RADIAN COMPLIANCE

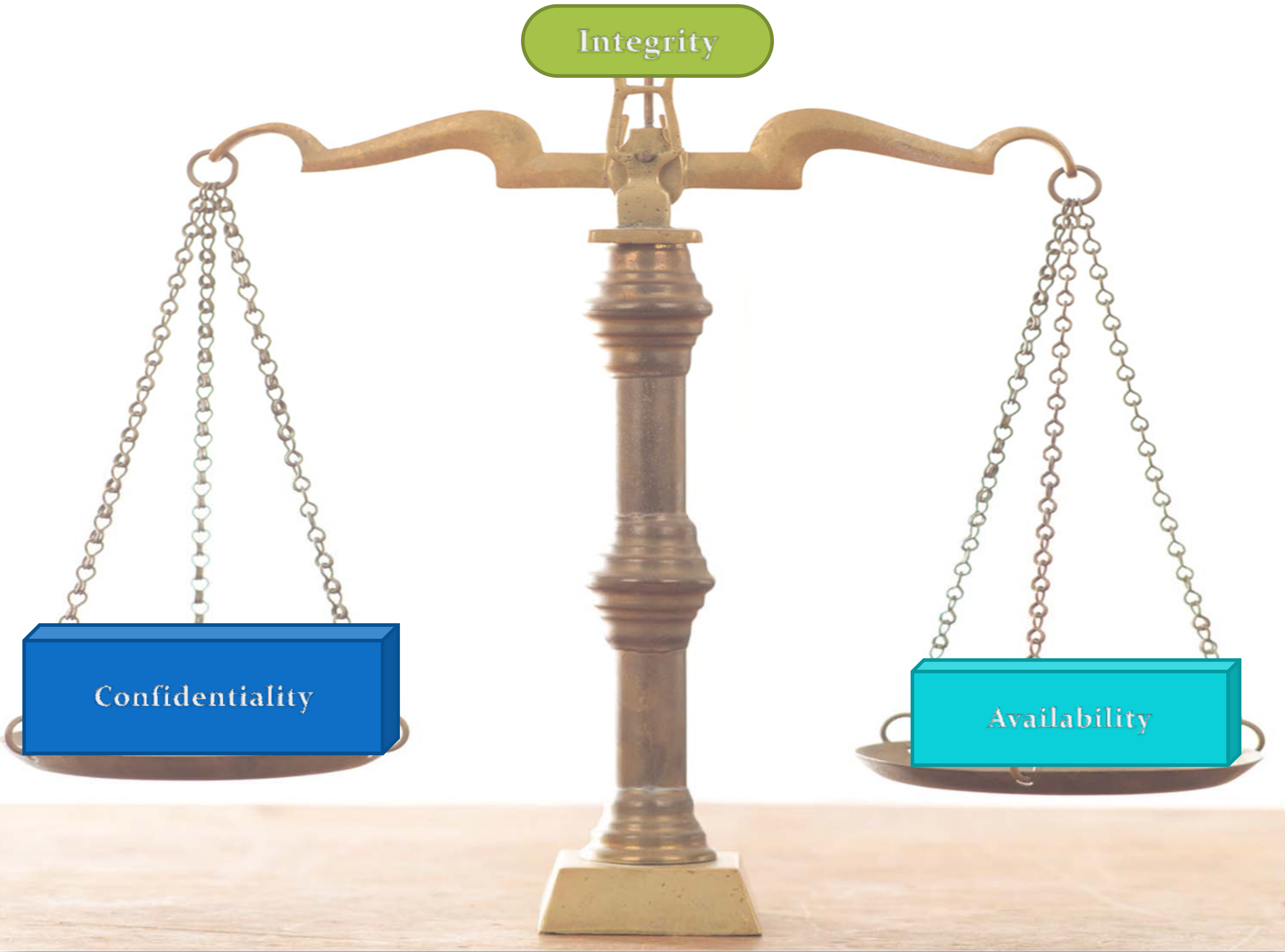
Over 25 years of rock-solid consulting for critical compliance needs.

Agenda

- Introductions
- Beyond the Project…
- ISO 27001 – Information Security Management System
- ISO 20000 – IT Service Management
- BS 25999 – Business Continuity Management System
- Overview of the Management System
- Case Studies
- Beyond the Project…

Beyond the project

- YABC
- Ensure policy and procedure has management commitment
- Repeatable processes throughout the organization, not just IT
- Faster, better, cheaper



Integrity

Confidentiality

Availability

ISO 27001 ~ Information Security Management System

- **ISO/IEC 27001:2005 Part 1, Specification** is the auditable standard (Shall's)
- **ISO/IEC 27002:2005 Part 2, Code of Practice** *(formerly ISO 17799)* is the Should's and provides the guidance

- **11** Domains / **133** Controls
- Additional guidance documents with the 27000 Series

11 Control Clauses(Domains)

- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

ISO 27001 is popular with

- Supply Chain
- Software as a Service (SAAS)
- Managed Service providers
- Educational Institutions
- Small and Medium organizations with internal IT
- Organizations with a global reach

ISO 20000 ~ IT Service Management

- **ISO/IEC 20000-1:2005 Part 1, Specification** is the auditable standard (Shalls)
- **ISO/IEC 20000-2:2005 Part 2, Code of Practice** *(formerly BS 15000)* is the shoulds and provides the guidance
- Based on ITIL processes and ISO 9000

Elements of Standard

- Service Management
- Service Delivery
- Service Continuity
- Service Availability
- Capacity Management
- Information Security Mgmt
- Configuration Management
- Business Relationship Management
- Supplier Management
- Resolution Process
- Incident, Problem Management
- Change Management
- Release Management

ISO 20000 is popular with

- Managed Service Providers
- Government Suppliers
- Enterprise organizations with large internal IT Service Delivery
- Mid Size organizations that use outsourced vendors to supports core IT services

BS 25999 ~ Business Continuity Management

- **BS 25999-2:2007, Part 2, Specification** is the auditable standard (Shall's)
- **BS 25999-1:2006, Part 1, Code of Practice** is the should's and provides the guidance
- Developed by leading experts in Business Continuity from both private and public sector
- Organizations on the Committee:
  - **Businesses :** Siemens, Royal Bank of Scotland, AON, Marsh, KPMG, Deloitte
  - **Institutes & Associations:** Small Businesses, IT and Emergency Management, BCI
  - **Government and Regulatory Bodies:** Financial, Emergency responders

Elements of Standard

- Requires Management Sponsorship and ongoing support
- Requires completion of a Business Impact Analysis and a Risk Assessment
- Requires the organization to build plans for emergency response and recovery
- Requires that training and plan testing programs be implemented and executed frequently
- Continuous Improvement

BS 25999 is popular with

- Supply Chain
- Organizations with an International customer base
- Any organization that is a critical supplier to consumer or business needs
- Businesses located in higher threat locations

The ISO Principles

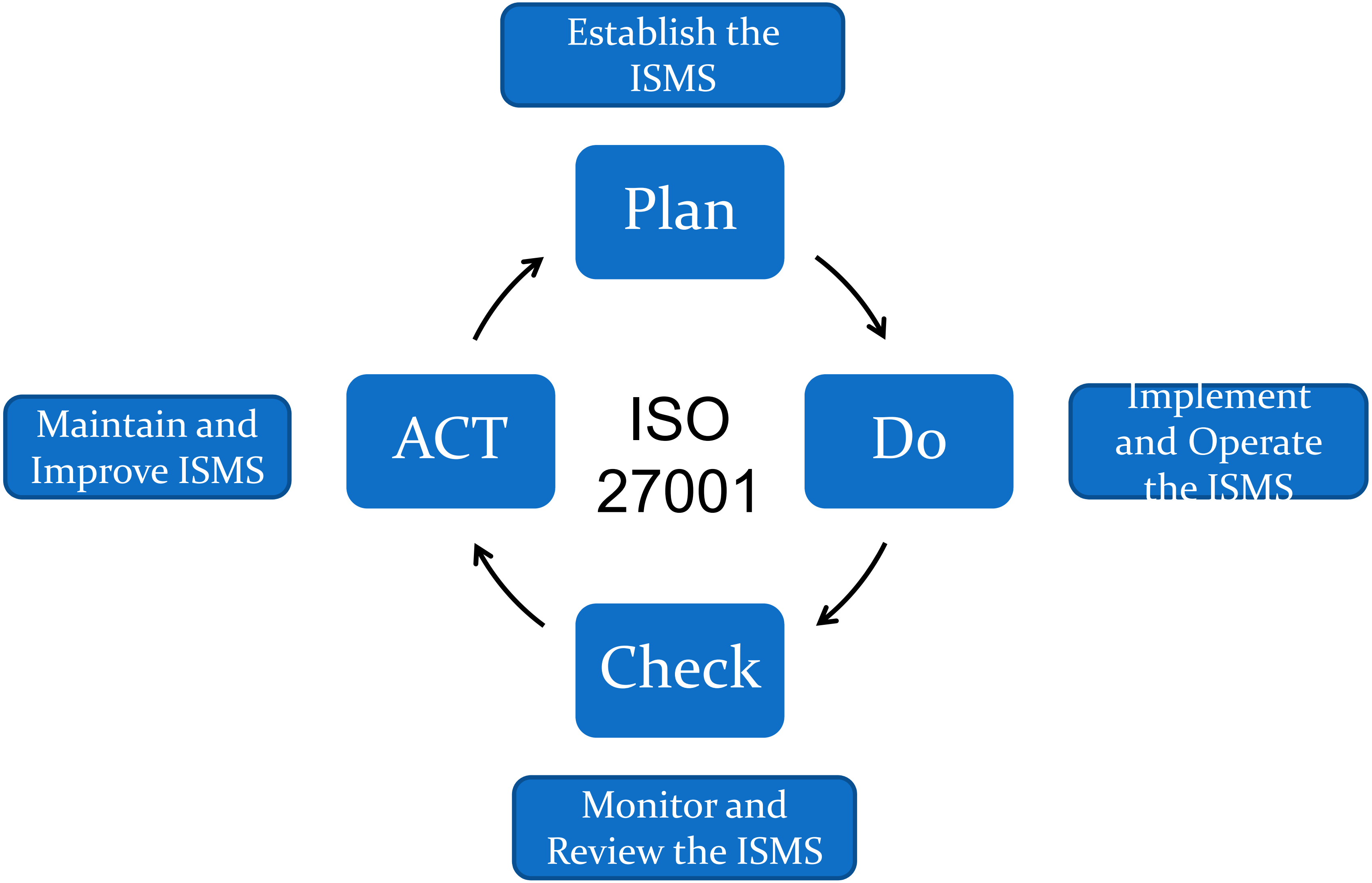
- Customer focus to meet requirements
- Leadership on purpose and direction
- Involvement of people at all levels
- Process approach to resources and activities
- Systems approach to management
- Continual improvement
- Factual approach to decision making
- Mutually beneficial supplier relationships

Understanding a Management System

- A management system is defined as

  A system to establish policy and objectives to achieve those objectives

- Uses Demming's theory of
  - Plan, Do, Check, Act
- **Management system** refers to what the organization does to manage its processes, or activities, so that its products or services meet the objectives it has set itself, such as:
  - satisfying the **customer's quality requirements**,
  - complying with **regulations**, or
  - meeting **environmental objectives**.



Establish the ISMS

Plan

Implement and Operate the ISMS

Do

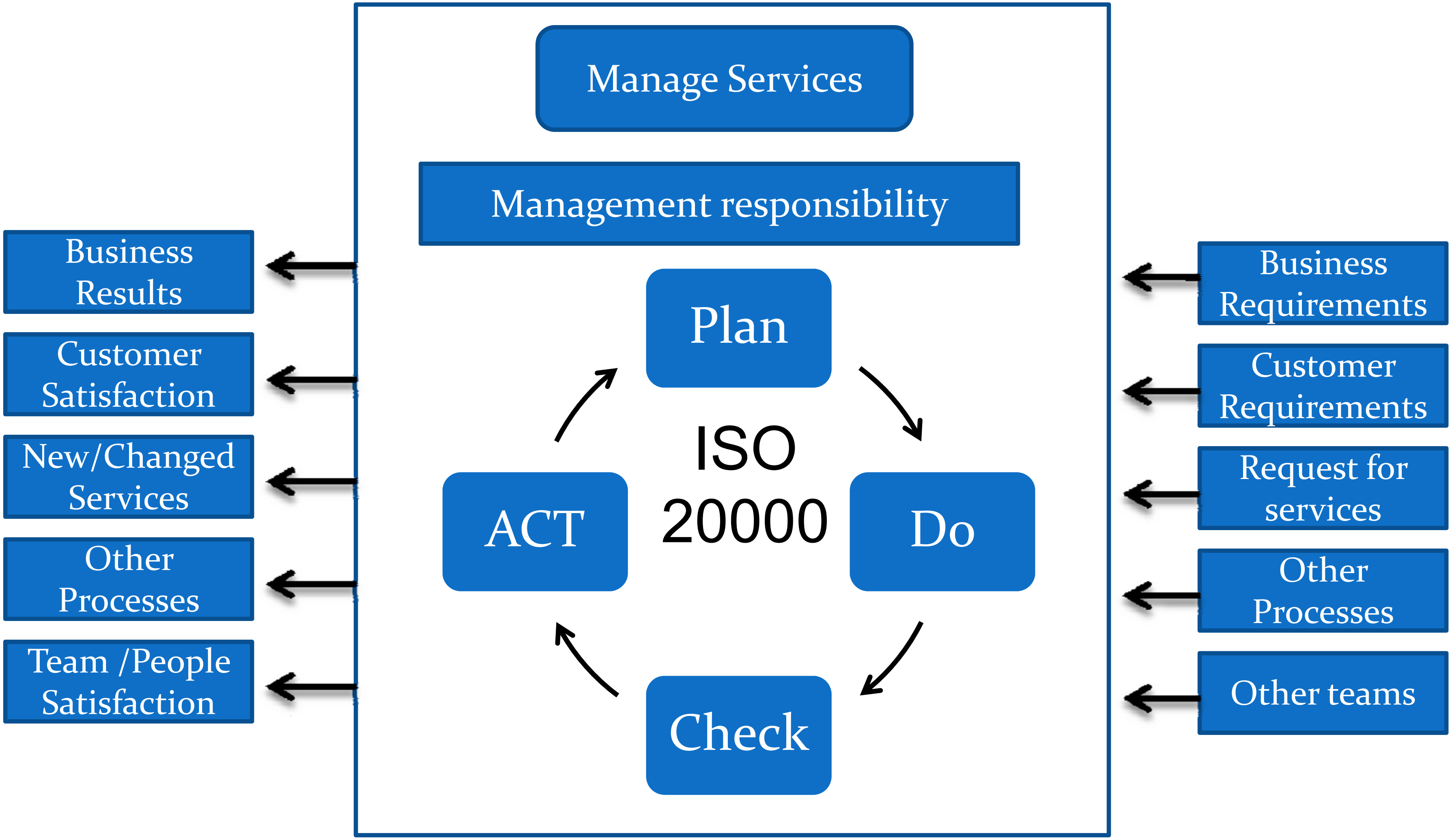
ISO 27001

Check

Monitor and Review the ISMS

ACT

Maintain and Improve ISMS



Manage Services

Management responsibility

ISO 20000

Plan

Do

Check

ACT

Business Results

Customer Satisfaction

New/Changed Services

Other Processes

Team /People Satisfaction

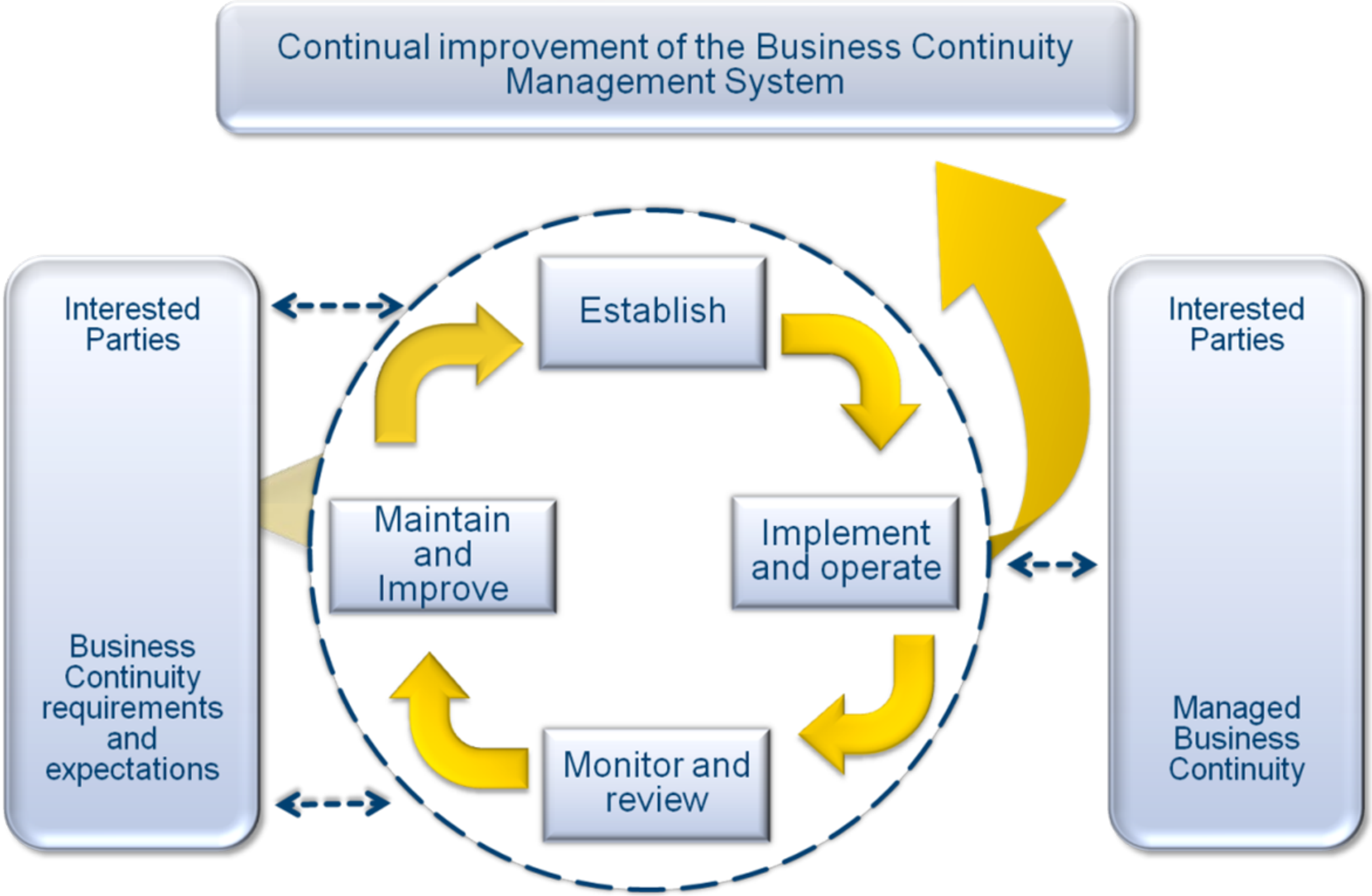
Business Requirements

Customer Requirements

Request for services

Other Processes

Other teams


Continual improvement of the Business Continuity Management System

Interested Parties

Business Continuity requirements and expectations

Establish

Implement and operate

Monitor and review

Maintain and Improve

Interested Parties

Managed Business Continuity

BS 25999

Case Study – ISO 27001

- **Company:** Midwest K-12 educational institution
- **Key Challenges:**
  - Security incidents continued to escalate in frequency and severity.
    - The district was paralyzed in their ability to address behavioral issues such as acceptable use.
  - There was significant liability concern.
    - Defensibility from frivolous lawsuits was marginal.
  - There was marginal management support
  - There was no management framework
  - There was no cohesion
  - There was no documented diligence
  - There was no mechanism to address behavioral issues
  - It was perceived as a technical issue
- **Solution: Implemented ISMS**
  - A management framework that was sensitive to the cultural and political environment unique to K-12 education.
  - Information security operations standards that clearly defined enforceable and auditable requirements.
  - Strategic plans that showed alignment with district goals and a going forward roadmap.
  - Incident management capabilities aligned with state guidelines.
  - Acceptable use policy, standards, and guidelines to serve as the basis for detective, corrective, or disciplinary actions.
- **Value**
  - A minimum baseline of information security throughout the district information systems.
  - Clear guidance to information technology employees and users.
  - Regulatory compliance
  - Behavioral enforcement

Case Study – ISO 20001

- **Company:** Verizon Business Solutions

- **Key Challenges:** Supplier requirement for government contracts to ensure key delivery of IT Services
- **Solution:** Received ISO 20001 certification for Government Network Operations and Security Center (GNOSC), located in Ashburn, Va.
- **Value :**
  - Improved quality of service through requirements such as system consistency and interoperability as well as internationally recognized third-party assessments and audits
  - Certification gives government customers the confidence that Verizon Business will continue to provide outstanding service and performance

Case Study – BS 25999

- **Company** - Repligen, a pharmaceutical company
- **Key Challenges**
  - Sole Source Company for their customers
  - Experienced increasing pressure from its customers to prove that they were not only improving their plan, but offer solid proof of the improvements
- **Solution** – Repligen became the 1st US company to be certified to BS 25999-2:2007
- **Value**
  - Build a level of confidence and trust in their supply chain
  - Communicate that level of confidence to their customers
  - Leverage the plans to identify areas that could be improved in the organization as a whole
  - Capture cost saving synergies between ISO 9000 and BS 25999

Beyond the project

- Using Internally recognized Standards gives your organization a GLOBAL advantage
- Doing more with less
- Faster, better, cheaper
- No longer the beggar in the boardroom

Upcoming Events

- March 19 NOON: IT Compliance Roundtable at the Illinois Technology Association, Chicago
- April 14-16: BSI present an ITIL Foundations course, Radian Training Center
- April 27– May 1: eFortress presents Holistic Information Security Practitioner, Radian Training Center

THANK YOU

RADIAN COMPLIANCE

Over 25 years of rock–solid consulting for critical compliance needs.

www.RadianCompliance.com

Lisa DuBrock	630-305-7100 x.227
Sally Smoczynski	630-305-7100 x.224