ASQ NORTHERN VIRGINIA SECTION 0511

ISO Management Systems

Guidance on understanding the benefits of an ISO Management System

RADIAN COMPLIANCE

Welcome & Introductions

RADIAN COMPLIANCE

www.RadianCompliance.com

	frameworks supported
Information Security	ISO 27001 • CobiT 5 • SSAE 16
Business Continuity	ISO 22301 • BS 25999 • NFPA 1600 SPC.1 • PS-Prep
IT Service Management	ISO 20000 • ITIL
Management Systems & Conformity Assessments	ISO 9001 • ISO 28000 • ISO 31000 ISO 17020 • FedRamp

Depend on Radian Compliance for:

Corporate Assessment • Implementation/Certification Readiness
Internal Audit • Education • Governance, Risk, Compliance

4031 University Drive, 206, Fairfax, VA 22030
3 Grant Square, 243, Hinsdale, IL 60521
www.RadianCompliance.com
Sally Smoczynski
SSmoczynski@RadianCompliance.com
630-728-7181

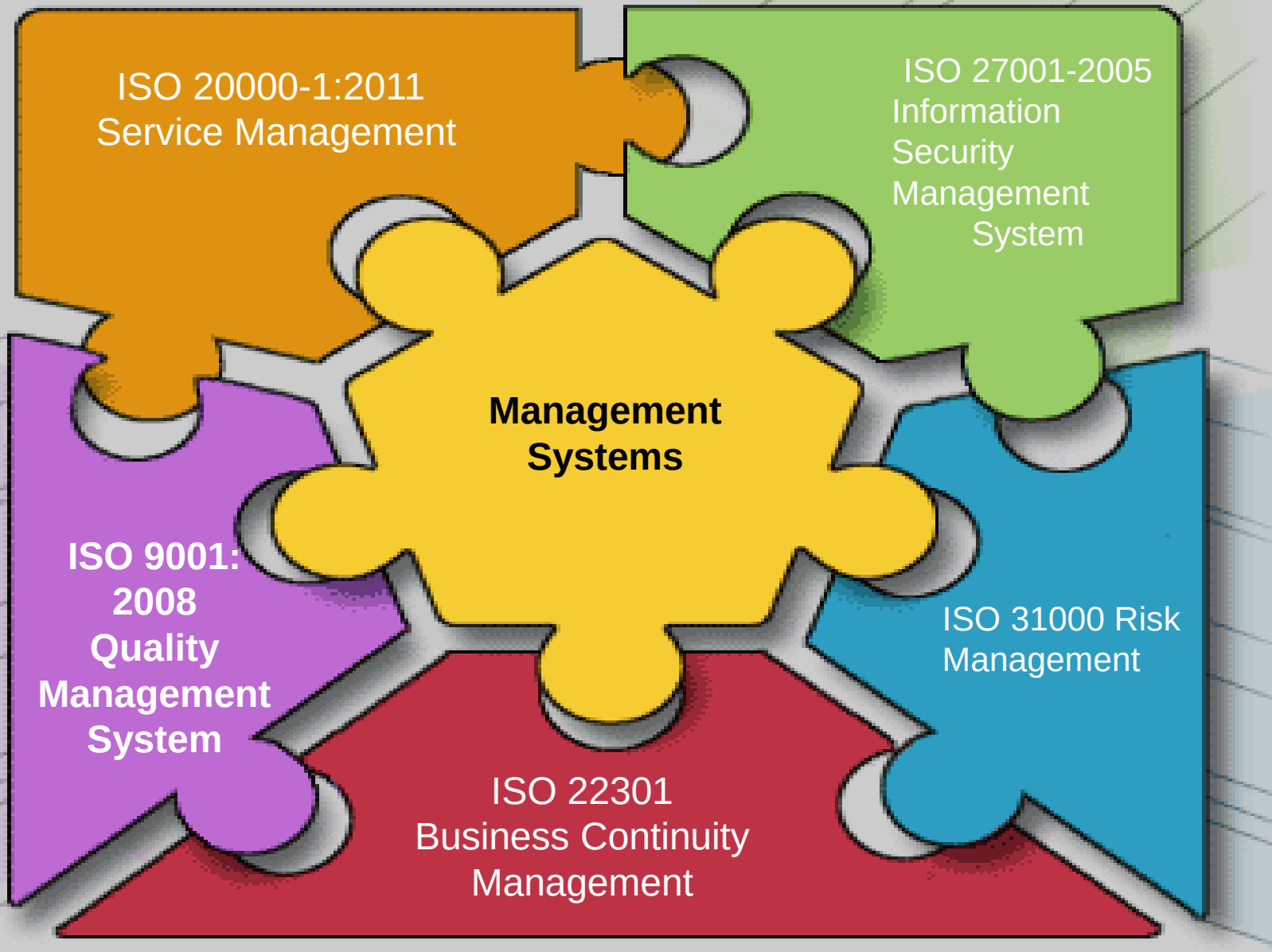
Agenda

- Brief intro to ISO
- General understanding for ISO certification
- Elements of an ISO Management System
- What's the new Annex SL?
- Benefits of an ISO Management System

Brief Introduction

Who is IOS and What Is ISO?

- The International Organization for Standardization (IOS) is a worldwide federation of national standards bodies.
- Working through Technical Committees, it has developed and published over 18,000 different ISO standards that are used internationally for subjects ranging from film speeds to wine glasses to quality management systems.
- The official purpose for the issuance of ISO Standards is to facilitate world trade through standardization.

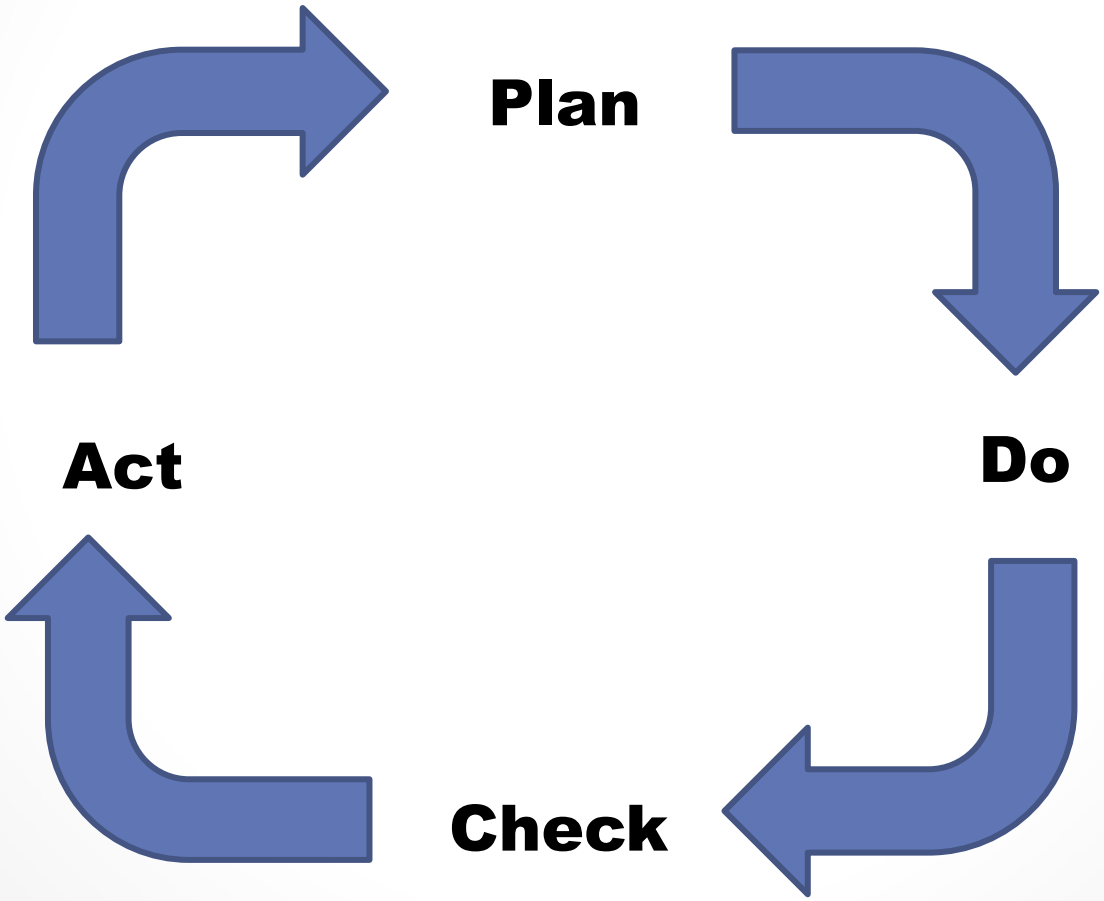

ISO 20000-1:2011
Service Management
ISO 27001-2005
Information
Security
Management
System
Management
Systems
ISO 9001:
2008
Quality
Management
System
ISO 31000 Risk
Management
ISO 22301
Business Continuity
Management

Understanding the Standards - Documents

Most standards have at least two supporting documents;

- **Requirements** – these are the "Shalls" and are required to be implemented unless exclusions can be taken. The auditor can only audit against the "Shalls".
- **Code of Practice** – these are the "Shoulds" and are guidance to assist you in implementation.
- **Guidance** – a fully implementable standard that does not have a "certification scheme". You can be compliant, but not certified.

Understanding the Standards - PDCA



Understanding the Standards - Scope

- Determine your Scope of Registration
- How many people within your organization support this Management System?
- How many processes are included?
- How many locations?

Requirements for Certification

Stages for Registration

- Submit application to registrar
- Stage 1: Assessment of readiness
- Stage 2: Assessment for registration audit
- Registration/certification awarded for 3 years
- Surveillance audits (at least annually)
- Recertification audit at the end of 3rd year

Registration

- Usually takes 1 or possibly 2 auditors 1 to 3 days
  - depending on scope, size, locations and personnel
- You will be told whether or not you will be recommended for registration at the completion of the Stage 2 audit
- Certificate usually arrives a 2 – 6 weeks later
- Maintaining your ISO Certification(s) is the first step in continuous improvement

Registrar/Auditor Selection Criteria

- Accreditation and scope of accreditation
- Reputation and customer acceptance
- Availability, cost, and location
- Knowledge of your business
- Culture fit with your organization
- Ability to audit all of your future standards

Note: The external auditor is hired by the Registrar and presented with qualifications to you upon agreement of audits. You cannot go out and hire your own external auditor.

Getting Ready for the Audit

- Determine team, set budget
- Internal auditor(s) training if using in-house resources
- Hire consulting firm if applicable
- Gap Assessment
- Implement requirements of standard to meet your business needs against the gap assessment
- Go-Live
- Hold Management Review Meeting
- Conduct Internal Audit
- Refine documentation
- Employee involvement training
- System adjustment
- Registration audit – Stage 1
- System adjustment
- Registration audit – Stage 2

Ongoing Commitment

- Getting certification is only the beginning
- Management Representative must keep up weekly/monthly/quarterly with tasks
- Internal audits are required at least annually
- Management review is required at least annually
- Timely completion and updates to CARs/PARs/OFIs
- Annual Surveillance audit by external registrar

An ISO Management System

Elements of a Management System

- Management Commitment
  - Top management shall……
  - Participation in Management Reviews
  - Provide input for continuous improvement
  - Accountable for resource management
- Resource Management
  - Identification of resources including human, technical, information and financial
  - Identification of roles, accountability and responsibility (RACI)
  - Competence, awareness & training

Elements of a Management System

- Management Reviews
  - Required inputs including reviews of audits, customer feedback, performance measurements, improvements, changes
  - Required outputs including actions recorded for improvements, documented improvements and the effectiveness of those improvements, additional follow-through of actions identified such as resource needs or completion of changes identified
- Document & Records Control
  - Documented procedure for creating, approving, maintaining, protecting archiving and destroying documents & records
  - Identifying documents of external origin

Elements of a Management System

- Internal Audit
  - Document an audit plan
  - Identify internal auditors, hire or train
  - Document outputs and act upon findings
  - Timely reporting

- Continual Improvement
  - Organization shall continually improve the effectiveness of the management system through the use of the policy, objectives, audit results, analysis of data, corrective and preventive actions and management review
  - Corrective/Preventive Actions recorded, planned and updated timely
  - Good Root Cause methodology
  - Review of effectiveness of actions taken

ISO 20000, 27001, 9001

ISO 20000	ISO 27001	ISO 9001
4.0 SMS General Requirements	4.0 ISMS 5.0 Management Responsibility	4.1 General requirements
4.1.1 Management Commitment	5.1 Management Commitment	5.0 Management Commitment
4.3.2 Control of Documents	4.3.2 Control of Documents	4.2.3 Control of Documents
4.3.3 Control of Records	4.3.3. Control of Records	4.2.4 Control of Records
4.4.1 Provision of Resources 4.4.2 Human Resources	5.2.1 Provision of Resources 5.2.2 Training, Awareness & Competence	6.0 Resource Management
4.5.4.2 Internal Audit	6 Internal ISMS audits	8.1.2 Internal audit
4.5.4.3 Management Review	7 Management Review	5.6 Management Review
4.5.5 Maintain and improve the SMS	8 ISMS improvement	8.4 Continual improvement

A New Structure

- Starting with ISO 22301, the Annex SL concept was introduced to standardize the management system requirements for ALL management system standards. The next standards to be published with the Annex SL is ISO 27001 later this year and the much anticipated 2015 release of ISO 9001.

Annex SL

- Introduction
- 1. Scope
- 2. Normative references
- 3. Terms and definitions
- 4. Context of the organization
- 5. Leadership
- 6. Planning
- 7. Support
- 8. Operation
- 9. Performance evaluation
- 10. Improvement

Benefits of ISO

Benefits of the Management System

- There are obvious internal benefits
  - Competitive Advantage
  - Commitment to detail for the scope; ie: quality, security, services, etc
  - Better employee engagement through training, communication and accountability
  - Formalized & repeatable processes
  - Accountability at all levels
  - Ongoing internal and external audits ensure weaknesses are identified and improvements are completed
  - Better governance and management of suppliers and outsourced processes
  - More efficient ability to change
  - Reduction in duplicate effort

Customer Benefits

ISO 9001 certified companies queried

- 75% improved their levels of customer satisfaction and loyalty
- 75% booster their operational performance
- 71% acquired new customers and retained existing ones.
- 55% achieved cost savings

- Source: BSI Excellerator Research 2011

Reducing Risk

- 85% of information security (ISO 27001) clients built stakeholder confidence
- 79% experienced faster recovery speeds from incidents
- 83% of business continuity (ISO 25999) clients reported enhanced reputation as the key benefit
- 64% of health & safety clients reduced incidents while 49% made cost savings
- 99% of organizations meets their Information Security objectives once they have implemented ISO 27001

- Source: BSI Excellerator Research 2011 and Erasmus University Study

Organizational Benefits

- 64% attribute direct cost saving to ISO 14001
- 74% report improvements to their corporate reputation
- 76% improve their compliance
- 61% report higher morale among staff

- Source: BSI Excellerator Research 2011

Client Insights

Large Printing Company

- The biggest benefit we have seen over the course of our ISO certification is a reduction in spoilage. Before we were ISO certified, we averaged about 6.5% spoilage per year. Last year our spoilage was 1.2%.

- Earnings for 2012 were 57 million so 1.2% was approx. $684,000 versus 6.5% would be 3.7 million. Pretty significant benefit.

- We have also benefitted from standardization of processes and improved communication.

Credits

- Google Images
- Clients personal benefit stats
- BSI marketing brochure “Why we do what we do”
- Quality Management CQI. CMI (BSI white paper)

Questions