Quality Control – Using Quality Assurance Methods to bring your Firm to the Next Level

"ISO-27001 for Law Firms - Is it right for your firm?"

S.S. RANA & CO.
ADVOCATES
AN ISO 27001:2013 CERTIFIED LAW FIRM
www.ssrana.in

Vikrant Rana
Managing Partner,
S.S. Rana & Co.
INDIA

Today's Agenda

1) What is ISO 9001?
2) What is ISO-27001? Why are you hearing so much about it?
3) What problems does it solve? Other benefits?
4) What does the process look like?
5) How much ? How fast ? How painful?
6) Why is it relevant to the Legal Vertical?

ISO 9000

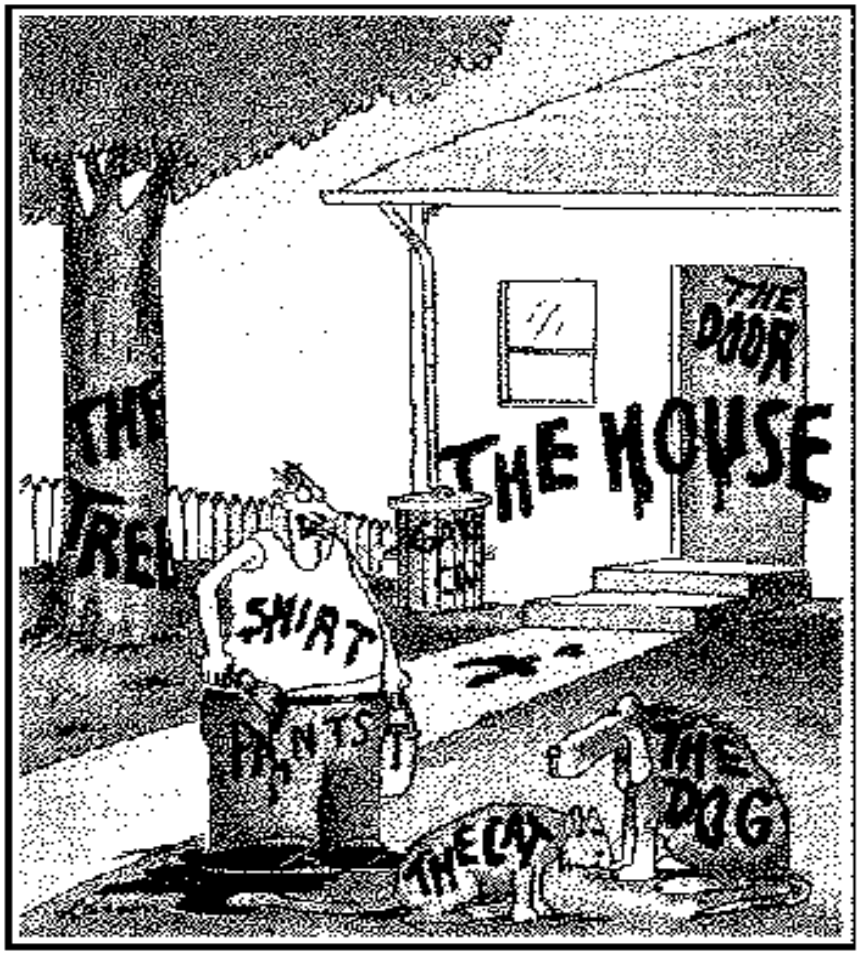
- The **ISO 9000** family of quality management system (QMS) standards is designed to help organizations ensure that they meet the needs of customers and other stakeholders while meeting statutory and regulatory requirements related to a product.
- ISO 9000 deals with the fundamentals of quality management systems, including the eight management principles upon which the family of standards is based.
- ISO 9001 deals with the requirements that organizations wishing to meet the standard must fulfill.

ISO 9001 ? ISO 27001?

- 27001 talks about security of information and data whereas 9001 provides framework for quality of products and services.
- 27001 is about building controls for Confidentiality, Integrity and Availability of information whereas 9001 helps to build policy at individual department level.
- 27001 talks about Information Technology whereas 9001 it does not focus on this.
- 27001 is more oriented towards IT related assets whereas 9001 is for entire business.

Quick Clarification

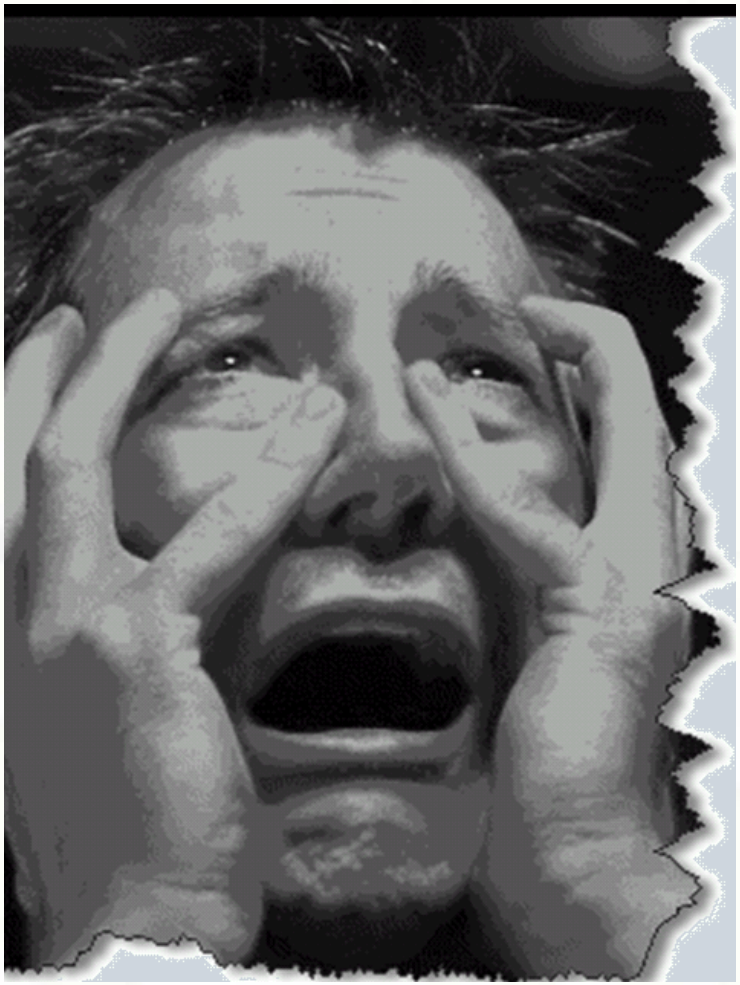
- ISO-27000 is a “series” of information security standards
- ISO-27001 “uses” ISO-27002



"Now! ... That should clear up a few things around here!"

Should we be thinking about 27001?

- ***How Bad is Your Pain?***
- We need to prove to many of our clients that we are “secure”
- We need to prove that many of our service providers keep our data secure
- We need to prove we are compliant with different regulations/standards
- We are struggling with regards to Information Security
- To take us to the next level



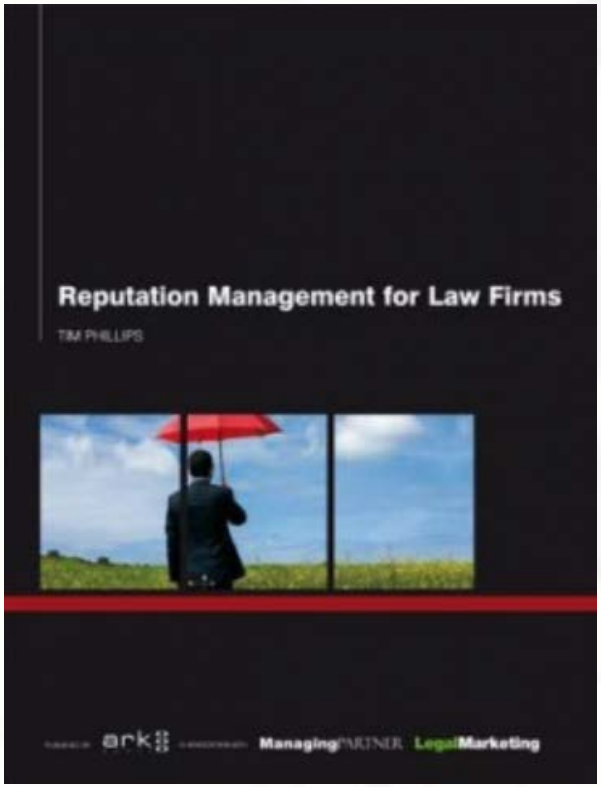
ISO Myths

- It is just a bunch of documents.
- It requires a huge investment in technology.
- It is only applicable to ‘big law’.
- It is something we can just pass off to our security manager.

Pain of a Law Firm is *(similar but)* Different

- Highly diverse levels of very sensitive data in a single firm
  - Diverse Client/Vendor Risk Management (VRM) practices
- National/International Client Base
  - International attestation
  - PII Data Protection laws (EU-DPA, 46 State PII, PIPEDA)
- Partner Model can be divergent with Fortune - 500 security requirements
- “Brand” is a priority

Pain of a Law Firm is *(similar but)* Different



Reputational Damage Is the Lingering Data Breach Injury

Organizations need incident response plans in place to mitigate harm to their brand and keep their customers.

By Judy Selby | **Contact** | **All Articles**

Law Technology News | November 21, 2013

Companies Asking for ISO-27001 Certification

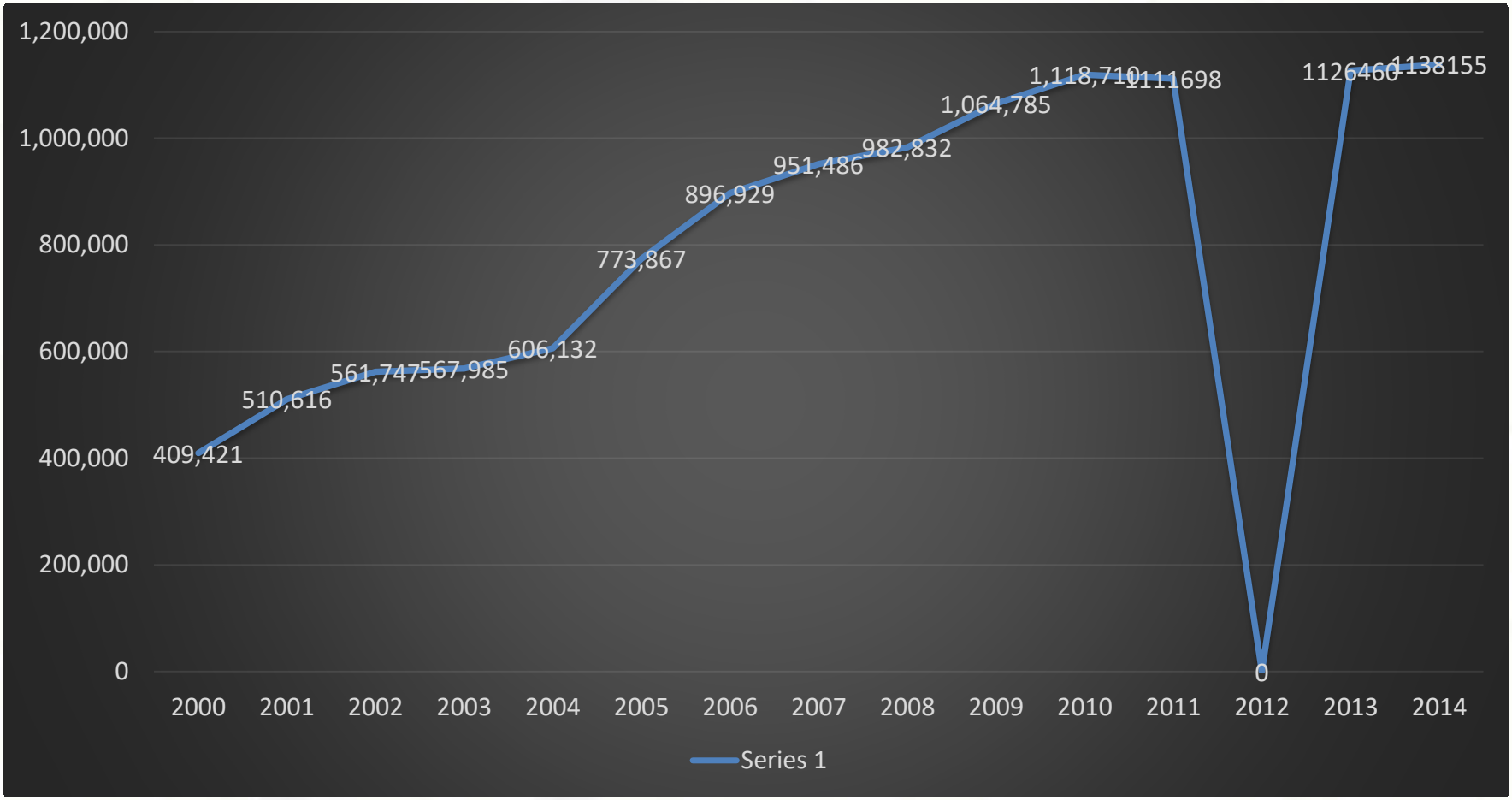
Growth of ISO-27001 Certifications

Top 10 countries for ISO certificates till the year 2013

Rank	Country	No. of Certificates
1	China	297,037
2	Italy	138,892
3	Russian Federation	62,265
4	Spain	59,854
5	Japan	59,287
6	Germany	50,583
7	United Kingdom	44,849
8	United States	25,101
9	Republic of Korea	24,778
10	India	22,349

Source: The ISO Survey of Management System Standard Certifications, 2013.

Worldwide total of ISO 9001 certificates (end of each year)



Source: The ISO Survey of Management System Standard Certifications – 2000-2014.

Note: The rapid drop in the graph for the year 2012 is because of lack of availability of data.

Law Firm Cyber Security Pain: Targeted Attacks

China-Based Hackers Target Law Firms to Get Secret Deal Data

By Michael A. Riley & Sophia Pearson - Jan 31, 2012 4:37 PM ET

China-based hackers looking to derail the $40 billion acquisition of the world's largest potash producer by an Australian mining giant zeroed in on the Canadian law firms handling the deal.

Mary Galligan, head of FBI's NYC cyber division convened a meeting with the top 200 law firms in New York City last November to deal with the rising number of law firm intrusions.

Panama Papers

- The Panama Papers are 11.5 million leaked documents that detail financial and attorney–client information for more than 214,488 offshore entities.

- The leaked documents were created by Panamanian law firm and corporate service provider Mossack Fonseca; some date back to the 1970s.
- The company informed clients on 3 April 2016, that files had been obtained through a hack of the company's email server. *Forbes* has suggested that the firm's information security was poor, running old versions of key tools, and other vulnerabilities.

Law Firm Operational Pain: Mobility & BYOD

Attacking the Weakest in the Law Firm Culture

Posted: 09/10/2013 5:40 pm

Read more > Technology News

Law Firm Pain: Desired (& un-desired) Use

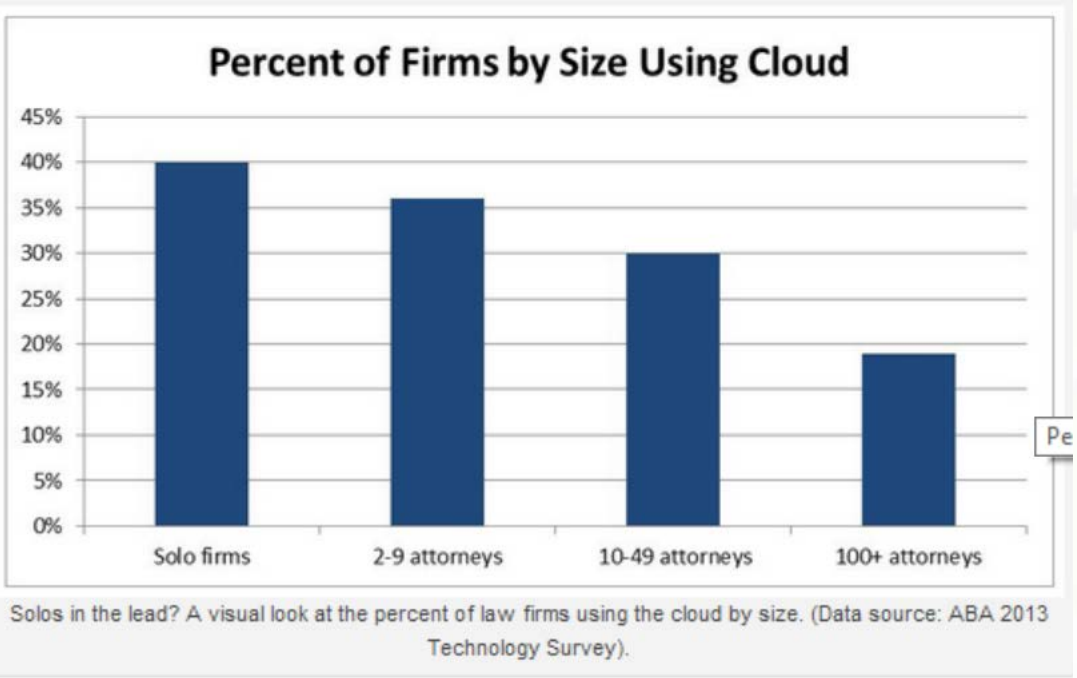
Microsoft® Office 365

Gmail by Google

EVERNOTE

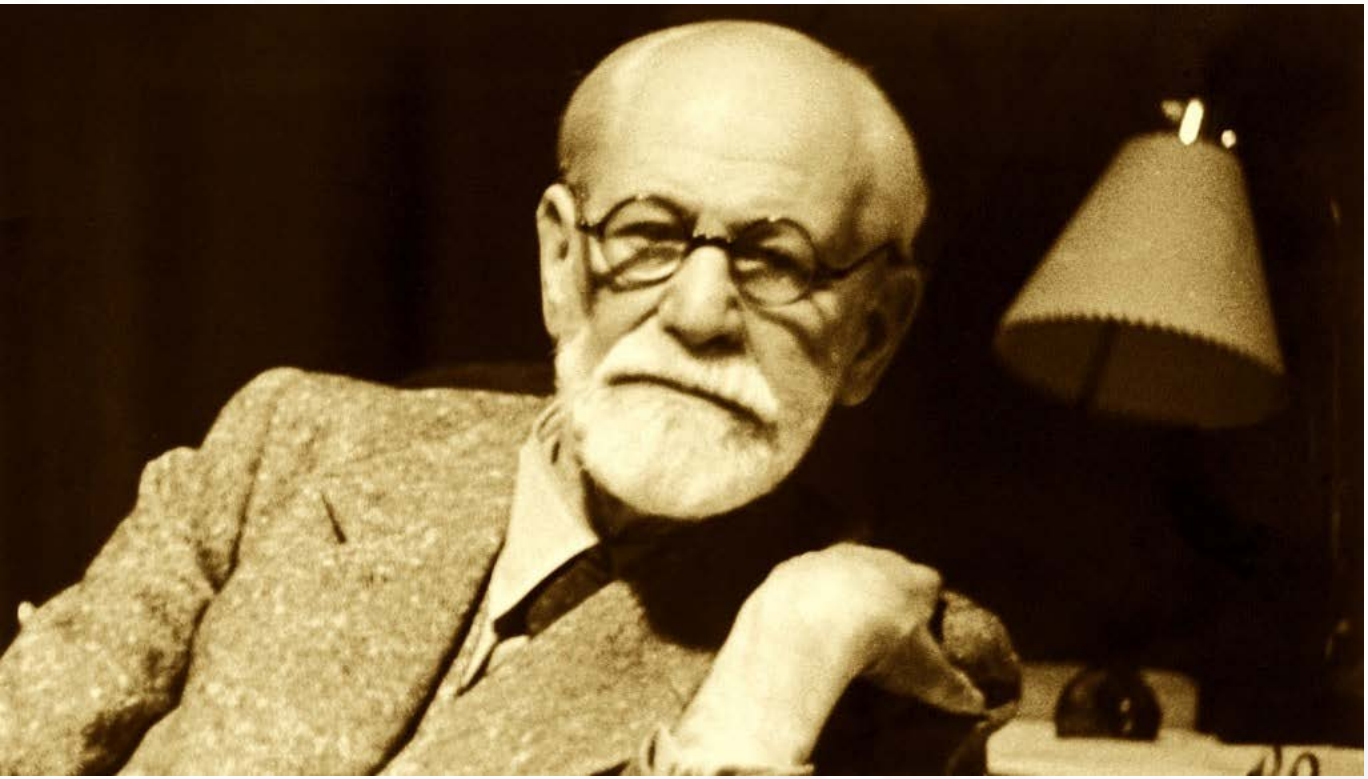
box

Dropbox



Solos in the lead? A visual look at the percent of law firms using the cloud by size. (Data source: ABA 2013 Technology Survey).

Good News: Freud would have liked 27001



In Freudian psychology, people seek pleasure and avoid pain …

A Competitive Differentiator *(for now)*

Allen & Overy gets cyber seal of approval in the U.S. for information security

27 January 2012

Firm stays ahead of competitors on information security with prestigious certification in the U.S., having already achieved it in Europe.

Allen & Overy announced today that it has received the prestigious ISO 27001 certification for the way it protects confidential information on its computer systems. The certification comes after a rigorous assessment by a certified examination body.

Allen & Overy achieved this highly sought-after mark of excellence in London three years ago – the first major law firm to do so – and it was later extended to include the firm's offices across Europe in 2011 and now the U.S. in 2012.

Allen & Overy's Chief Information Officer Gareth Ash said, "We are leading the pack on information security. This certification provides real business benefits when working with our clients and future clients, especially within the financial industry."

SO, HOW DO WE OVERCOME THESE PROBLEMS?

Features of ISO 27001

- Plan, Do, Check, Act (PDCA) Process Model
- Process Based Approach
- Stress on Continual Process Improvements
- Scope covers Information Security not only IT Security
- Covers People, Process and Technology
- 5600 plus organizations worldwide have been certified
- 11 Domains, 39 Control objectives, 133 controls

ISO 27001 Standard

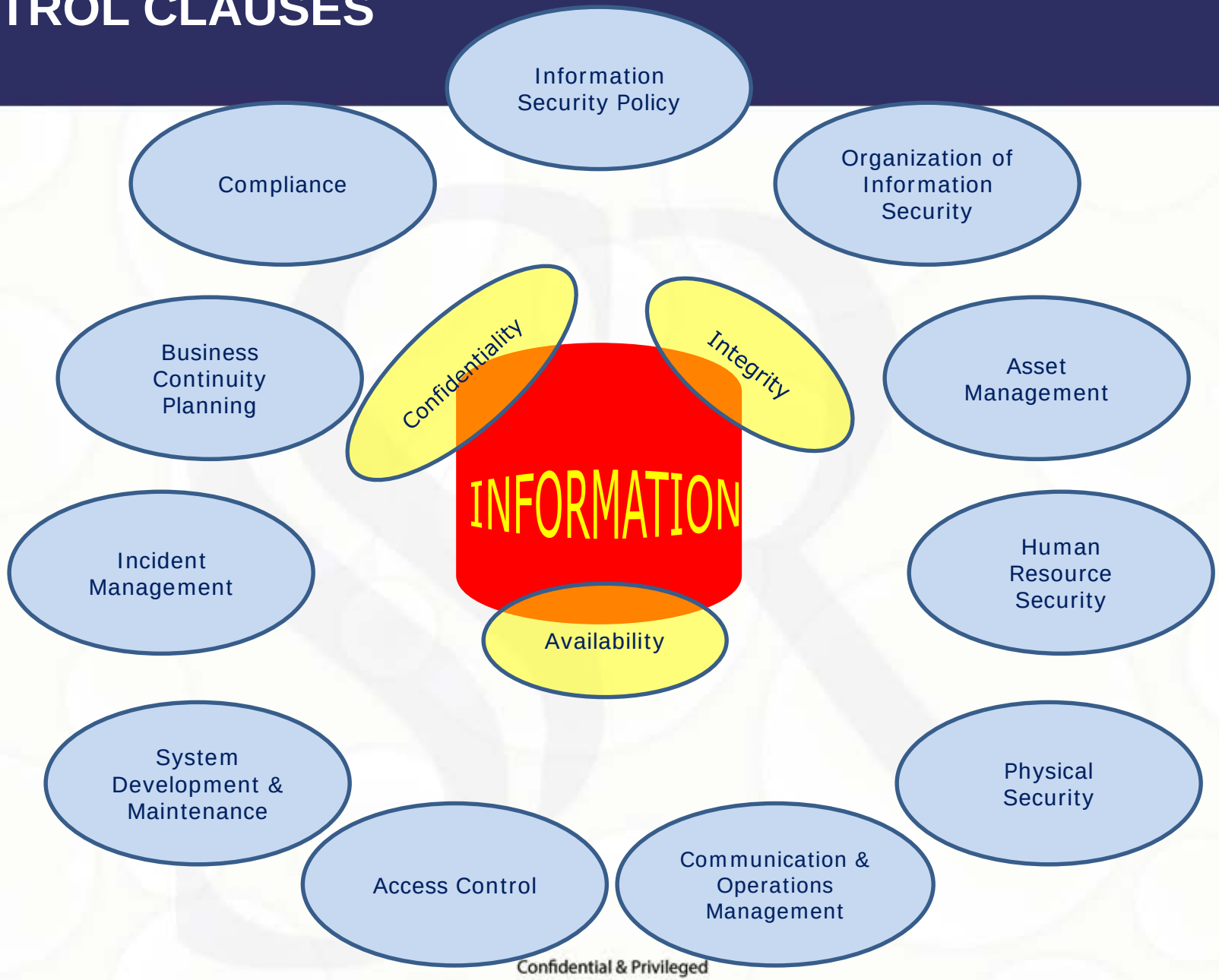
ISO 27001: This International Standard covers all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations). This

International Standard specifies the requirements for establishing; implementing, operating, monitoring, reviewing, maintaining and improving documented ISMS within the context of the organization's overall business risks.

It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

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

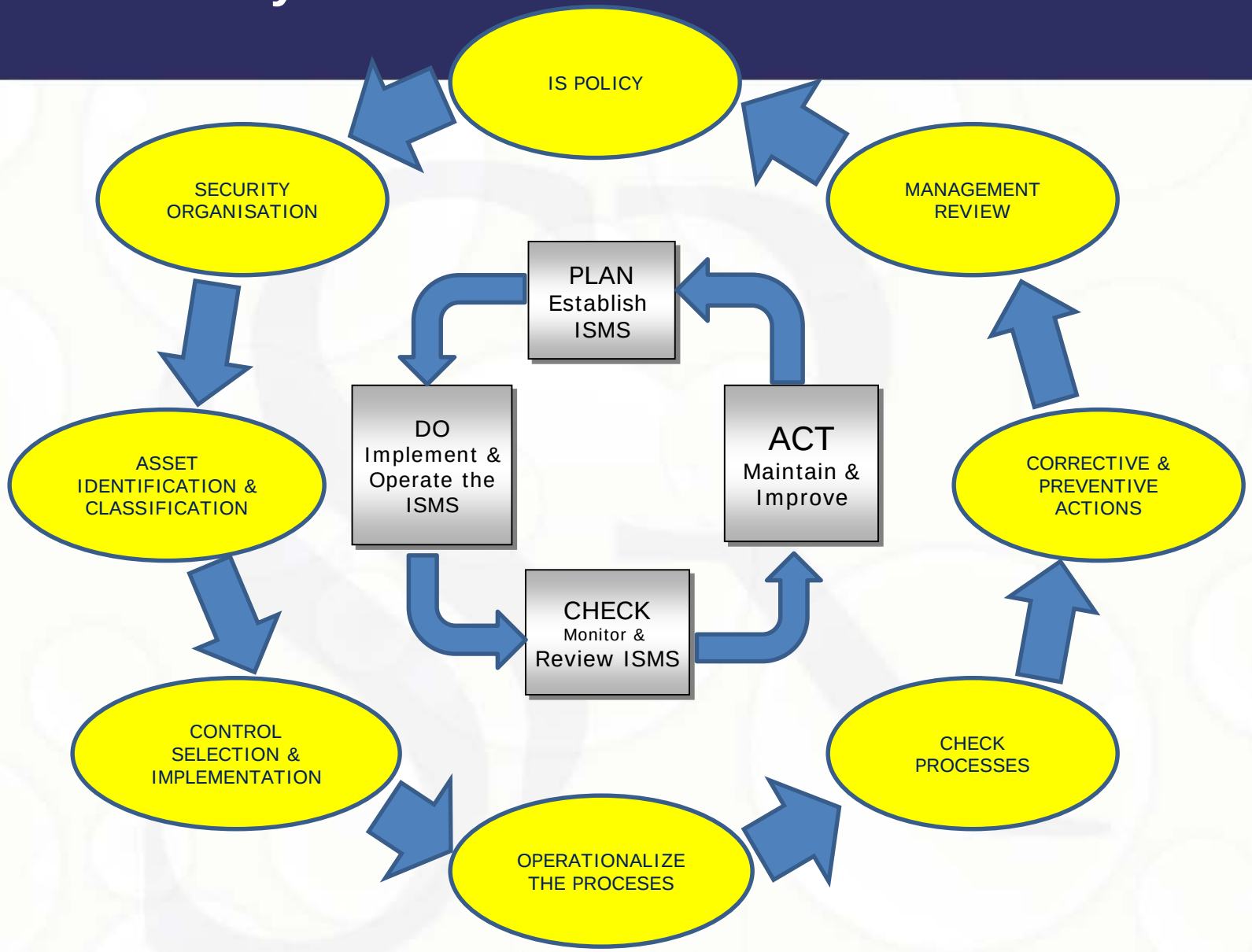
CONTROL CLAUSES



Summary

- Information Security Management System is part of the overall management system, based on business risk approach to establish, operate, monitor, review, maintain and improve information security.
- Information security protects information from a wide range of threats to ensure business continuity, minimize damage and maximize return on investment and business opportunities

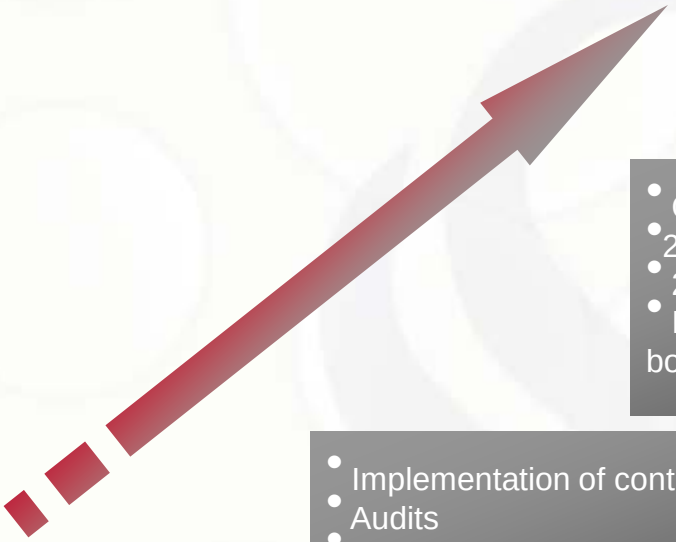
Implementation Cycle



Benefits of Implementing ISMS

- At the organizational level – Commitment
- At the legal level – Compliance
- At the operating level - Risk management
- At the commercial level - Credibility and confidence
- At the financial level - Reduced costs
- At the human level - Improved employee awareness

ISMS Roadmap



- Closure of gaps/non--compliances
- 3rd cycle of audit
- 3 cycle of review
- Readiness for pre-audit

Phase 4 (2 months)

- Closure of gaps
- 2nd Audit cycle
- 2 Management Review
- Identification of Certification body

Phase 3 (2months)

- Implementation of controls
- Audits
- Management Reviews
- Risk Assessment
- BCP/DRP

Phase 2 (2 months)

- Security council Formation
- High level policy definition
- Documentation of procedures, policies
- Intro to 27K training
- Identification of Assets and classification

Phase 1 (2 months)

In 3 months
Policy formulation
ISMS launch
Controls implementation
In next 3 months
Audit Cycle
Management Reviews
Continual improvements

Roadmap for Implementation

ISMS policy formulation at company level

Documentation of policies, procedures for

- HR
- IT
- Admin
- Finance
- Software

Identification of Assets and Classification

Application of Controls

Risk Assessment

Audits

Management Reviews

Our Journey

Reasons for our choice

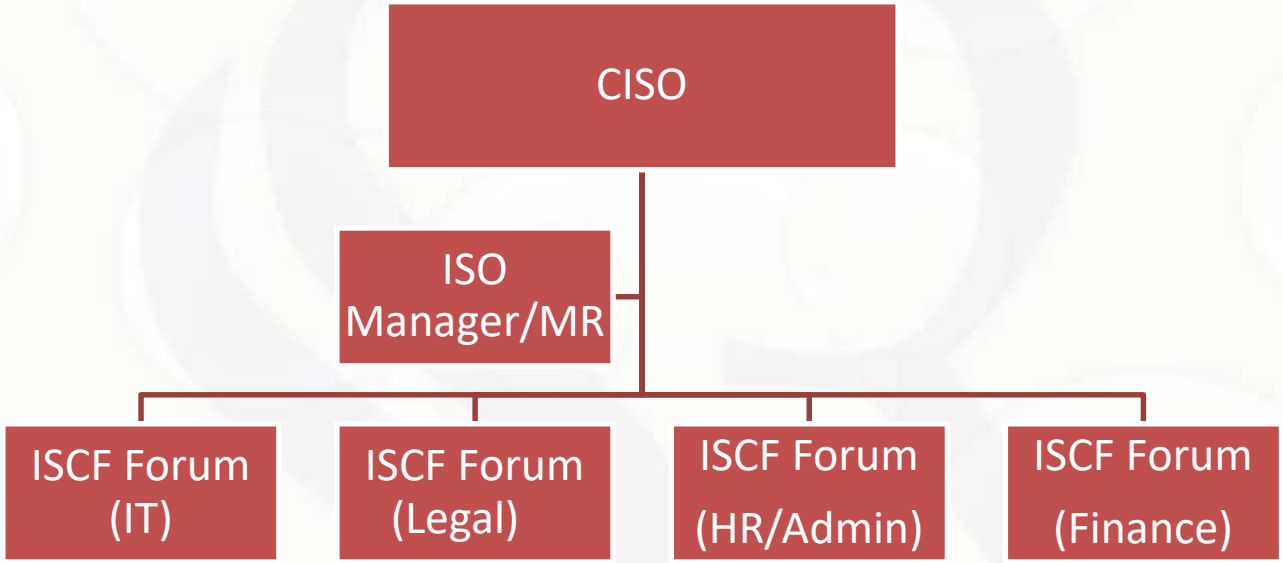
- General Data Protection Management
- Family concern – to a – Professional Structure
- Corollary to the above - Person Driven – to a – Process Driven
- To embrace global technological advances & go to the next level with Information Technology
- Business continuity & Disaster Recovery Plan
- Integrating technology with law

- We mapped out the main stages of the project that we would need to follow to reach our goal, the main ones being –
  - Initial Planning & Documentation
  - Training & Awareness
  - Setting the Scope
  - Critical Path
  - Gap Analysis
  - Risk Assessment Report & Treatment Plan
  - Statement of Applicability
  - Policies & Procedures Documentation
  - Certification Audit
  - Monthly Internal Audits & Annual Certification Compliance Audits

Initial Training

- Setting up an Internal Project Team.
- An ISMS Steering Committee was formed.

CISO – Chief Information Security Officer
ISCF - Information Security Co-ordination Forum
MR – Management Representative



- Attended a two day training session.
- The training session also gave the Project Team a valuable insight in exactly what was involved and also the amount of work required to achieve our goal.

Setting the Scope

- The ISO27001 Standard is often implemented for a part of an organization e.g. the IT Department or Software Development Department.

- But, we wanted more.

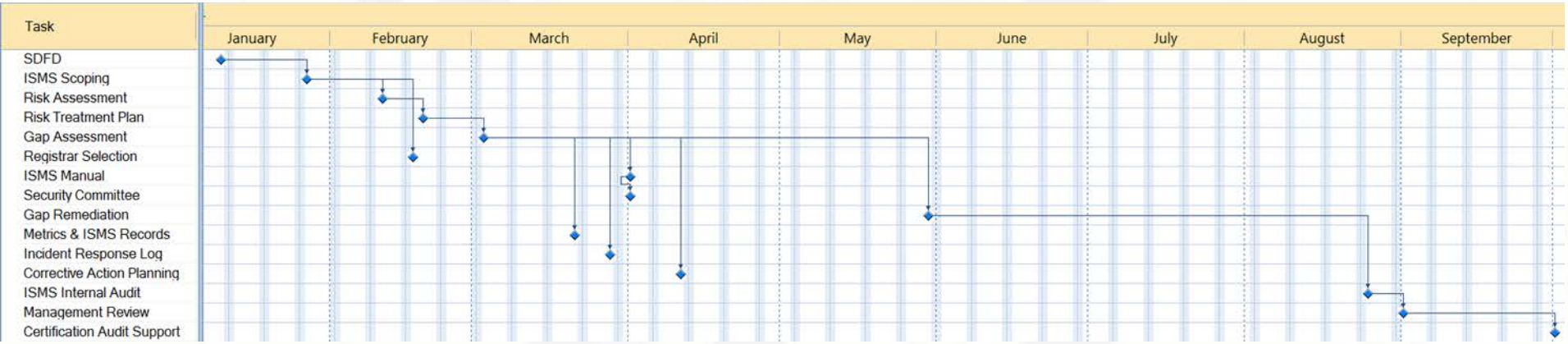
- We considered whether we could apply it to the whole organization and everything that we did. This approach was taken to give maximum assurance to clients.

Critical Path

- The training identified the key tasks & requirements.
- We mapped them out inserting key dates.
- We estimated that it would take approximately eighteen months to achieve Certification.

When: Typical Timeline?

4 – 18 months dependent upon Scope, Gap, Resource Availability, ISMS Expertise, Budget, Client Demand, & Willingness



Gap Analysis

- Before we could proceed any further we needed to know exactly how our existing controls, policies and procedures measured up to the Standard.
- Our external auditor performed a gap analysis for us and pointed us in the direction we needed to go.
- We received excellent guidance on the requirements and modified our plan accordingly.

ISMS Documentation

Risk Assessment Report & Treatment Plan

- We initially identified and categorized all of our Information Assets and General Assets.
- We then formulated a risk methodology.
- It was imperative that the risk methodology could be applied to each vulnerability, threat and risk on a consistent basis.
- Each information asset that we had identified was logged in the spreadsheet and a risk assessment was carried out considering vulnerabilities, threats, and the likelihood of it arising and how each risk should be treated.

Measurement & Monitoring

- **Top Measurements for monitoring**

  - No of NCs per department - Target (< 3)
  - No of Incidents reported - Target (<10% of previous month)
  - No of Opportunities identified – Target (> 1 per month)

  Monitoring on a monthly basis - MRMs

Difficulties experienced

- Taking the Examination to become a certified Auditor.

Difficulties experienced

- Preparing SOP's and guidelines for each & every department., as well as for each and every process.

Difficulties experienced

- Non-Compliance (NC) used as a mechanism to implement corrective actions – Unpopular amongst Employees at the beginning.

Difficulties experienced

- In general people are less receptive to change in their core areas of work.

Difficulties experienced

- Physical access restrictions by way of Access cards.

Difficulties experienced

- Difficulty in inculcating new habits in people.

What we learnt?

- Know where you are before you start and what the gap is that needs to be overcome to achieve Certification.
- ISO27001 will not just require a formal Information Security Management System it will also require additional formal documentation such as Office and IT Policies and Procedures.
- Ensure that every member of the organization has been bought into the project.
- The system is ever-evolving and must be updated regularly. We hold ISMS Committee Meetings every quarter.
- Develop a Risk Methodology that suits your organization and can be applied consistently.
- Develop an Information Classification Policy that suits your organization.
- When it comes to Information Security, the more you know, the more you don't know. The controls, policies and procedures that we had at the start of the Project have been completely overhauled and added to as areas of concerns were identified.

MANAGEMENT SYSTEM CERTIFICATE

Certificate No:	Initial certification date:	Valid:
181467-2015-AIS-IND-UKAS	02, July, 2015	02, July, 2015 - 01, July, 2018

This is to certify that the management system of

S.S. Rana & Co.

81/2, 2nd and 3rd Floor, Sri Aurobindo Marg, Adhchini, New Delhi - 110 017, India

has been found to conform to the Information Security Management System standard:
ISO/IEC 27001:2013

This certificate is valid for the following scope:
Provision of information security management system for providing services in the area of trademarks, patents, designs, copyrights, litigation, legal services in India & abroad and for support operations which include HR, admin, IT & accounts, the management of information in accordance with the statement of applicability, version no. 2.1 dated 31st March 2015

Place and date:
Chennai, 03, July, 2015

UKAS MANAGEMENT SYSTEMS
0013

For the issuing office:
DNV GL – Business Assurance
ROMA, No. 10, GST Road, Alandur, Chennai, PIN – 600 016, India

Shvadasan Madhyath
Management Representative

Lack of fulfilment of conditions as set out in the Certification Agreement may render this Certificate invalid.
ACCREDITED UNIT: DNV GL Business Assurance UK Limited, Palace House, 3 Cathedral Street, London SE19DE, United Kingdom.
TEL: +44(0) 207 357 6080. www.dnvba.com

Questions?