Integration Technologies Group, Inc.

Uncompromising Performance

ISO 27001 OVERVIEW

BY MARKUS DARBY
VICE PRESIDENT – QUALITY STANDARDS & PERFORMANCE

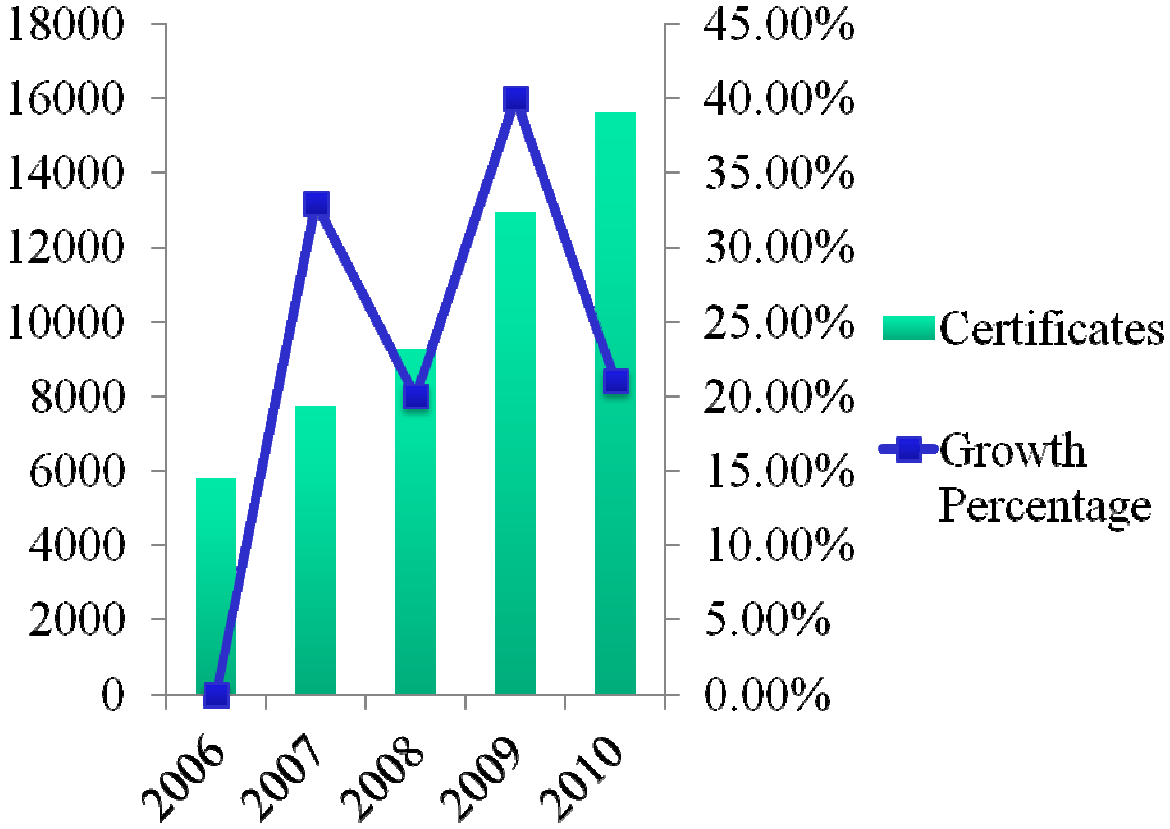
ITG

Agenda

- Current Market Information
- Overview of ISO 27001
- Overview of ISO 27001 Requirements, Controls and Assets
- Identify the Scope
- Overview of the Implementation Process
- Implementation Resources
- Overview of the Certification Process

ITG

ISO 27001 Adoption



- Interest continues to build
- Heaviest volume of registrations are in:
  - Japan
  - India
  - United Kingdom
- Most popular industry sections include:
  - Information Technology
  - Other Services

US Registrations

Microsoft

Keane an NTT DATA Company

Bechtel

citi

International Monetary Fund

Concur

salesforce

amazon web services

xerox

Fidelity Investments

SAP

SIEMENS

Medtronic
When Life Depends on Medical Technology

Kentucky Lottery

ORACLE

UNISYS

CSC

The World Bank
Working for a World Free of Poverty

Pacific Life

ADP

Northrop Grumman

Federal Reserve Bank of New York

PHILIPS
sense and simplicity

ITG

ITG Integration Technologies Group, Inc.
Uncompromising Performance

Lockheed Martin

verizon

Overview of ISO 27001

ISO/IEC 27001:2005 is an investment in the company's future.

- A "risk based" management system to help organizations plan, implement, and maintain an information security management system (ISMS).
- Assists organizations by providing a structured, proactive approach to information security by:
  - Ensuring the right people, processes, procedures and technology are in place to protect information assets.
  - Minimizing possible harm to organizations caused by deliberate or accidental acts.

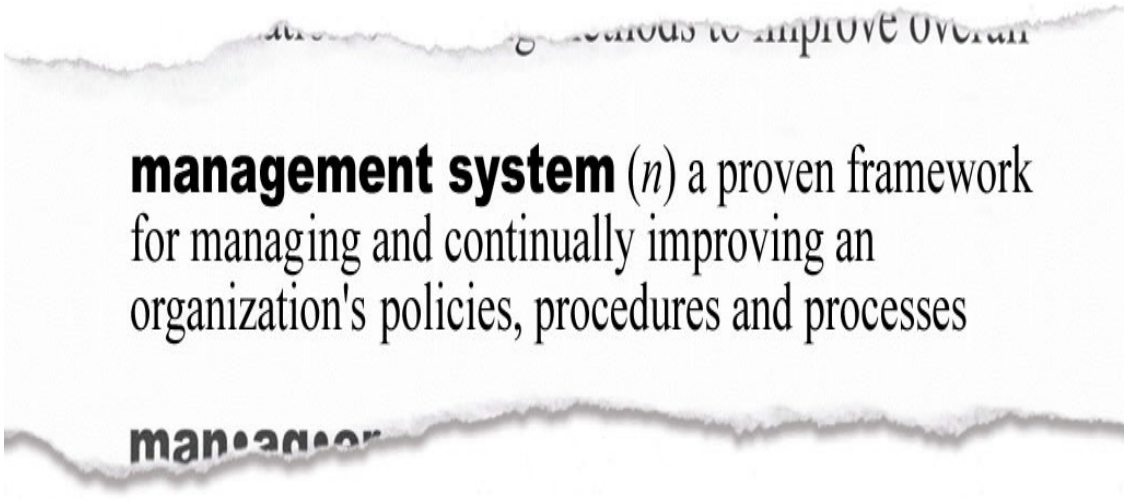
ITG

Overview of ISO 27001

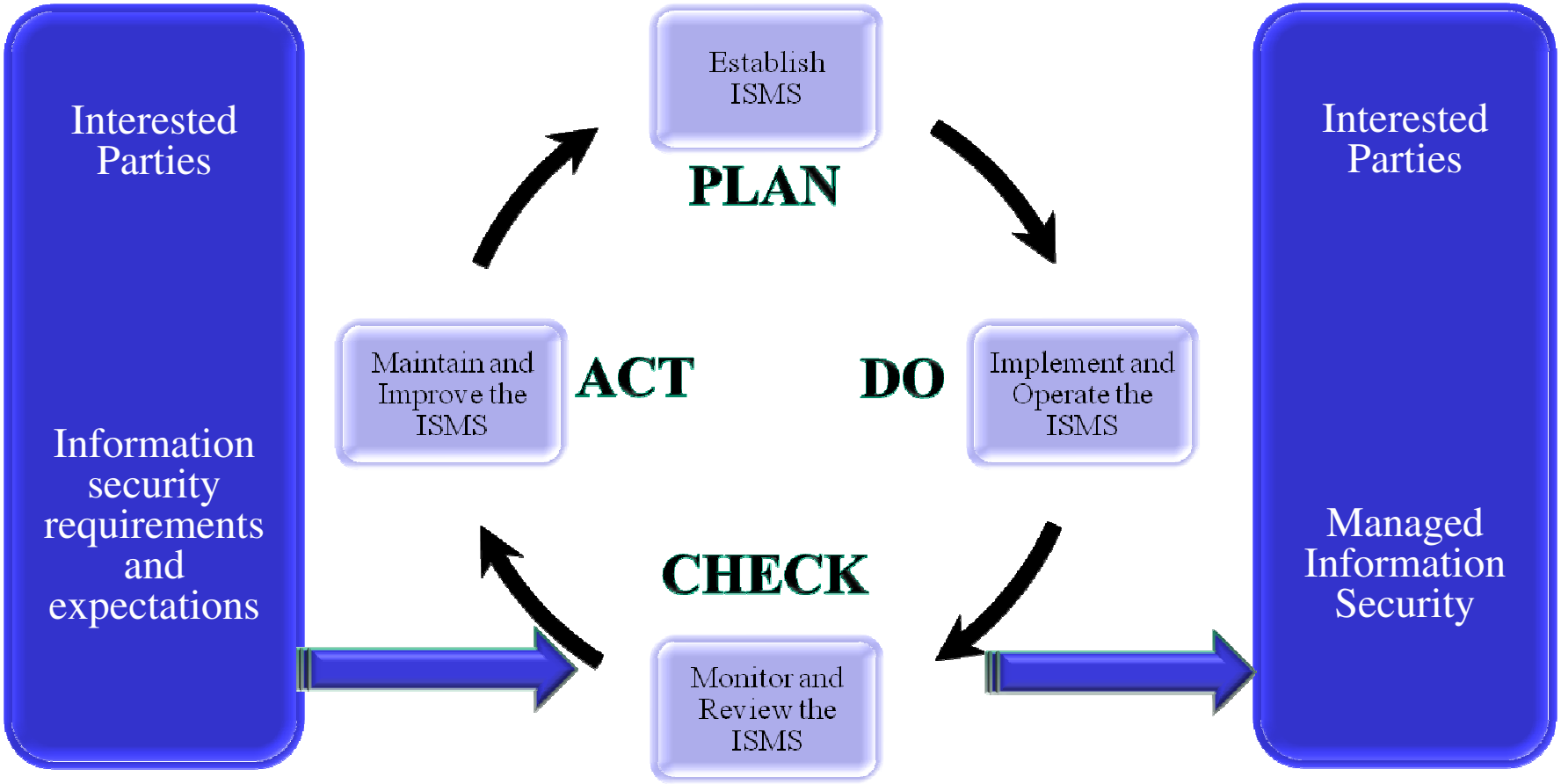
- ISO/IEC 27001 defines the requirements for an Information Security Management System.
- The standard is designed to ensure that you select adequate and proportionate security controls which helps you protect information assets and to give confidence to interested parties, including your customers.
- ISO/IEC 27001 is not an IT only standard; information is an organizational asset.
- The standard has no technology requirements; although there are IT related controls, as the majority of information is held on your IT systems.
- Protect the Confidentiality, Integrity and Availability (CIA) of assets

ITG

Overview of ISO 27001 (con't)



Overview of ISO 27001 (con't)



ISO 27001 Requirements

Mandatory Requirements (Sections 1-7)

- Section 1 - Scope
- Section 2 – Normative References
- Section 3 – Terms
- Section 4 – ISMS
- Section 5 – Management Responsibility
- Section 6 – Internal Audits
- Section 7 – Management Review
- Section 8 - Improvement

4.2 Establishing and managing the ISMS

4.2.1 Establish the ISMS

The organization shall do the following.

a) Define the scope and boundaries of the ISMS in terms of the characteristics of the business, the organization, its location, assets and technology, and including details of and justification for any exclusions from the scope (see 1.2).

b) Define an ISMS policy in terms of the characteristics of the business, the organization, its location, assets and technology that:

Annex A (Controls)

- Control objectives and controls
  - Based on the 12 domains of security
  - Includes 133 controls to evaluate, and take appropriate action on
- * - Can substitute more stringent controls from other frameworks

A.13 Information security incident management		
A.13.1 Reporting information security events and weaknesses *Objective:* To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.		
A.13.1.1	Reporting information security events	*Control* Information security events shall be reported through appropriate management channels as quickly as possible.
A.13.1.2	Reporting security weaknesses	*Control* All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.

ITG

ISO 27001 Mandatory Requirements

ISMS	• Set policies, procedures and posture • Implement and ISMS • Set monitoring steps • Maintain and improve • Document and record control
Management Responsibility	• Define policy, determine resources, set risk thresholds • Provide resources • Ensure competency
Internal Audits	• Develop an audit program • Review standard, legal and contractual requirements • Document activities
Management Review	• Review performance • Track achievement to target • Review suitability
Improvement	• Demonstrate improvement • Corrective and preventative action

ITG

ISO 27001 Controls

Control Area	
A.5 – Security policy	A.11 – Access control
A.6 – Organization of information security	A.12 – Information systems acquisition, development and maintenance
A.7 – Asset management	A.13 – Information security incident management
A.8 – Human resources security	A.14 – Business continuity management
A.9 – Physical and environmental security	A.15 – Compliance
A.10 – Communications and operations management	

Are all controls applicable in every scenario?

ITG

ISO 27001 Assets

- An Asset is defined as anything that has value to the organization
- Don't forget the scope of the Standard is:

  to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties

ITG

ISO 27001 Asset Identification

Primary Assets

- Business processes & activities
- Information (and Customer Data)

Supporting Assets

- Hardware
- Software
- Network
- Personnel
- Site
- Organization's structure

ITG

ISO 27001 Scoping

Desires

- What do we care about?
- What do our customers care about?

Responsibilities

- What can we change?
- What do we have control over?

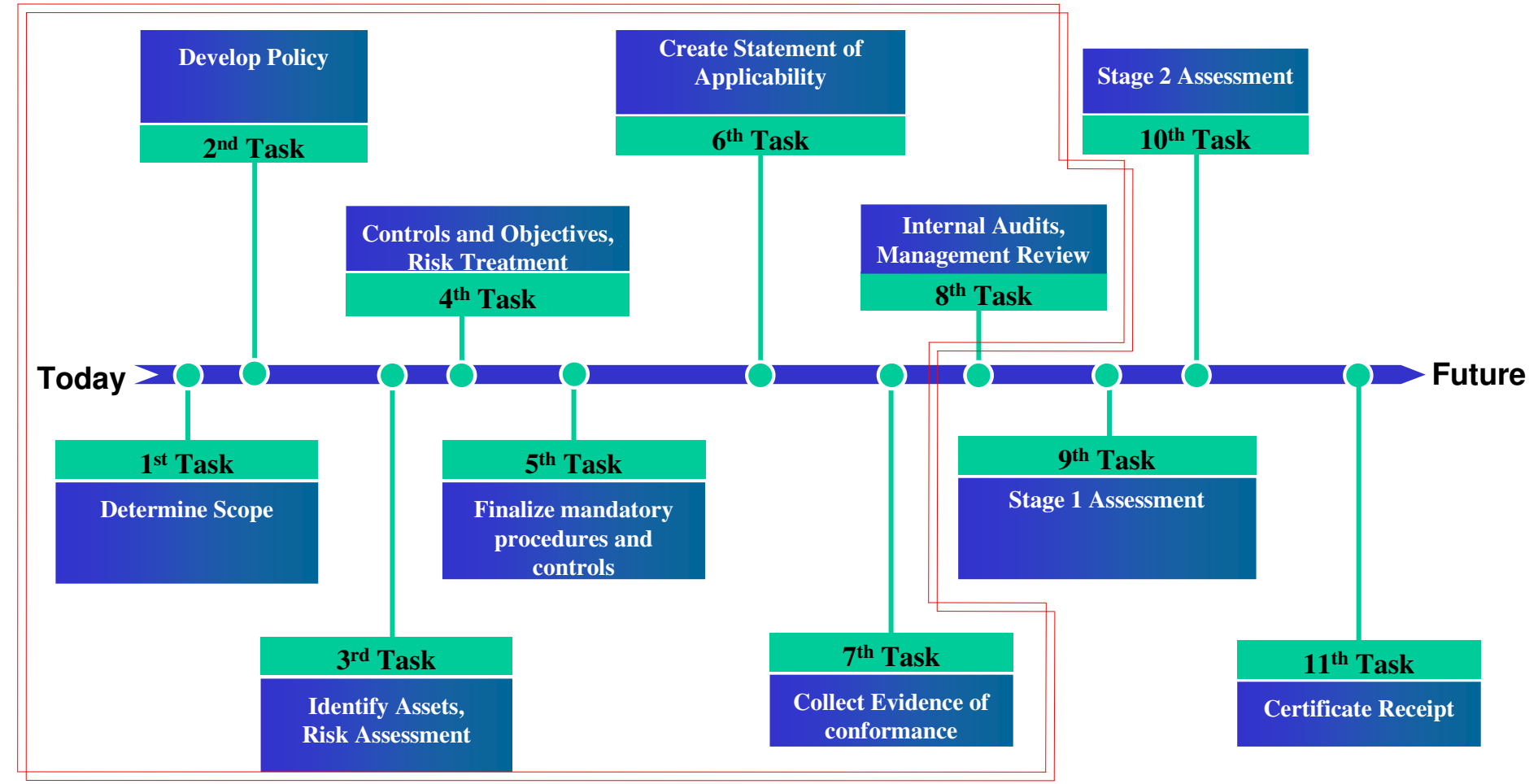
Impacts

- What can we do to benefit the organization?
- What assets are involved?
- What will we need to define?

Protection of company and customer information in the provision of Information Technology equipment, software and services to public and private sector organizations. The ISMS is managed in accordance with the Statement of Applicability dated 07/29/2011.

ITG

Implementation Overview



ITG

Resource Identification

Technical

- Security specializations
  - Physical
  - Logical etc.
- Documentation development

Managerial

- Business objective focus
- Obstacle removal
- Inter department negotiation
- Project management experience

ISO 27001 Achievement

Attributes

- Motivated
- Eager for opportunity
- Task achievement oriented
- Team oriented

Skills

- Training
- Coaching
- Influencing
- Analytical

ITG

Summary

Proposal Request
- Provide information on employees, locations, scope, assets under management

Contracting
- Sign and return paperwork to Perry Johnson Registrar

Scheduling
- Plan your audits approximately90 – 120 days in advance
- Auditor contact to organize logistics

Pre-assessment
- "Practice" Audit
- Preparation Confirmation
- Auditor Styles and Focus Items

Stage 1
- Review Documentation
- Examine Statement of Applicability
- Plan for Stage 2 – Implementation Audit

Stage 2
- Observe processes being performed
- Review records of completed activities
- Validate risk assessment results

ITG

PERRY JOHNSON REGISTRARS, INC.

Certificate of Registration

Perry Johnson Registrars, Inc., has assessed
the Information Security Management System of:

Company Name
755 West Big Beaver Rd., Suite 1340, Troy, MI 48084 United States

(Hereinafter called the Organization) and hereby declares that
Organization is in conformance with:

ISO/IEC 27001:2005

This Registration is in respect to the following scope of supply:

Embedded Systems and/or Device Driver Development
and Web Applications Development

Statement of Applicability Version 1 dated September 12, 2011

Such products shall be manufactured by the Organization at, or such processes or services shall be offered at or from, only the address given above. This Registration is granted subject to the system rules governing the Registration referred to above, and the Organization hereby covenants with the Assessment body duty to observe and comply with the said rules.

For PJR:

Terry Boboige, President

Perry Johnson Registrars, Inc. (PJR)
755 West Big Beaver Rd., Suite 1340
Troy, Michigan 48084
(248) 358-3388

UKAS MANAGEMENT SYSTEMS

PERRY JOHNSON REGISTRARS, INC.

The validity of this certificate is dependent upon ongoing surveillance and fulfillment of required sampling of sites.

Effective Date:	Expiration Date:	Certificate No.:
January 12, 2012	January 11, 2015	123456

Summary

ISO 27001 is a risk based security standard with a focus on business operation, not just IT. Remember:

- Implementation speed will be dependent upon:
  - Resource commitment
  - Desire
  - Current infrastructure
- By standardizing a common approach the implementation timeline can be reduced
- Carefully analyze the controls to determine if they apply to your situation and provide value to your security management system
- Maintain management commitment and support throughout the implementation
- Define a strong project plan and measure the results frequently

ITG

Contact Us

PERRY JOHNSON REGISTRARS, INC.

Perry Johnson Registrars, Inc.

Address: 755 W. Big Beaver Rd., Suite 1340
Troy, Michigan 48084

Telephone: 1-800-800-7910

Email: customerservice@pjr.com

Links: www.pjr.com

Name: Markus Darby

Title: Vice President QS & P

ITG INTEGRATION TECHNOLOGIES GROUP, INC.
UNCOMPROMISING PERFORMANCE

Integration Technologies Group, Inc.

Address: 2745 Hartland Road
Falls Church, VA 22043

Telephone: 571-422-0061

Email: markus.darby@itgonline.com

Links: www.itilsoftware.net

ITG