



Information Security & Management Systems



LRQA
Measure the Difference

Or would you rather like to know our views on relationships between professional Information Management and achieving Business objectives?

..... and how to improve!



LRQA
Measure the Difference



What drives Information Security?

- Regulators?
 - SOX, BASELL II, Personal Privacy Protection Acts?
- Certification Bodies / Auditors?
 - Annual reports, ISO certification?
- Company objectives?
 - Business continuity, clients, employees, suppliers?

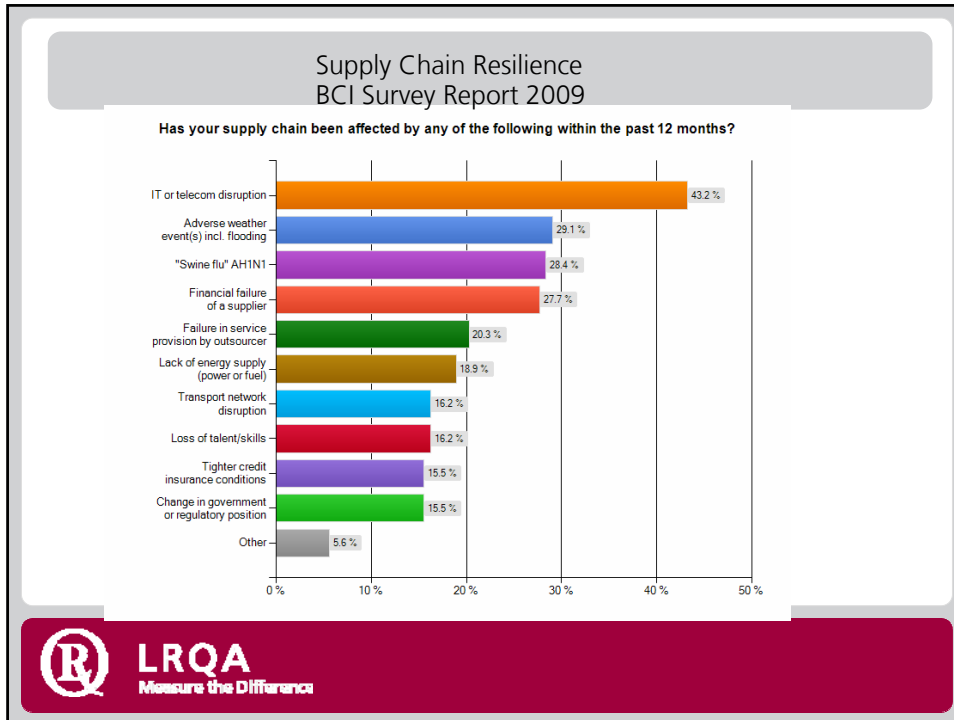


Importance of Information Management

- Information is a key asset of any company
- What if your information is NOT:
 - Confidential?
 - Integer?
 - Available?
- Supply Chain Performance is closely linked to Information "CIA"
- Dependency on IT systems increasing
- Yet - people do the job
- TAPA theft statistics – high level of "inside information"
- E-commerce

CIA

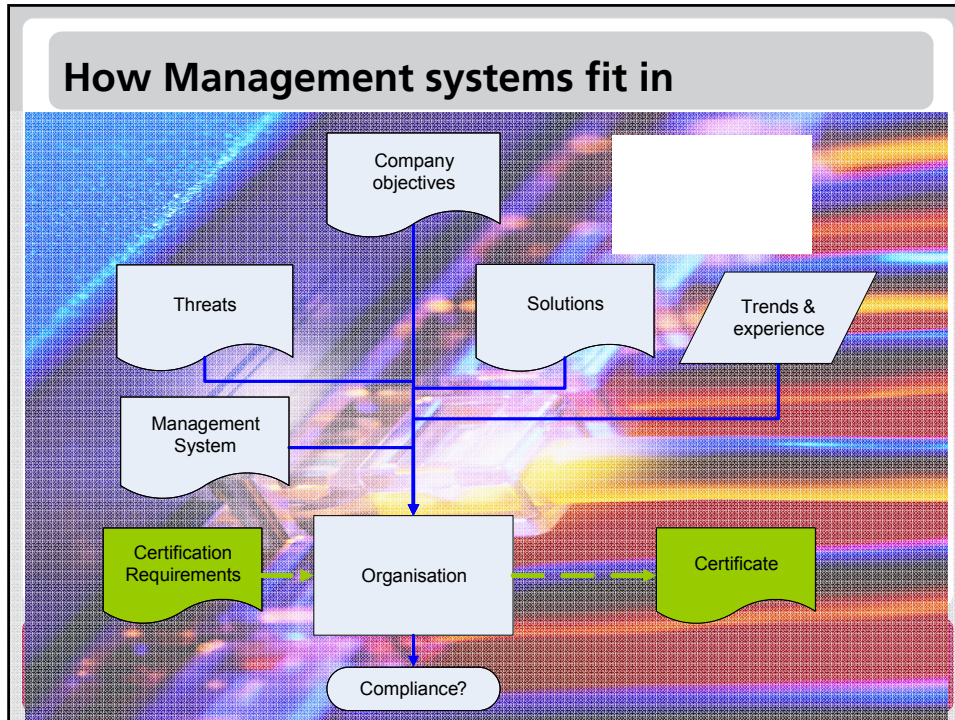




**BUY A COPY OF ISO 27001,
GET CERTIFIED
AND OFF YOU ARE.....**

LRQA
Measure the Difference

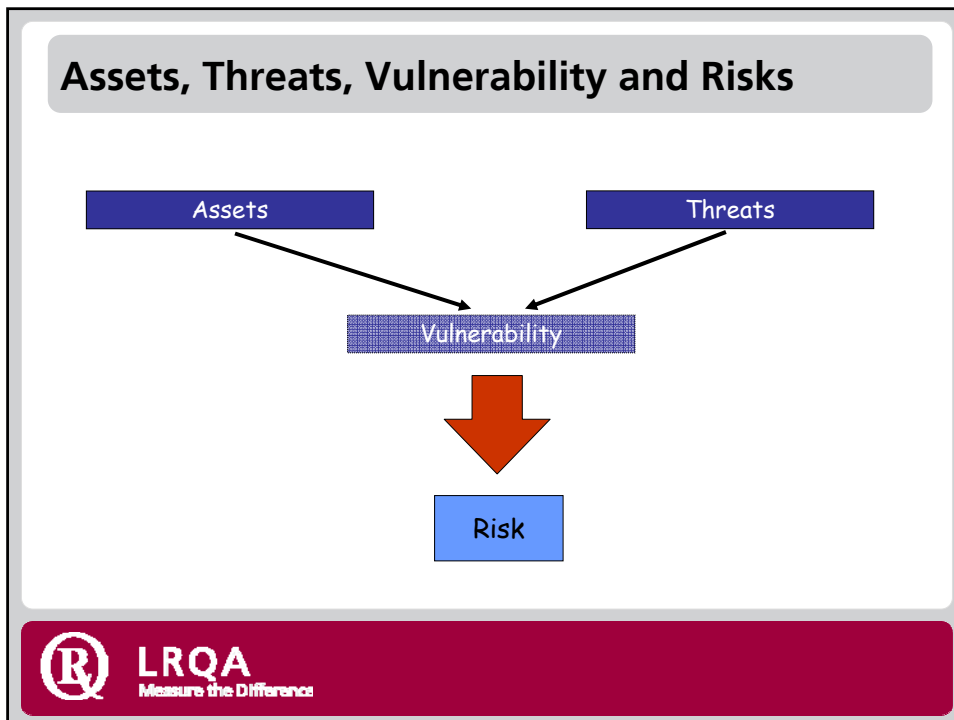
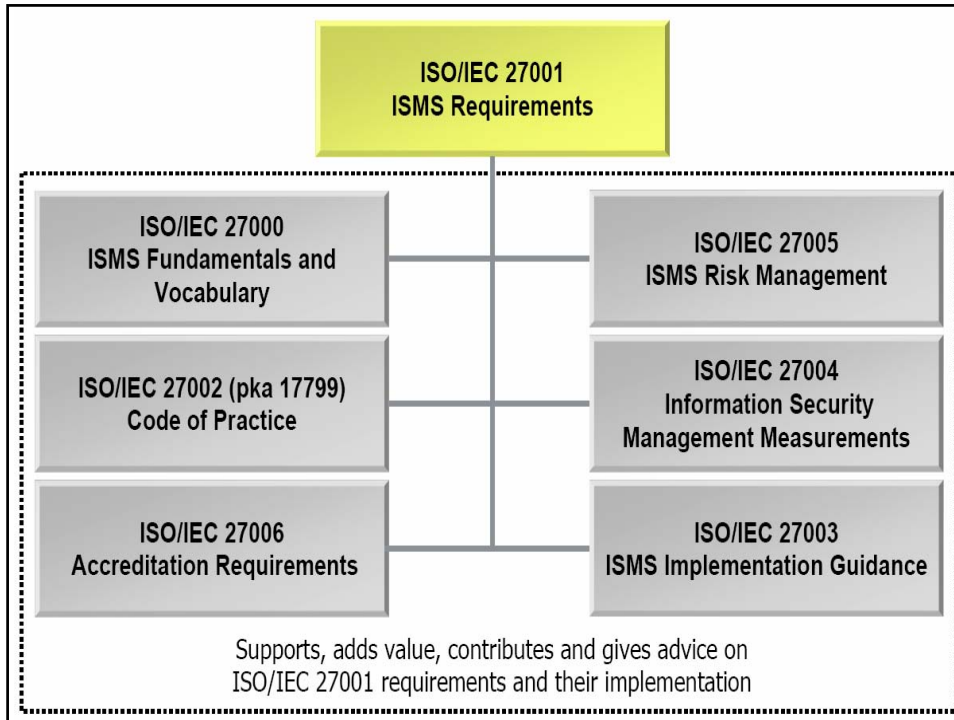




ISO 27000 will help you to stay in control

- Risk based
- Business oriented / adaptable
- 133 recommended controls
- Guidance documents available (27002 - 27005)
- Consistent with other corporate management systems
 - ✓ Quality (ISO 9001)
 - ✓ Environment (14001)
 - ✓ Health & safety (18001)
 - ✓ Business Continuity (25999)
 - ✓ Supply Chain Security (28000)
- Risk based

 **LRQA**
Measure the Difference





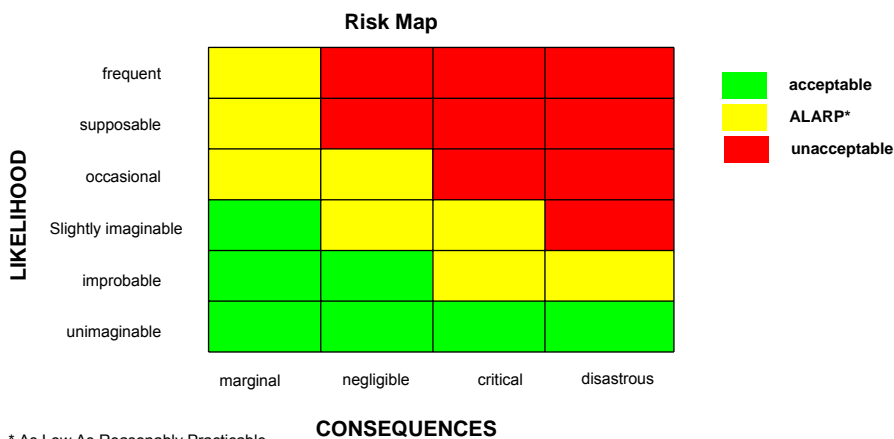
Assets, Threats, Vulnerability and Risks

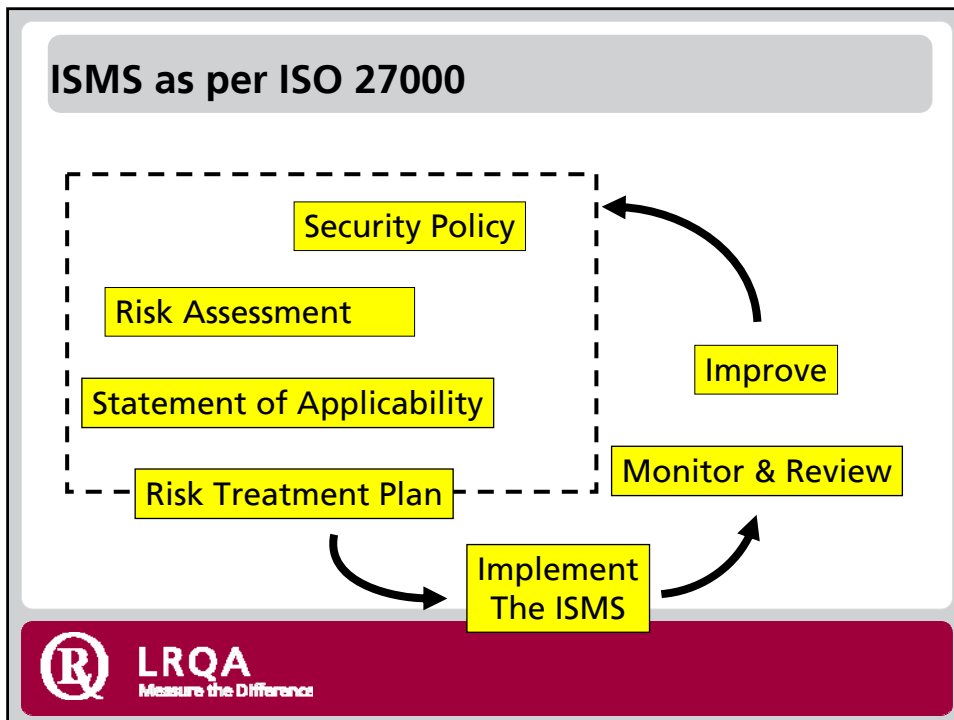
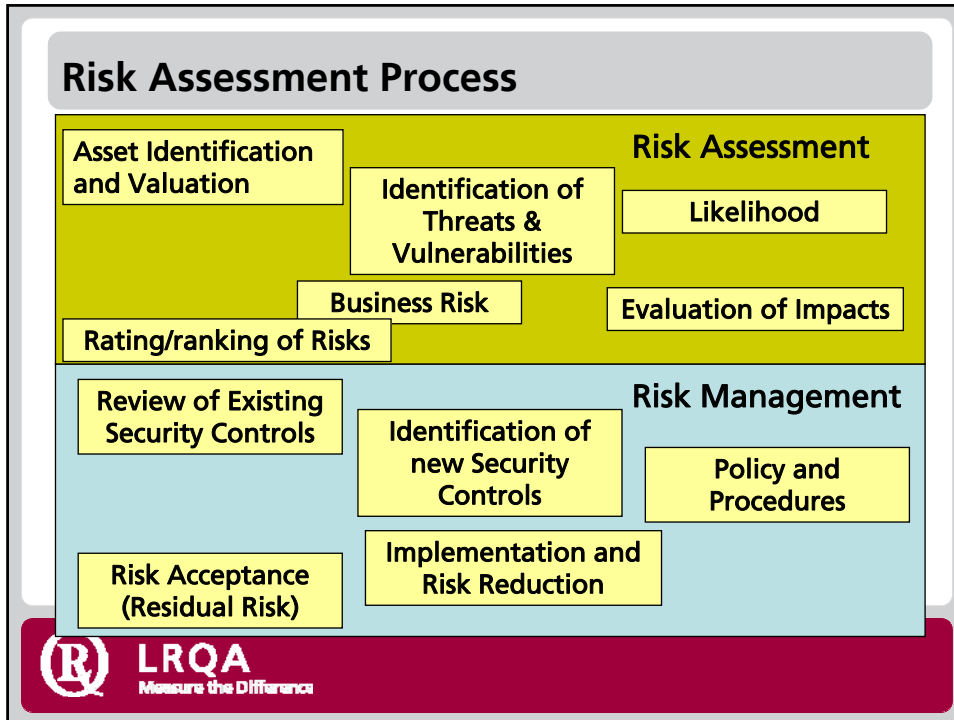
Assets
Threats
Vulnerability
Risks
Measures
Procedures
Implementation
Control

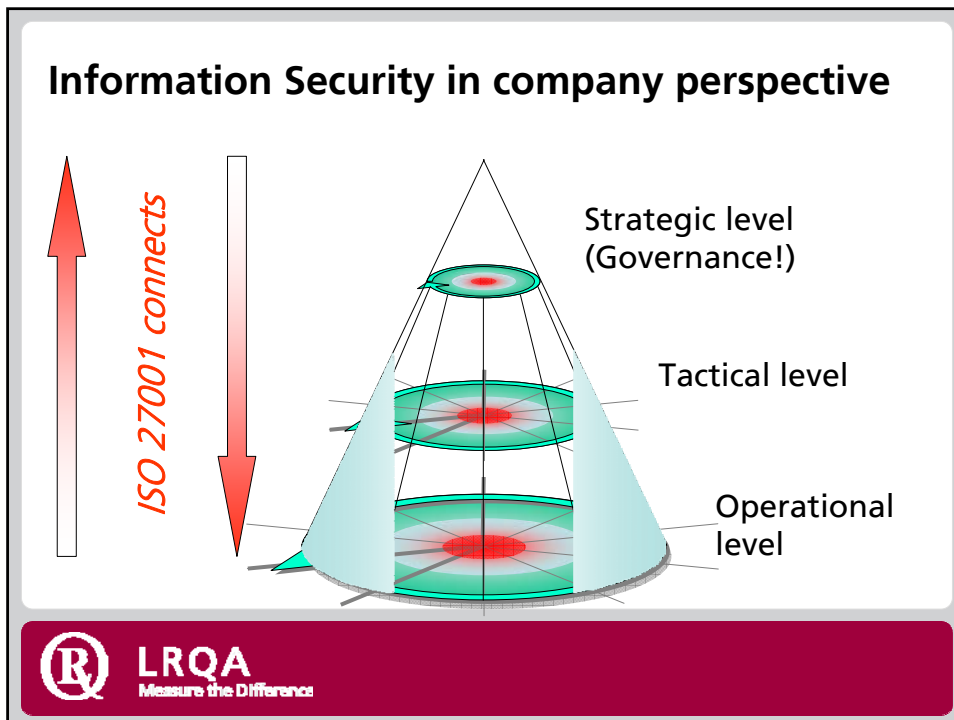
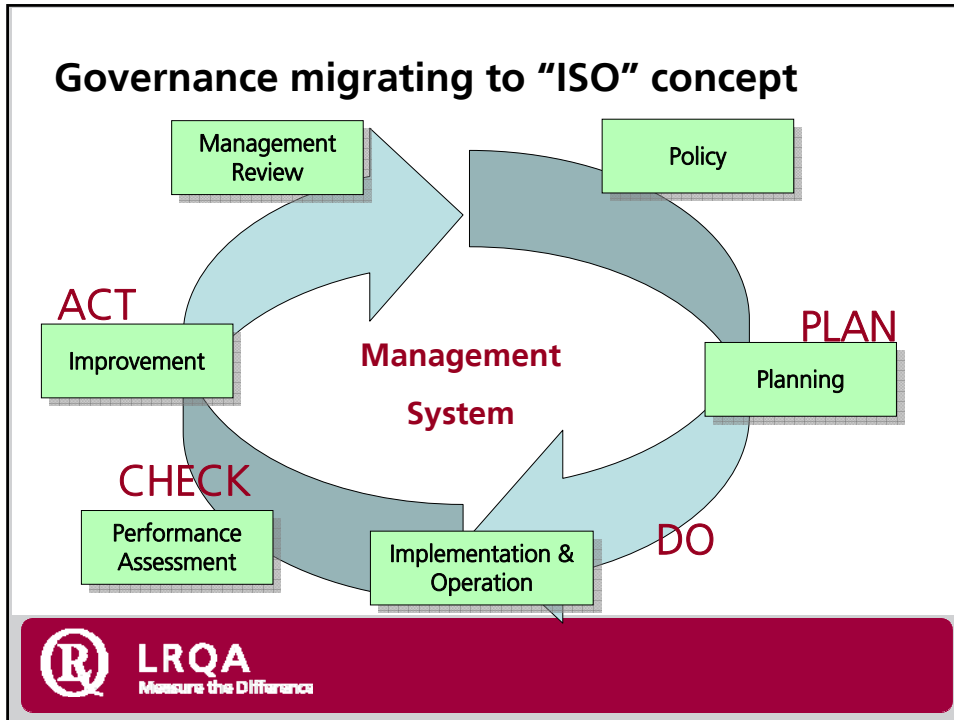
- Which assets do you want to protect?
- What could threaten your assets?
- Are your assets vulnerable to these threats?
- What are likelihood & impact of the threats?
- What are you going to do about the risks?
- How do you manage the selected measures?
- How do you make the measures work?
- How do you know it is effective?



Risk Management covers all corporate activities









ISMS – Operating best practice (ISO 27002)



Security is a prerequisite, not the objective!

**Stopping Flow of Information
is
Stopping your Business**





Performance Measurements

1. Management Controls

- Security & IT Policies, Procedures, Business Continuity Plans, Improvement Plans, Business Objectives, Management Reviews

2. Business Processes

- Risk Assessment & Risk Treatment Management Process, HR, SOA

3. Operational Controls

- Operational Procedures, Change Control, Incident, Release and Capacity Management, Back up, Disposal, Equipment off site etc

4. Technical Controls

- Information Access & Usage, authorisations, Firewalls, spyware etc.



Objectives of measuring performance

- Confidence for senior management and stakeholders
- Ongoing improvement
- Compliance
- Cost / benefits and ROI
- Effectiveness & appropriateness of implemented controls





Benefits of (certified) management system

- External proof
 - Stakeholders (clients, suppliers, investors, governments)
 - Senior management (Budgets!)
 - Employees (safe at work)
 - Insurance provider – policy conditions
- Forward looking (what is required x years down the road?)
- Reduction of (supply chain) disruptions, improved Business Continuity
- Motivates staff; common language
- Integration with other risk aspects (quality, environment, OHSAS)
- Audits (internal and external) focus on adequate risk management



Benefits of (certified) management system

- External proof
 - Stakeholders (clients, suppliers, investors, governments)
 - Senior management (Budgets!)
 - Employees (safe at work)
 - Insurance provider – policy conditions
- Forward looking (what is required x years down the road?)
- Reduction of (supply chain) disruptions, improved Business Continuity
- Motivates staff; common language
- Integration with other risk aspects (quality, environment, OHSAS)
- Audits (internal and external) focus on adequate risk management



Certification is only the start, not the end



Conclusions

- Compliance is not the finish but only the start
- Information Security is about people managing the organisation, not IT systems
- Internal audits, training & awareness are crucial elements
- Audit bodies can provide the experience and skills to support your business
- Certification is also our start into improvements
- Try and challenge us! We call it "Business Assurance"

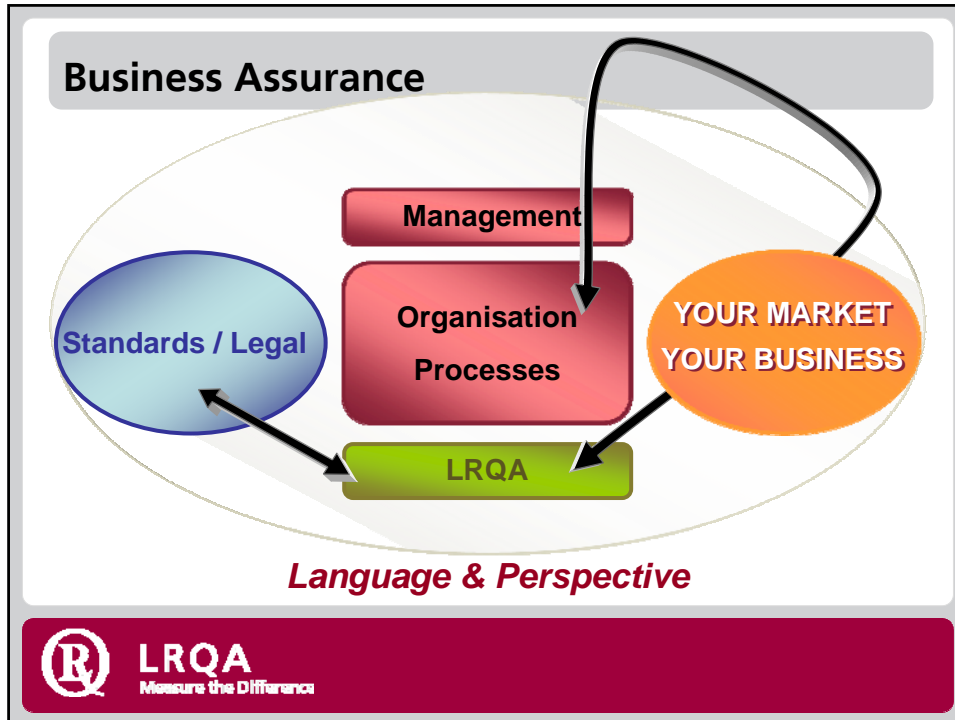


Conclusions

- Compliance is not the finish but only the start
- Information Security is about people managing the organisation, not IT systems
- Internal audits, training & awareness are crucial elements
- Audit bodies can provide the experience and skills to support your business
- Certification is also our start into improvements
- Try and challenge us! We call it "Business Assurance"

TALK MONEY





LRQA Contact details

Lloyd's Register Quality Assurance, EMEA

- **Ronald de Kok**
- E Ronald.dekok@lr.org
- M +31 620 709 149

