PALADION
HIGH SPEED CYBER DEFENSE

AND

DEKRA

ISO 27001 Professional Services

Guide to Implementation and Certification

DEKRA Company Overview

GLOBAL PARTNER
FOR A SAFE WORLD

Founded in Stuttgart, Germany in

1925

In more than

50 countries around the world

Over

44,000 employees

Paladion Company Overview

Global cyber security company with
18 Years of Experience

A team of over
1000 cyber warriors

Served over
700 Clients,
43 of them in
Fortune 500

- Delivering compliance services over a decade
- Recognized by Gartner in market guide report for MDR services
- Consistently rated in Gartner MSSP Reports since 2008
- Listed as MSSP specializing in mid market in Gartner report “options for mid market”
- Accredited PCI QSA & ASV since 2009
- Recognized by Forester & IDC analysts

SOC Locations

- Monitoring 25 billion security events daily across six geographies.
- Responding to over 100 incidents daily.
- ISO 27001, ISO 20000 and SOC 1 attested

Speakers

Tom McDonald

VP – US Enterprise Engagements, Paladion

30+ years of industry experience

Has presented papers and been a speaker at major technology conferences in the U.S. and abroad

Hariharan A.

Principal Consultant, Paladion

11+ years of industry experience

Has performed 50+ compliance/risk assessment projects

Agenda

- Need for ISMS
- Intro to ISMS and ISO 27001
- 5 Steps towards ISO 27001 certification
- ISO 27001 Benefits
- Q&A

PALADION
HIGH SPEED CYBER DEFENSE

Need for Information Security Management System (ISMS)

Need for ISMS

Information Explosion

- Terabytes and peta bytes of data
- Structured & Unstructured data
- Increased complexity in managing & securing data

Rising security threats, incidents

- Rapid evolution and high level of innovation
- Statistically 3.5M records are breached everyday
- Impact on financials, reputation, customer

Demonstrate higher assurance

- Adopting global best practices
- Defining clear accountability for security
- Measuring effectiveness of security controls

An Information Security Management System enables an organization to safeguard their sensitive information and continuously protect it.

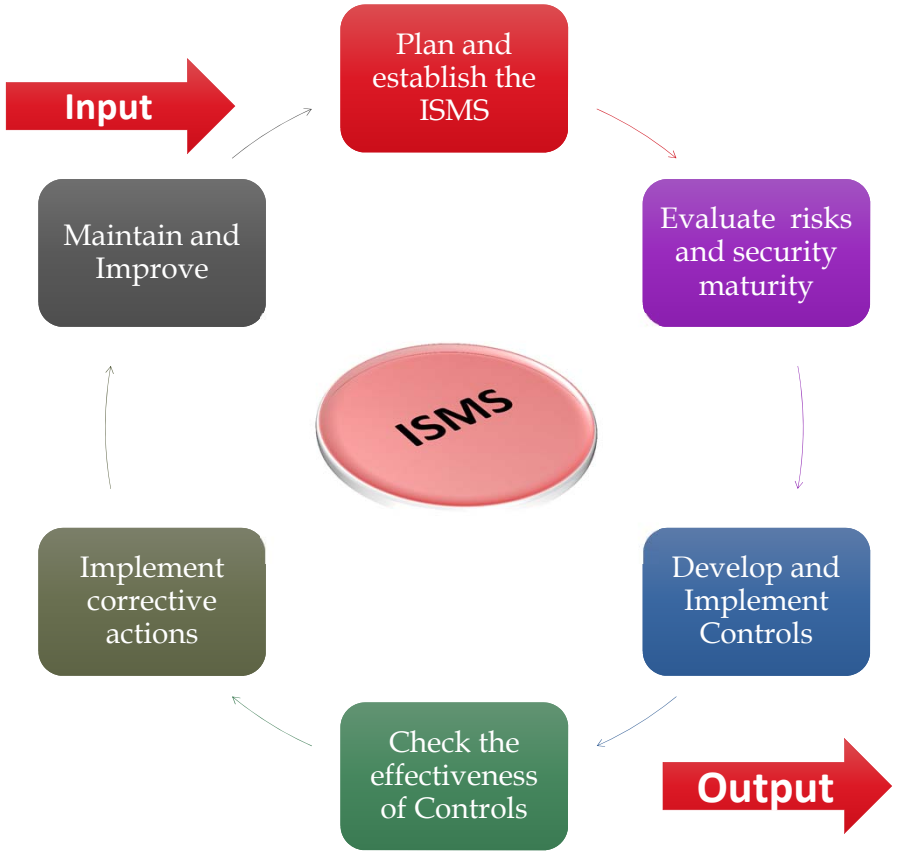
PALADION
HIGH SPEED CYBER DEFENSE

Introduction to ISMS

Introduction to Information Security Management System

Business Goals

ISMS Goals



Value From ISMS

1. Commitment to customer
2. Customer goodwill
3. Competitive advantage
4. Reduced security Incidents
5. Process maturity
6. Platform for enterprise wide Security Framework

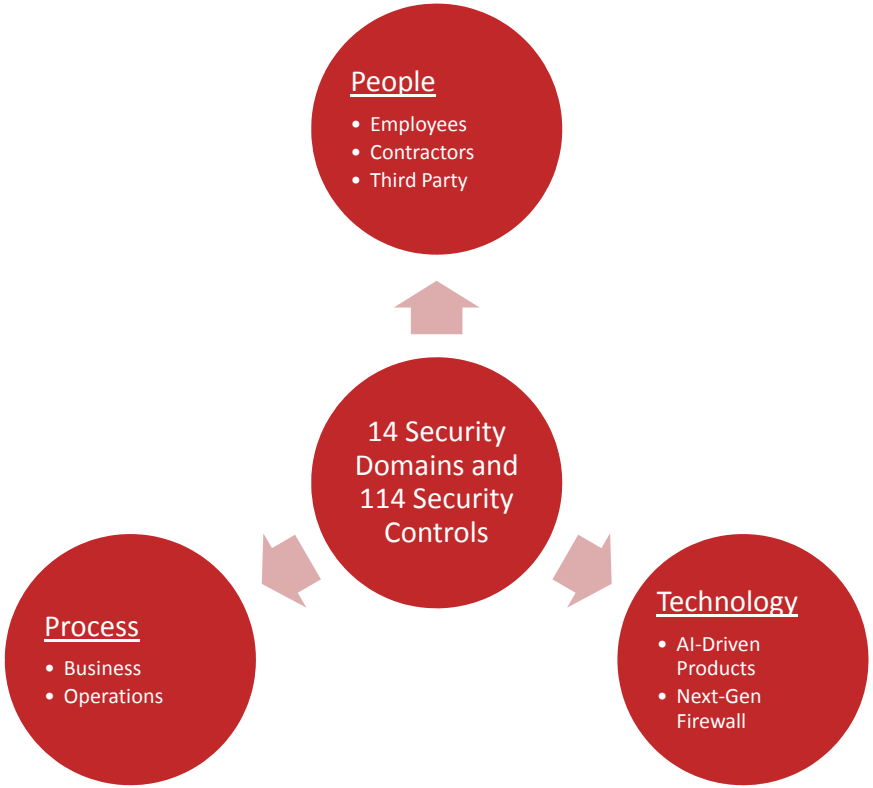
Intro to ISO 27001

- Strategic decision for over 20 years.
- First published during 1995 by BSI Group
- Originally known as BS 7799
- Later adopted by ISO in 2000 as ISO/IEC 17799 (Information Technology - Code of practice for information security management)
- ISO/IEC 17799 was then revised in June 2005 and finally incorporated in the ISO 27000 series of standards as ISO/IEC 27002 in July 2007
- Current version is ISO 27001:2013
- As of today there are 45 standards published under ISO27000 standards related to "information technology - security techniques"

ISO 27001 Information technology – Security Techniques – ISMS

- The standard specifies an Information Security Management System (ISMS) in formalized, structured and succinct manner.
- The current version (ISO 27001:2013) has 14 information security domains that consist of 114 security controls
- Ensures security of all information assets including people, process, and technology including suppliers and vendors.

ISO 27001 14 Security Domains	
IS POLICIES	HUMAN RESOURCE SECURITY
ASSET MANAGEMENT	CRYPTOGRAPHY
ACCESS CONTROL	COMMUNICATIONS SECURITY
OPERATIONS SECURITY	SUPPLIER RELATIONSHIPS
SYSTEM DEVELOPMENT	IS ASPECTS OF BCM
IS INCIDENT MANAGEMENT COMPLIANCE	PHYSICAL & ENVIRONMENTAL SECURITY
ORGANIZATION OF INFORMATION SECURITY	SECURITY COMPLIANCE



PALADION
HIGH SPEED CYBER DEFENSE

Implementation Approach

The 5 Steps towards ISO 27001 certification

PHASE 1

Define Scope and Perform Risk Assessment

PHASE 2

Security Framework Development

PHASE 3

Implement ISMS

PHASE 4

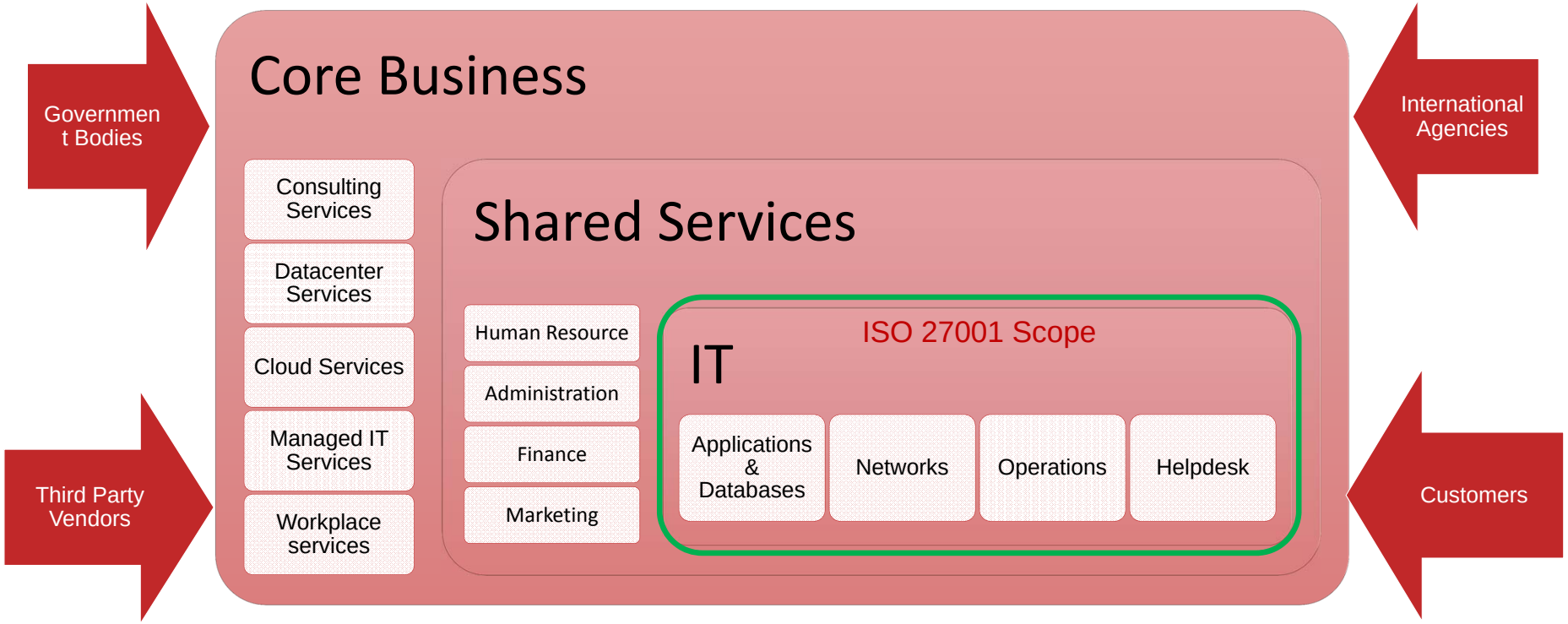
Certification

PHASE 5

Sustaining Compliance

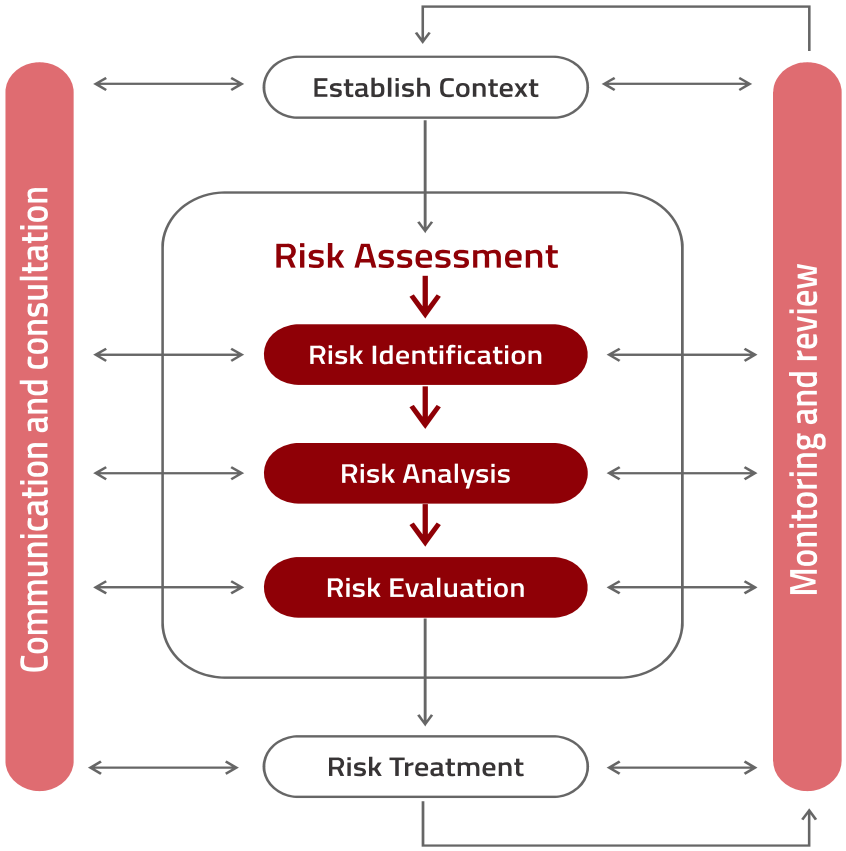
PHASE 1

Scope Definition



PHASE 1

Perform Risk Assessment



PHASE 2

Develop ISMS framework

- Plan and establish the ISMS
- Evaluate risks and security maturity
- Develop and Implement Controls
- Check the effectiveness of Controls
- Implement corrective actions

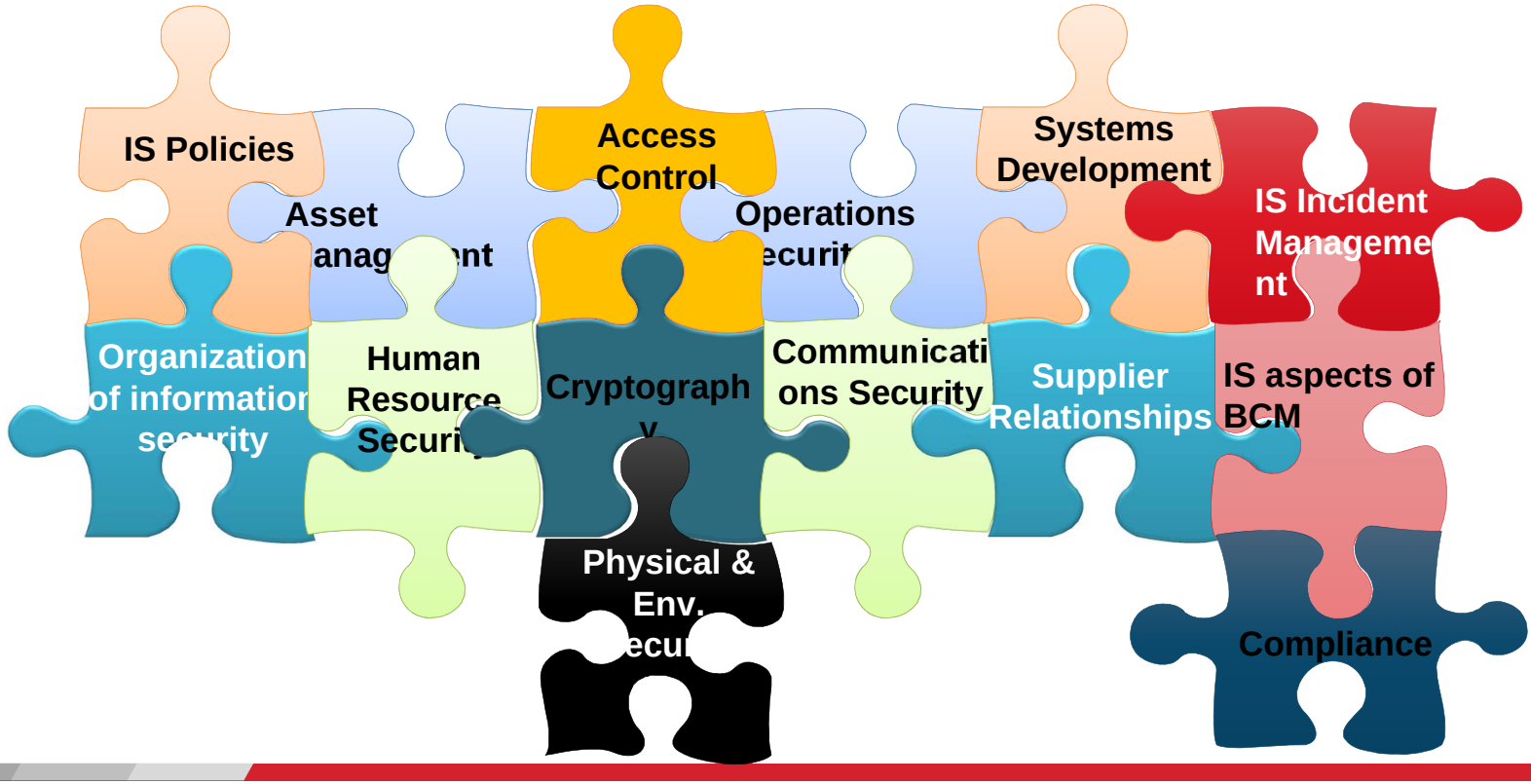
ISO 27001 Mandatory Clauses

4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

PHASE 3

Implement ISMS

- ISO 27001:2013 specifies 14 control objectives broken into 114 IS controls that organizations can deploy based upon acceptable risk posture and statement of applicability to the standard.



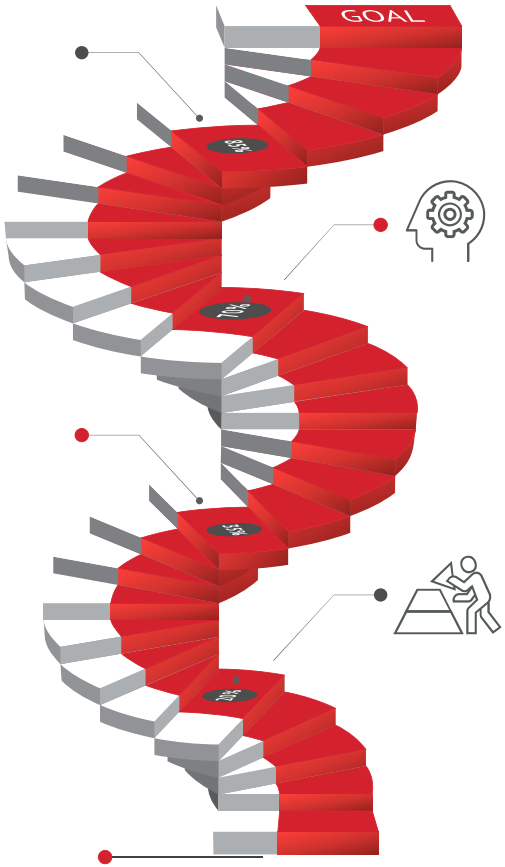
PHASE 4

Certification

Certification Audit

Internal Audit Reporting

Internal Audit Planning



Internal Audit Tracking and Closure

Internal Audit Execution

PHASE 4

Certification

Year 1 – Certification

Stage 1 – Readiness Review

Stage 2 – Implementation Audit

Year 2 – Surveillance 1

Year 3 – Surveillance 2

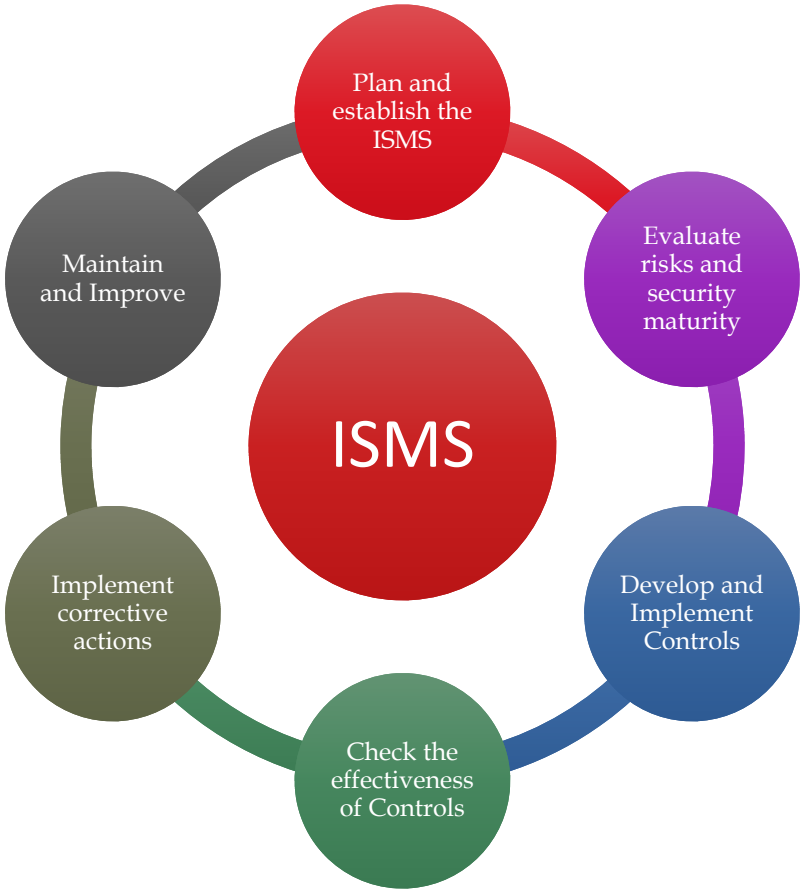
Year 4 - Recertification

Repeat

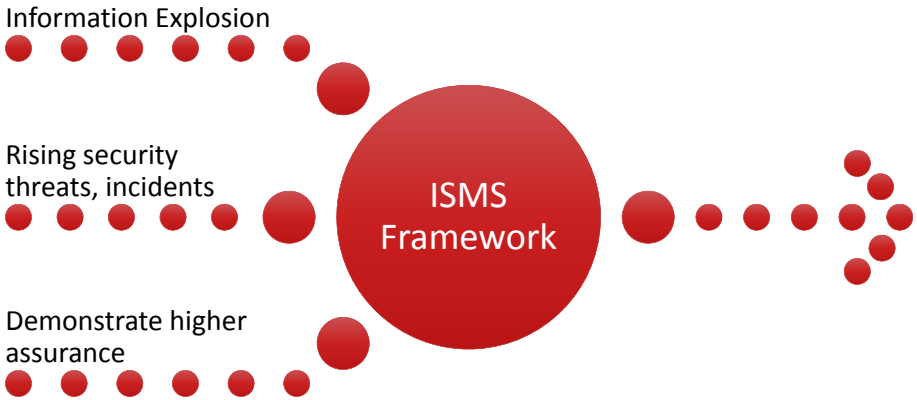
PHASE 5

Sustaining compliance

- Validation is one point in time but your compliance efforts are ongoing
  - Plan and schedule ongoing activities
  - Regular compliance check and reports
- Ensure management buy-in and commitment is visible
  - Monthly review meetings
  - Mails and reminders



Benefits of ISO 27001



Classified data. Multi-tiered security controls focusing on CIA triad.

Frameworks includes people, process and technology

Certifiable standard. Applies risk management process. Derives effective metrics.

Resources

- Learn more about the standard
  https://www.dekra.us/en/system-certification/iso-27001/
- ISMS for Cloud service providers – e-Guide
  http://www.paladion.net/isms_for_cloud_service_providers/
- What to look for in a Managed GRC vendor – Blog
  http://www.paladion.net/managed-grc-vendor/

PALADION
HIGH SPEED CYBER DEFENSE

Questions?

PALADION
HIGH SPEED CYBER DEFENSE

Thank You!