ISO 27001 – Is your sensitive data secure?

Presented by:
Paul Silva from Security Limits LLC
John Laffey from Perry Johnson Registrars

Paulo H. Silva CISSP, CISA, ABA, IRCA
Chief Information Security Advisor
Perry Johnson Registrars

- Currently serves as a Chief Enterprise Security Architect for Eversource Energy®.
- Over 15 years of experience, has served as Chief Security/Audit Executive and Head of Technology Compliance for multinational conglomerates such as Citigroup, Reuters®, and U.S Trust Bank®.
- Senior IT executive and information security/audit expert in financial, legal, utilities, and market-data processing industries.
- Carried out over 500 audits for fortune 500 companies in recent years.
- Associate member of the American Bar Association with hands on experience with cloud contract negotiations, ISO/27001, ISO/20000, and ISO 27001 implementations.

Please note:

- All participants have been muted.
- Please type your questions in the “Question” section of the dashboard – we will make time for as many questions as possible at the conclusion of this presentation.

Overview of Topics

- Roadmap to IEC/ISO 27001 Certification
- Misconceptions about ISO 27001 Certification
- ISO 27001 Certification Benefits
- ISO 27001 Requirements Structure
- Documentation Requirements
- Risk Assessment Process
- How Top Management Views ISO 27001
- Securing Commitment and buy-in from top management
- You are closer to ISO 27001 Certification than you think
- Real World examples, Q&A.
- Next Steps to become Certified

Is Your Sensitive Data Secure?

Identity Theft Resource Center

2014 Data Breach Category Summary

How is this report produced? What are the rules? See last page of report for details. Report Date: 1/5/2015 Page 1 of 1

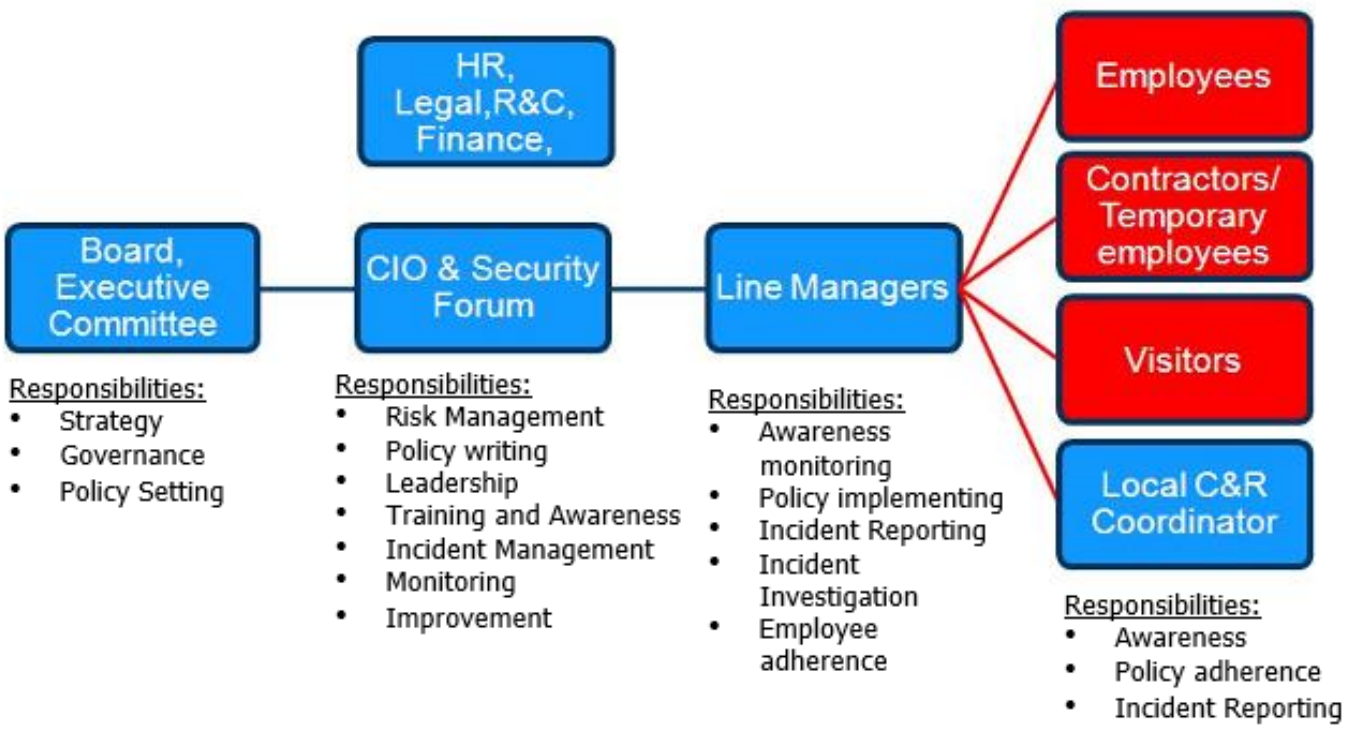
Totals for Category:	Banking/Credit/Financial	# of Breaches: 43	# of Records:	1,198,492
		% of Breaches: 5.5%	%of Records:	1.4%
Totals for Category:	Business	# of Breaches: 258	# of Records:	68,237,914
		% of Breaches: 33.0	%of Records:	79.7%
Totals for Category:	Educational	# of Breaches: 57	# of Records:	1,247,812
		% of Breaches: 7.3%	%of Records:	1.5%
Totals for Category:	Government/Military	# of Breaches: 92	# of Records:	6,649,319
		% of Breaches: 11.7	%of Records:	7.8%
Totals for Category:	Medical/Healthcare	# of Breaches: 333	# of Records:	8,277,991
		% of Breaches: 42.5	%of Records:	9.7%
	Totals for All Categories:	# of Breaches: 783	# of Records:	85,611,528
		% of Breaches: 100.0	%of Records:	100.0%

2014 Breaches Identified by the ITRC as of:	1/5/2015

Total Breaches:	783
Records Exposed:	85,611,528

Roadmap to IEC/ISO 27001:2013

Typical ISO 27001 Security Structure & Organization



Misconceptions about ISO 27001 Certification

- Implementing an information security management system that is certified to ISO 27001 is too costly.
  - Download documentation kit for approximately $1,200.00 dollars
  - Average Cost per Audit Day – $3,500.00 (Includes T&E)
  - Approximately 160-240 hours of IT security consulting services to support development and implementation of security management system; estimated at $150-$200 hourly.

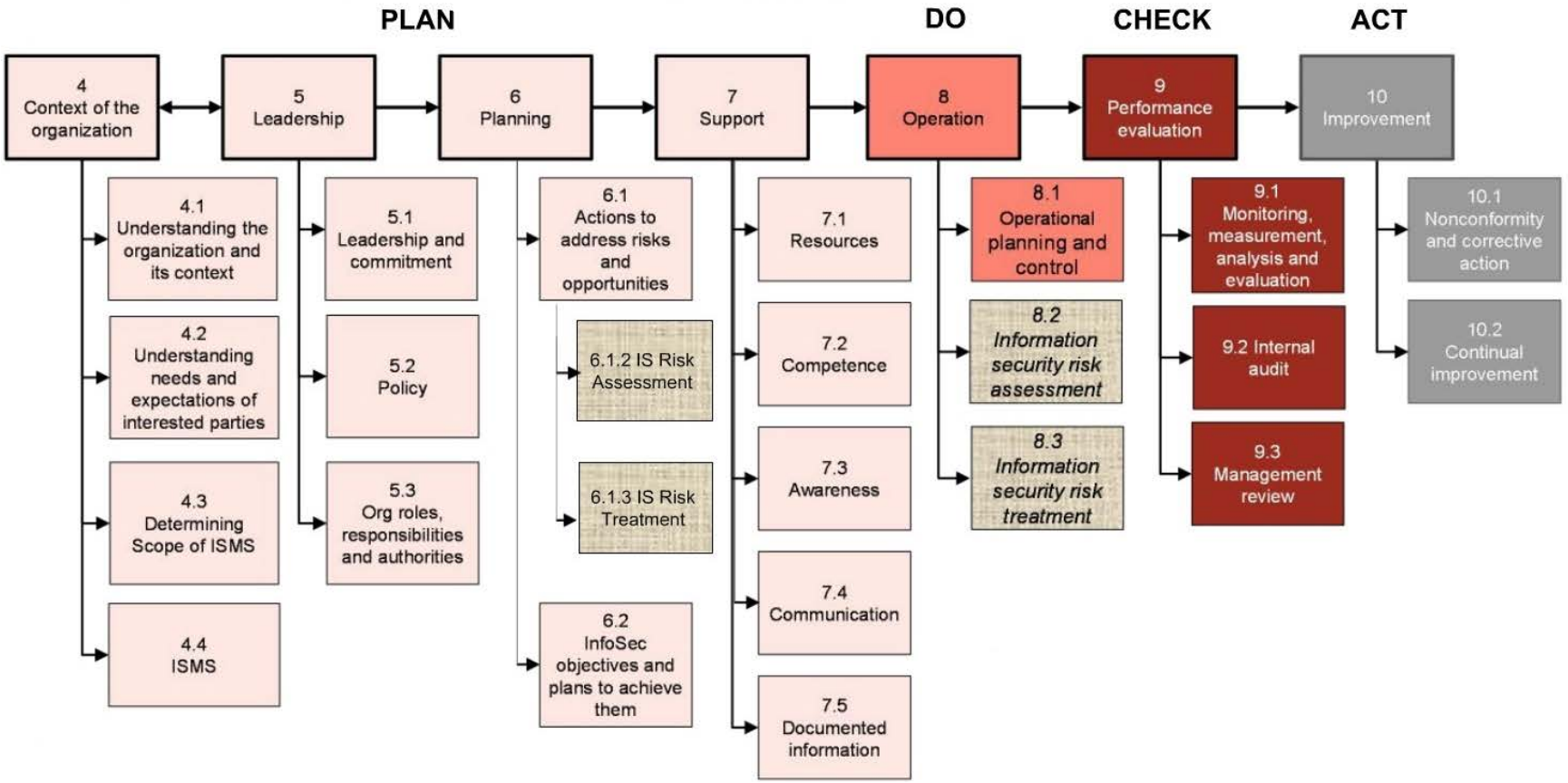
Misconceptions about ISO 27001 Certification

- Achieving ISO 27001 certification is only feasible for large organizations with huge amounts of resources.
- Implementing an ISO 27001 certified ISMS is too complex.
- Implementing an information security management system that is certified to ISO 27001 is too costly.
  - Documentation kit for approximately $1,200.00 dollars
  - Average Cost per Audit Day – $3,500.00 (Includes T&E)
  - Approximately 160-240 hours of IT security consulting services to support development and implementation of security management system; estimated at $150-$200 hourly.
  - One fulltime resource per 1000 users in scope

ISO 27001:2013 Certification Benefits

- Protects your reputation
- Provides reassurance to clients that their information is secure
- Cost savings through reduction in incidents
- Confidence in your information security arrangements
- Improved internal organization
- Better visibility of risks amongst interested stakeholders
- Meet customer and tender requirements
- Reduce third party scrutiny of your information security requirements
- Get a competitive advantage
- Improved information security awareness
- Reduces staff-related security breaches
- Demonstrates credibility and trust
- Improves your ability to recover your operations and continue business as usual

ISO 27001 Requirements Structure



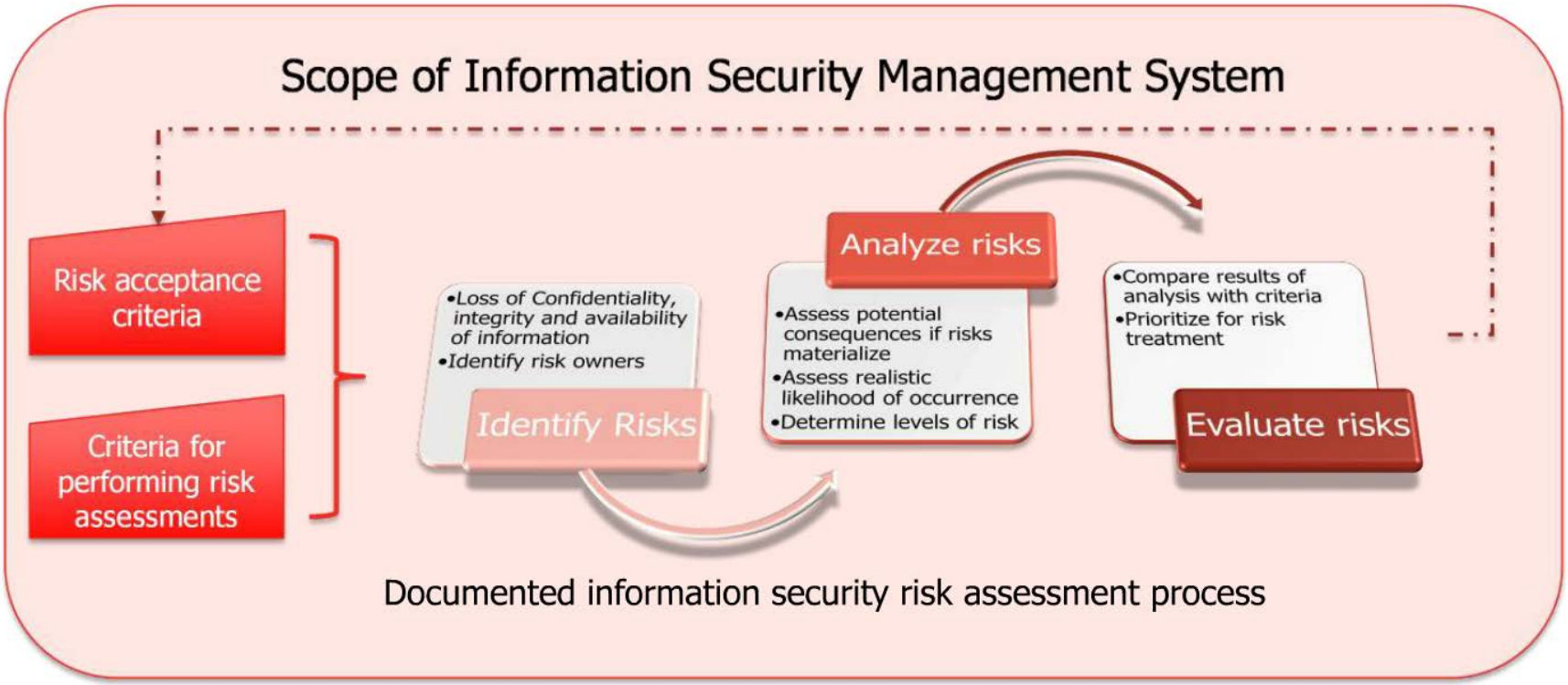
Documentation Requirements

- Documented information necessary for the effectiveness of the information security management system

documented information required

- 4.3 Scope of the ISMS
- 5.2 Information security policy
- 6.1.2 Information security risk assessment process
- 6.1.3 information security risk treatment process
- 6.1.3 d)Statement of Applicability
- 6.2 Information security objectives
- 7.2 d) Evidence of competence
- 7.5.1 b)documented information determined by the organization as being necessary for the effectiveness of the ISMS
- 8.1 Operational planning and control
- 8.2 Results of the information security risk assessments
- 8.3 Results of the information security risk treatment
- 9.1 Evidence of the monitoring and measurement results
- 9.2 g) Evidence of the audit programme(s) and the audit results
- 9.3 Evidence of the results of management reviews
- 10.1 f) Evidence of the nature of the nonconformities and any subsequent actions taken
- 10.1 g) Evidence of the results of any corrective action

Risk Assessment Process



How Top Management Views ISO 27001

Securing Commitment and buy-in from top management

- Must demonstrate ROI; simple business case
- Leverage existing statistical data
  - Present a realistic budget
  - Identify and Analyze man hours associated with regulatory compliance work
  - Security Breaches case studies
  - Cost reduction related to RFP bidding work
  - Competitive Advantage in the market place
  - Professional Liability and Cyber Security insurance reduction

You are closer to ISO 27001 Certification than you may think

- Hire a consultant to ensure rapid implementation success and ROI
- Take a look at specific business processes your organization already follows
- Define your certification scope; start small
- Be prepared to document all critical processes and functions into formalized procedures

Real World Examples

- Start with a Gap Analysis (Very Cost Effective)
- Proposal/RFP Bidding and Evaluation Process
- Real Positive Changes in Business Processes
- Market Differentiator (Certification has a direct link to market expansion and capital growth
- Microsoft…

Real World Examples

Managing Expectations in a New World…

Next Steps to become Certified

- For additional information and to begin the process of becoming certified please contact your Account Executive.
- John and I are available for calls to answer further questions you have regarding your companies next steps in becoming ISO 27001 Certified.