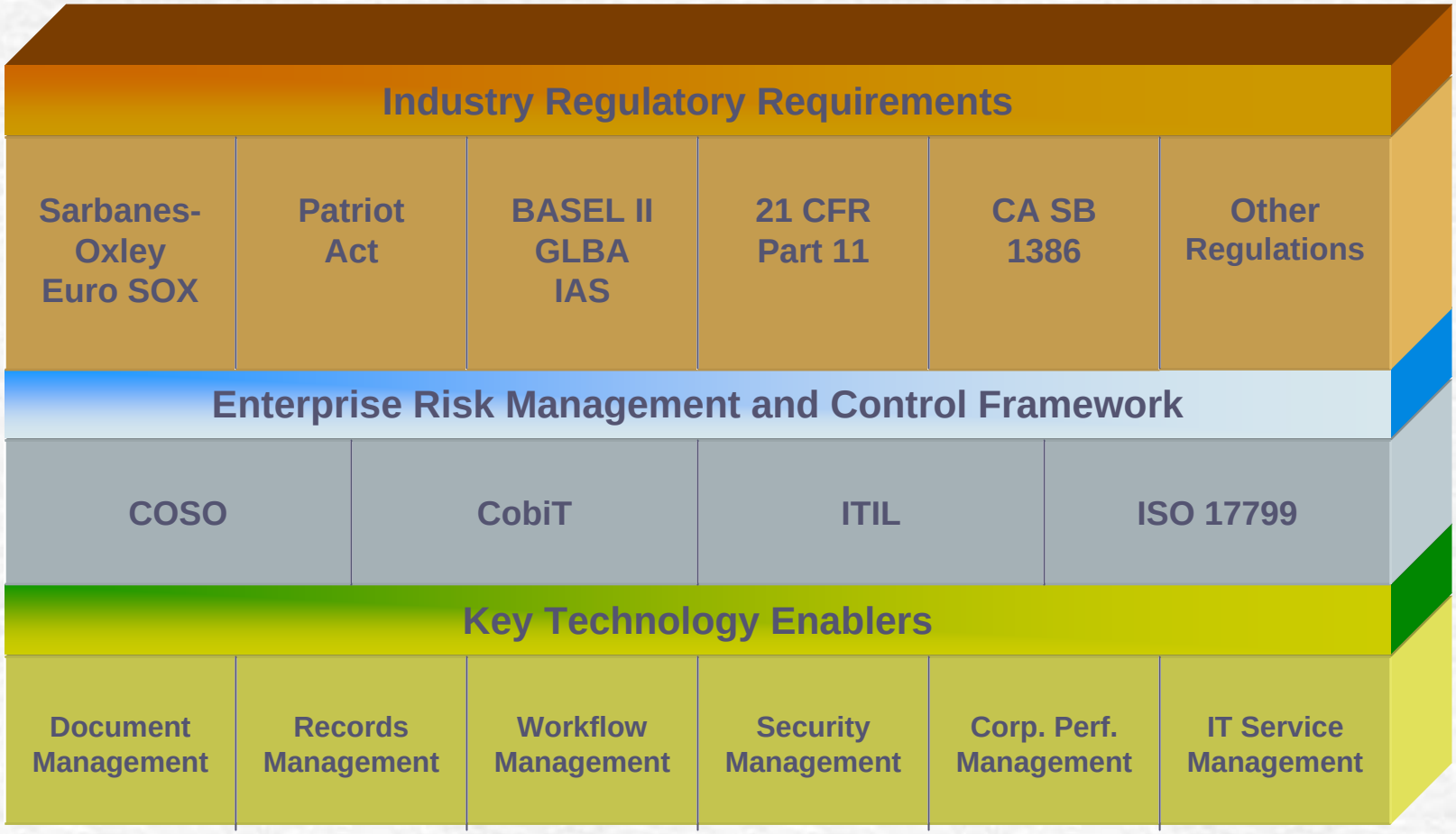
Leveraging a Compliance Management Architecture

- Complying with the latest regulatory requirements does not have to be treated as a one off activity. There are a number of common themes that run through most regulations. By using a Compliance Management Architecture framework organizations can save significant time and energy in meeting their compliance objectives.
- A Compliance Management Architecture Framework enables a comprehensive approach to managing an organization's compliance efforts.

"According to Gartner, by 2006, public companies that do not adopt a compliance management architecture will spend 50 percent more annually to achieve SOX compliance (0.8 probability).

Companies that choose one-off solutions to each regulatory challenge they face will spend 10 times more on compliance projects than their counterparts that take a proactive approach (0.9 probability)."

Compliance Management Architecture



NAI Nouri Associates Inc. "where experience counts"

Benefits of Compliance Architecture

- Security and privacy regulations typically have common concerns and requirements
  - As much as 80% overlap in functional requirements
  - Strategy: use one approach for all
- Compliance Frameworks are based on standard auditor recommendations and regulator expectations
  - “Here’s what we’d like to see...”
- Compliance Framework strategy can be based on industry best practices
  - Industry best practices have been tried and tested in many organizations
  - Efficient and effective (can result in competitive advantage)
  - Support materials available off the shelf
    - Procedures, policies, role descriptions
    - Don’t have to spend staff and management time creating equivalent processes

Internal Control Framework

- A Compliance Architecture can provide a set of internal controls for managing organizations
- Within the Compliance Management Architecture there are four compatible frameworks operating at different levels of detail and scope, that provide a set of controls and governance for IT
  - **COSO**
    - Organization wide controls
  - **COBIT**
    - Can satisfy and extend COSO controls relating to IT
  - **ITIL**
    - Can satisfy and extend COBIT controls relating to Service Management (Problem Management, Change Management, Release Management, etc.)
  - **ISO 17799**
    - IT Security Controls to meet and extend COBIT Security

Use of the Compliance Management Architecture

- COBIT and ISO 17799 health checks are used to determine current status and identify weaknesses in processes and controls
- ITIL is used to improve IT processes and controls, and ISO 17799 is used to improve security processes and controls
- ITIL is used to determine technology requirements and identify possible organizational structure, roles and responsibilities
- COBIT is used to define metrics.

What is COSO?

- Committee of Sponsoring Organization (COSO) of the Treadway Commission "*Internal Control – Integrated Framework*"

  (http://www.coso.org/)
- Organization-wide applicability
- Reporting target is Executive Board
- Created by professional auditor associations

COSO Components

- Five interrelated COSO components, derived from the way management runs a business
  - Control Environment
  - Risk Assessment
  - Control Activities
  - Information and Communications
  - Monitoring
- Each component has an associated set of sample audit questions & materials

COSO Enterprise Risk Management Framework

- The four objectives categories – strategic, operations, reporting and compliance – are represented by the vertical columns
- The eight components are represented by horizontal rows
- The entity and its organizational units are depicted by the third dimension of the matrix.

What is COBIT?

- Control Objectives for Information and related Technology (COBIT)

  (http://www.isaca.org/cobit.html)
- Covers all controls within or relevant to IT organization
- Reporting target is CIO
- Created by Information Systems auditors and IT Governance Institute in 1992
- First version launched in 1996 containing a new Framework, control objectives and audit guidelines
- Based on major research study into all relevant existing standards and best practices
- In 2000 management guidelines added providing maturity models, performance indicators and critical success factors

What is COBIT?

- Controls for IT Governance
  - Add value while balancing risk versus return for IT and its processes."
- Format
  - "The control of *IT Processes* which satisfy *Business Requirements* is enabled by *Control Statements* considering *Control Practices*"
  - There are 34 Processes defined in the framework
- Evaluation of COBIT controls
  - Assessment of maturity rating described for each control, ranging from 0 (non-existent) to 5 (optimized),
  - Critical Success Factors
  - Key Goal Indicators
  - Key Process Indicators (Metrics)

COBIT Control Domains

- Planning and Organization Controls
  - PO1 Define a strategic IT Plan
  - PO2 Define the Information Architecture
  - PO3 Determine the technological direction
  - PO4 Define the IT organization and relationships
  - PO5 Manage the IT investment
  - PO6 Communicate management aims and direction
  - PO7 Manage human resources
  - PO8 Ensure compliance with external requirements
  - PO9 Assess risks
  - PO10 Manage projects
  - PO11 Manage quality

COBIT Control Domains (cont'd)

- Acquisition and Implementation Controls
  - AI1 Identify automated solutions
  - AI2 Acquire and maintain application software
  - AI3 Acquire and maintain technology infrastructure
  - AI4 Develop and maintain procedures
  - AI5 Install and accredit systems
  - AI6 Manage changes

COBIT Control Domains (cont'd)

- Delivery and Support Controls
  - DS1 Define and manage service levels
  - DS2 Manage third-party services
  - DS3 Manage performance and capacity
  - DS4 Ensure continuous service
  - DS5 Ensure systems security
  - DS6 Identify and allocate costs
  - DS7 Educate and train users
  - DS8 Assist and advise customers
  - DS9 Manage the configuration
  - DS10 Manage problems and incidents
  - DS11 Manage data
  - DS12 Manage facilities
  - DS13 Manage operations

COBIT Control Domains (cont'd)

- Monitoring Controls
  - M1 Monitor the processes
  - M2 Assess internal control adequacy
  - M3 Obtain independent assurance
  - M4 Provide for independent audit

COBIT Processes Relevant to SOX Compliance

Compliance Management Imperatives	COBIT Processes
Manage Operations	DS 2 — Manage third-party services DS 7 — Educate and train users DS 13 — Manage Operations
Manage Risk and Controls	PO 9 — Assess risks PO 8 — Ensure external compliance M1 — Monitor M2 — Assess internal control adequacy
Manage Reliability	DS 5 — Ensure system Security DS 10 — Problems and incidents
Manage Systems	PO 5 — Manage the IT investment AI 4 — Develop and maintain procedures DS 9 — Manage the configuration
Manage Change	PO 11 — Manage quality *AI 5 — Install and accredit systems* *AI 6 — Manage change*
Manage Records and Data	PO 2 — Define IT Architecture DS 11— Manage data

What is ITIL?

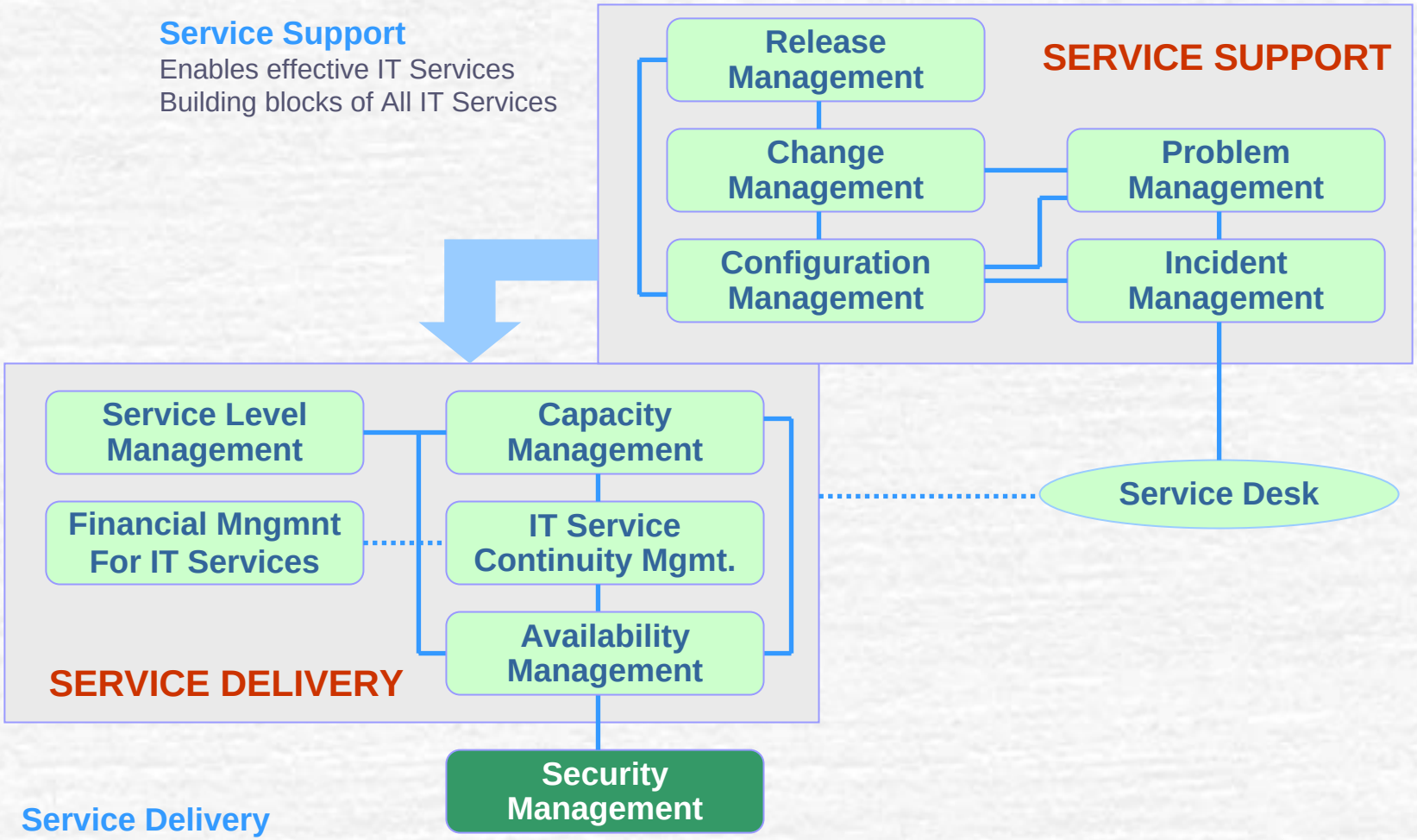
- IT Infrastructure Library (http://www.ogc.gov.uk/)
- Descriptions of IT processes and controls, especially Service Management
- Reporting target is CIO and IT senior management
- Created by British Gov., using set of IT best practices from public and private sectors worldwide
- ITIL (IT Infrastructure Library) is the most widely accepted approach to IT Service Management in the world.
  - provides a cohesive set of well defined best practices, drawn from the public and private sectors internationally.
- It is supported by a comprehensive qualification scheme, accredited training organizations, and implementation and assessment tools.

ITIL Framework

- Service Support Processes
  - Incident Management
  - Problem Management
  - Change Management
  - Configuration Management
  - Release Management
  - Service Desk Function
- Service Delivery Processes
  - Service Level Management
  - IT Financial Management
  - Capacity Management
  - Availability Management
  - IT Service Continuity Management

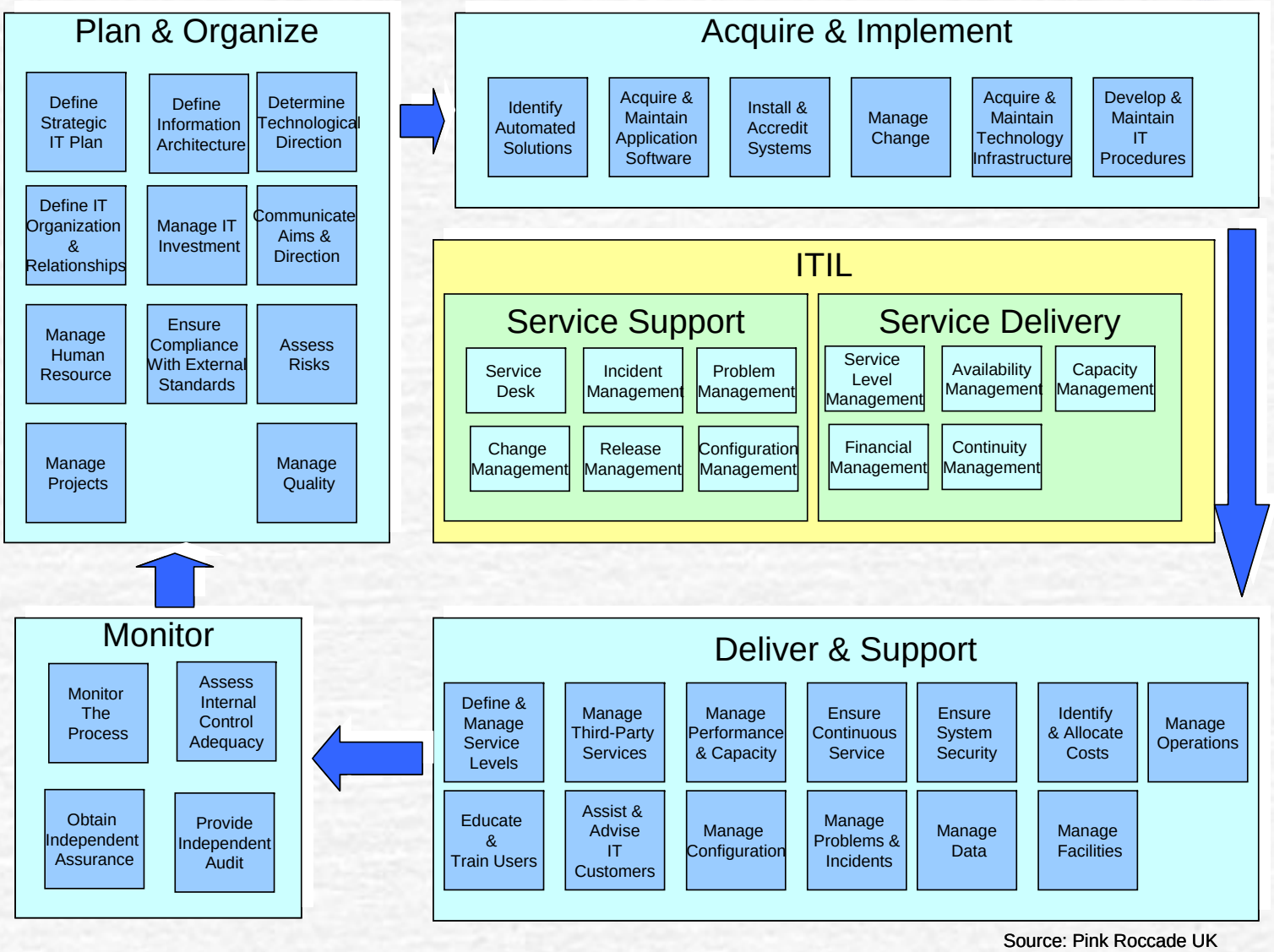
ITIL Framework

Service Support
Enables effective IT Services
Building blocks of All IT Services



Service Delivery
Management of the IT services

COBIT and ITIL



Source: Pink Roccade UK

What is ISO 17799?

- ISO is a widely accepted set of guidelines and controls for Information Security
- Controls are either based on essential legislative requirements or considered to be common best practice for information security.
- Controls considered to be essential to an organization from a legislative point of view include:
  - data protection and privacy of personal information
  - safeguarding of organizational records
  - intellectual property rights

Speaker Background

Speaker Background

- **Nouri Associates, Inc. (NAI)** is an international Information Technology Management Consultancy based in Northern California. NAI focuses on solving challenging IT related issues faced by an organization's senior management team. NAI specializes in providing highly experienced and expert talent to its global client base in a number of key practice areas such as IT Strategic Planning, IT Service Transformation, Compliance and Risk Management, Enterprise Architecture, IT Optimization and Sourcing Strategies.
- **NAI** assists organizations prepare for a successful audit and identify opportunities to leverage technology for effective and efficient compliance efforts. NAI also focuses on helping companies transform their IT Service Management capability by leveraging best practice frameworks such as ITIL.
- **Mr. Nouri** has over 25 years of experience in a number of IT leadership and management consulting roles. Prior to co-founding of NAI, he spent seven years at Gartner in a number of senior management roles in IT Management Consulting and Client Services. Prior to Gartner, he was the Executive Director of Distributed Systems at Countrywide Funding Corporation. He is a Certified Information Systems Security Professional (CISSP) and possesses the highest level of certification (Master/Manager) in IT Infrastructure Library (ITIL). He can be contacted directly at **1 (888) 556-3618 Extension 612** or via email at hamid.nouri@nouriassociates.com.

Nouri Associates, Inc.
One Embarcadero Center Suite 500
San Francisco, CA 94111
Telephone: 1 (888) 556-3618
Facsimile: 1 (415) 267-6127
eMail: info@nouriassociates.com
www.nouriassociates.com

NAI
Nouri Associates Inc.
"where experience counts"