

## The SME pocket guide to achieving ISO/IEC 27001 certification

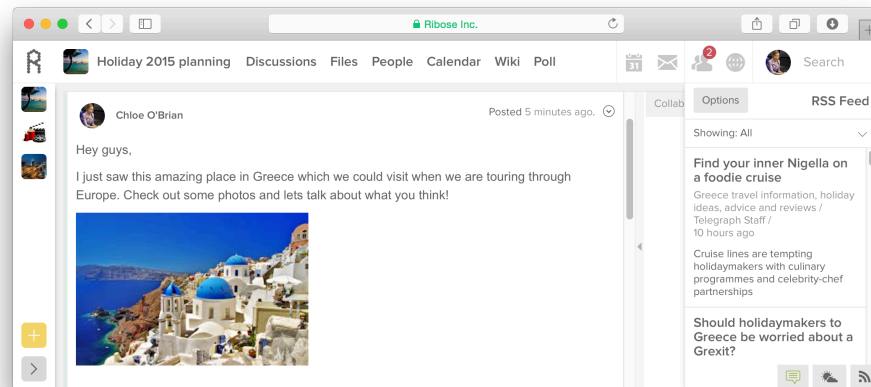
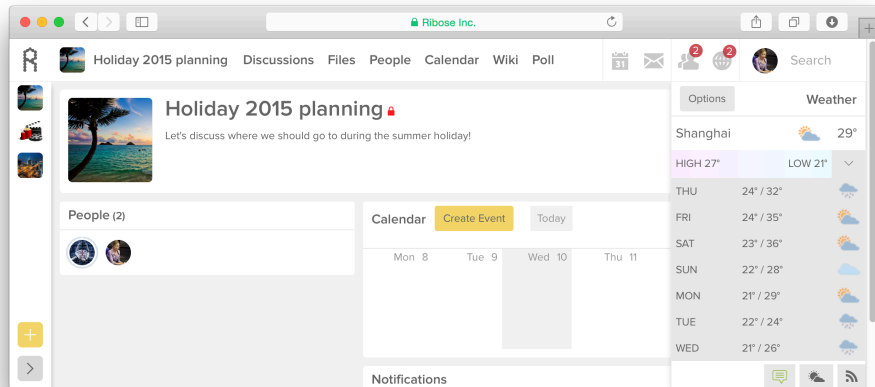
Workshop on ISO/IEC 27001 Information Security Management  
System Certification

Organized by HKCTC, HKAS and WGCSP (OGCIO)

Ronald Tse, founder of Ribose, HK Delegate to ISO/IEC JTC 1/SC 27  
2015/06/19



# RIBOSE IS A SECURE CLOUD COLLABORATION SERVICE



- Hong Kong home-grown startup
- Multiple “global firsts” in cloud security
- Highly-secure platform with top-level ratings:
  - CSA STAR Attestation, STAR Gold Certification (highest security maturity rating), C-STAR
  - Singapore MTCS Level 3 (Mission-critical, highly-confidential)

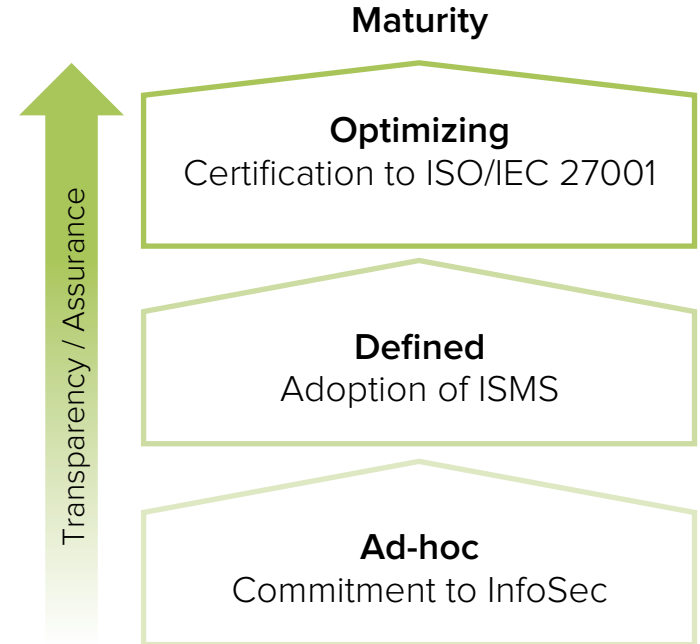


# WE ARE HERE TO SHARE SOME TIPS FOR YOUR CERTIFICATION JOURNEY

- Embarked on ISMS certification for user trust
- Previously certified to ISO/IEC 27001:2005
- Hong Kong's first to achieve ISO/IEC 27001:2013 certification (by an accredited certification body, of course)
- We believe:
  - international management system standards (MSSs) help improve core competency
  - certified assurance is key to trust between the user and the provider
- Gone through certification processes many, many times
- And... we're an SME!
  - a small one  $\leq 10$  FTEs
  - Big names say: "we are ACME therefore your data is secure"
  - SMEs can say: "we are independently certified for ISO/IEC 27001!"

# THE ELEPHANT IN THE ROOM ASKS: WHY, WHY AND WHY?

- Why do we care about information security?
  - Protect customers and trade secrets
  - Guard against information risks
  - Good for business
- Why do we need an ISMS?
  - Systematic manner to manage information risks
  - International best practices: if you're doing it anyway, better to do it right
  - Byproducts: increase transparency and efficiency
- Why do we certify?
  - Measureable, verifiable, then improvable
  - Competitive advantage, e.g., contract bids



# MYTH BUSTED: INFORMATION SECURITY MANAGEMENT APPLIES TO ALL ORGANIZATIONS WITH INFORMATION RISKS

- Information risks: you have valuable information assets
- Information security risks are organizational threats
- ISO/IEC 27001 applies to all industries and all sizes: not only for IT companies!
- ISMS is a systematic approach to managing information risks
- Obviously, some industries benefit more from an ISMS

## Attributes ISMS excels in managing

Data integrity  
Intellectual property  
Privacy / Customer data  
Business continuity

## These industries benefit especially from certified security assurance

Biotech / Pharmaceuticals / Medical  
Entertainment / Fashion / Media  
Engineering / Manufacturing  
Legal / Consulting

# STANDARDS ARE \*GOOD\* FOR SMES: NOT ONLY CAN WE DO IT, WE BENEFIT MORE FROM IT

A lot of people think standards are just for large companies because they are complex, expensive tools. Nothing could be further from the truth.

Howard Kerr, Chief Executive of BSI (British Standards Institution), the originator of ISO/IEC 27001

## MYTHS

- Larger organizations:
  - have more money and time – we are focused on sustaining and growing our business
  - need to do it – no one asked us
  - know how to do it – we don't

## FACTS

- Discover value of security from risk assessments, ROI<sup>[1][2]</sup>
- Materialization of information risks can be more dangerous for SMEs: a data breach may break the organization!
- Improvements are more pronounced in SMEs by aligning to best practices and building process maturity.
- SMEs get results faster and leaner. Larger organizations are forced to spend more resources to cut through bureaucracy.
- ISO/IEC 27001 now a common requirement<sup>[3]</sup>
- Easy to find someone who can help!

[1] ["The ROI of Security", Stephanie Losi, 2006](#)

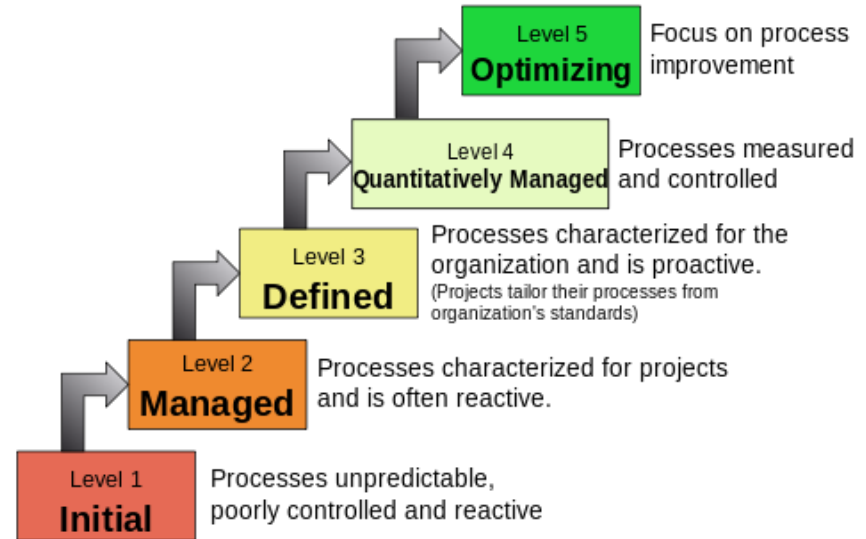
[2] ["Security Watch: The Challenge of Information Security Management, Part 1", Jesper M. Johansson, 2009](#)

[3] [ITGovernance ISO 27001 Global Report 2015](#) (67% says clients asked about it; 50% says required for contracts and tendering.)

# FOR ORGANIZATIONS THAT HAVE NOT ADOPTED A MANAGEMENT SYSTEM: ISMS HELPS IMPROVE PROCESS MATURITY

- ISMS is a management system based on the Deming cycle (Plan, Do, Check, Act / PDCA)
- Organization is required to plan out its objectives and processes
- Framework applies to an entire business, not only to the information security aspect:
  - P: write down policies and procedures
  - D: do it according to procedures
  - C: ensure the results are correct
  - A: fix if unsatisfactory
- Sustainable, consistent, and continually improving organizational performance

## Characteristics of the Maturity levels



"What is CMMI?" Sally Godfrey. NASA 2008. Accessed from Wikipedia 2015/06/11.

# ESTABLISHING AN ISMS BRINGS A TON OF BENEFITS

- Better risk management
  - The ISO/IEC 27001 ISMS uses a risk-based approach
  - Helps your organization focus on risks and good risk management practices
- Management system and process approach
  - Keeps people focused on organizational objectives
  - Helps business processes mature for consistency and efficiency
- Operational improvement and excellence
  - Better performance measurements leading to continual improvement
- More transparency to management
  - Performance and process transparency
  - Able to drive organization with defined objectives
- Aligns your organization with international best practices
- Solid basis for integrated compliance



# LEADERSHIP COMMITMENT IS CRUCIAL TO A SUCCESSFUL ISMS IMPLEMENTATION

- Most important thing in ISMS
  - Leadership commitment
- Implementation of an ISMS requires top-down commitment
  - To cut through the red-tape
  - Perform consent-building and involve stakeholders
- Leadership should take advantage of being an SME:
  - Flexible, quick to change (and adapt)
  - Clear hierarchy of authority
  - Clear responsibilities given leadership commitment
- Leadership should also get trained in ISMS (implementer or auditor) in order to understand role and responsibilities of top management
- Leadership must commit to doing things right:
  - In the end your organization will be more efficient and transparent.
  - Mitigated risks pay dividends to the business purpose.
  - Shortcuts damage integrity of the ISMS and cause unwanted overhead.

# ISMS PROCESSES AND HIERARCHY ARE CLEARLY SHOWN IN THE BIG PICTURE

By functional area



By business unit



## ... WITH SPECIFIC DUTIES LISTED HERE

### Top management

- IS performance managed by CISO
- defines the context (4)
- demonstrates leadership (5), sets policies (5.2), assigns responsibilities (5.3)
- performs high-level risk management (8.2, 8.3)
- sets organizational IS objectives (6.2)
- measures and evaluates performance (9)
- performs management reviews (10)
- manages processes (8.1), define and enforce policies and procedures

### Each subunit

- IS performance managed by single point of contact
- performs risk management on risks it faces (6, 8.2, 8.3)
- sets appropriate IS objectives (6.2)
- manages processes (8.1), define policies and procedures according to needs
- measures and evaluates performance (9)
- continuously improve (10)

# ONLY A PROPERLY SCOPED ISMS CAN ACHIEVE INTENDED BUSINESS GOALS

- Arguably the most important part of the ISMS.
- Scope must be according to natural boundaries: if your business has different, mostly-independent business units, scoping should probably be at the business unit level.
- Some organizations want to get certified without systematic change that brings benefits:
  - Minimize ISMS scope, e.g., to their IT department. ISMS will have limited effect on business.
  - But this creates bureaucracy. Internal agreements will be made between different departments to the IT department, because an ISMS needs a coherent whole.
  - Everything in the organization outside the ISMS is considered external.
  - Such shortcut is counter-productive and does not help achieve business goals
- Smaller SMEs often consider including the entire organization in the ISMS scope
  - This is what we do.

# YET ANOTHER LEADERSHIP COMMITMENT (YALO): ADEQUATE RESOURCES ARE NEEDED TO IMPLEMENT AN ISMS

- The second most important thing: resources
- Employ a dedicated Chief Information Security Officer / Security Manager
  - Or share your “Compliance Manager”
  - Directly reports to the C-suite<sup>[1]</sup>
- CISO is tasked to setup the security organization
  - Size: benchmark security/IT staff ratio within your industry<sup>[2]</sup>
  - Responsible for the numerous ISMS processes and ISMS implementation
- Involve people at all levels
  - Assign a single point of contact in each team with ISMS training
  - Always do implementation together with people who perform daily work with organizational objectives in mind
- Many ISMS processes will need resources to implement
  - Patch management
  - Vulnerability management
  - Incident management
  - Embed security in existing processes (e.g., project management)

[1] “Defending yesterday: Key findings from The Global State of Information Security® Survey 2014”, 2014, PwC

# PROPER IMPLEMENTATION REQUIRES PROPER TRAINING

Information security understaffed in 70% organizations<sup>[1]</sup>, most unfilled<sup>[2]</sup>

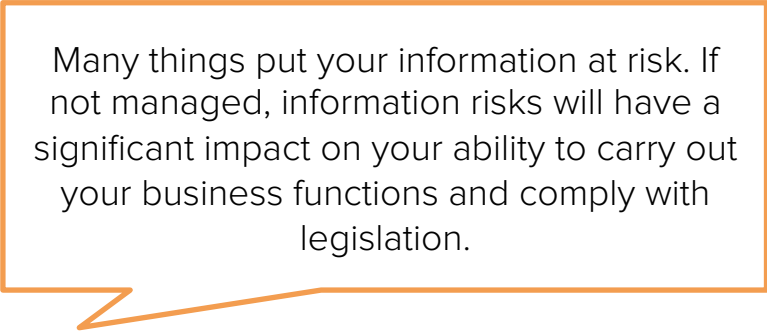
- Train the ISMS implementation team! (strongly recommended)
- Offered by certification bodies:
  - ISMS Implementation training for proper implementation
  - ISMS Internal or Lead Auditor training for internal auditors, ensure continuous improvement of the ISMS
- Train IT staff in InfoSec.
- Offered by many organizations:
  - (ISC)<sup>2</sup>: CISSP, SSCP, CSSLP...
  - ISACA: CISM, CISA, CRISC, CSX...
  - SANS Institute: GSEC, GIAC...
  - CSA: CCSK



[1] "Understaffed and at Risk: Today's IT Security Department", Ponemon Institute, 2014

[2] Ibid., 58% senior, 36% junior information security positions unfilled

# INSTILL A CULTURE OF RISK MANAGEMENT IN THE ORGANIZATION



Many things put your information at risk. If not managed, information risks will have a significant impact on your ability to carry out your business functions and comply with legislation.

UK HM Government, National Archives

- ISO/IEC 27001 uses a risk-based approach
- Require risk assessments, treatments
- Many risk owners don't realize that they are liable to risks

- Organization-wide risk management<sup>[1]</sup>
  - Only risk owners can accept risks: Board, CEO/CIO/CISO or delegates<sup>[2]</sup>
  - Security organization advises risks to risk owners
  - Risk treatments aligned with objectives
  - Each subunit faces its own risks – delegate risk management in a hierarchy allowing comprehensive coverage of risks
  - Use Annex A controls to treat risk!

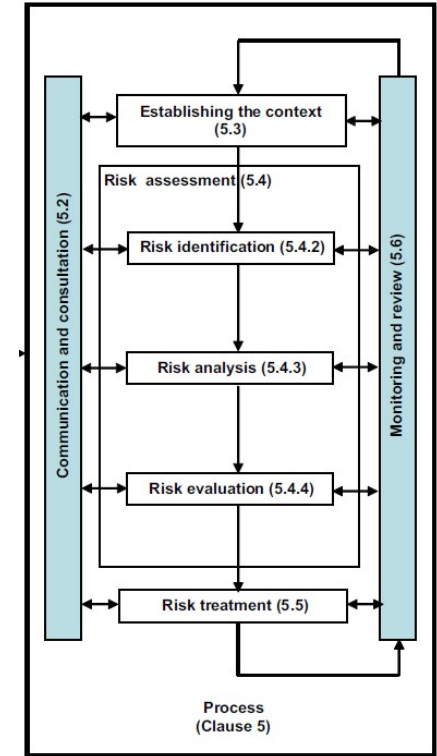
[1] [“Managing Information Risk,” HM Government, National Archives, 2013](#)

[2] [“Why Information Risk is a Board-level Issue”, IAAC](#)

[3] [“5 Non-Technical Reasons Organizations Get Breached”, Don Morash, 2012](#)

# USE RISK MANAGEMENT FRAMEWORKS

- Plenty of mature, risk management frameworks:
  - ISO/IEC 27005, ISO 31000, NIST SP800-37 (RMF)
- Risks arise from existing assets
  - What information do we have?
  - Who are responsible for them?
  - Which of those should we protect?
  - In what priority should we protect them?
  - What costs are we willing to treat these risks?
- Use the ISMS defined context
- Define risk appetite and tolerance: how much is too much risk.
- Remember, only risk owners can accept risks and their treatment!



ISO 31000 risk management flowchart



# SECURITY IS ONLY AS STRONG AS THE WEAKEST LINK – DON'T LET THAT BE YOUR PEOPLE

Challenge 1: Organization “unaware” due to lack of vision or structure<sup>[1]</sup>

- Humans are usually the weakest link
- Develop a culture of security
  - Integrate security into corporate structure and daily operations
  - Strive for whole company awareness, core competency
- Leadership commitment
  - Must start with top management being fully committed to security
  - Embed security into culture

Challenge 2: CISOs struggle between strategic and operational security<sup>[1]</sup>

- Find the right security structure
  - Handle strategies and policies centrally
  - Implementation by individual groups
  - Not overly centralized: only security team cares about security, other staff lacking security awareness
  - Not overly distributed: people end up working in separate silos, overall security posture compromised

[1] [“Security Watch: The Challenge of Information Security Management, Part 1”, Jesper M. Johansson, 2009](#)

# MORE PRACTICAL ADVICE ON COMPLYING TO THE STANDARD

- ISMS motto: “the less you {own, do, manage, keep...}, the easier to comply!”
  - Outsource non-essential services, leverage cloud services: email, antivirus, server monitoring, infrastructure and backups
  - Do not keep data that is not necessary (data = burden)
  - Automate, automate, automate. Don’t do things that the computer can do for you.
  - Mobile device management (MDM), log management, SIEM
- Align with realistic and current security demands to ensure a minimal attack surface<sup>[1]</sup>
- KISS
  - Simple policies can be understood, simple procedures can be followed
  - Small is beautiful in documenting ISMS<sup>[2]</sup>.
- Statement of Applicability (SoA)
  - Most controls apply to the full scope
  - Tailor at the operational / functional levels (teams)
- Try self-assessment checklists from CBs<sup>[3]</sup>!

[1] [“How to optimize your security budget”, George V. Hulme, CSO Magazine, 2014](#)

[2] [List of mandatory documents required by ISO 27001 \(2013 revision\), 27001 Academy, 2013](#)

[3] [“BSI ISO/IEC 27001:2013 Self-assessment questionnaire”, BSI, 2014](#)

# THE FASTEST WAY TO IMPLEMENT A SUCCESSFUL ISMS: LEAD YOURSELF (WITH HELP) – DO NOT SHORTCUT

## Consultants

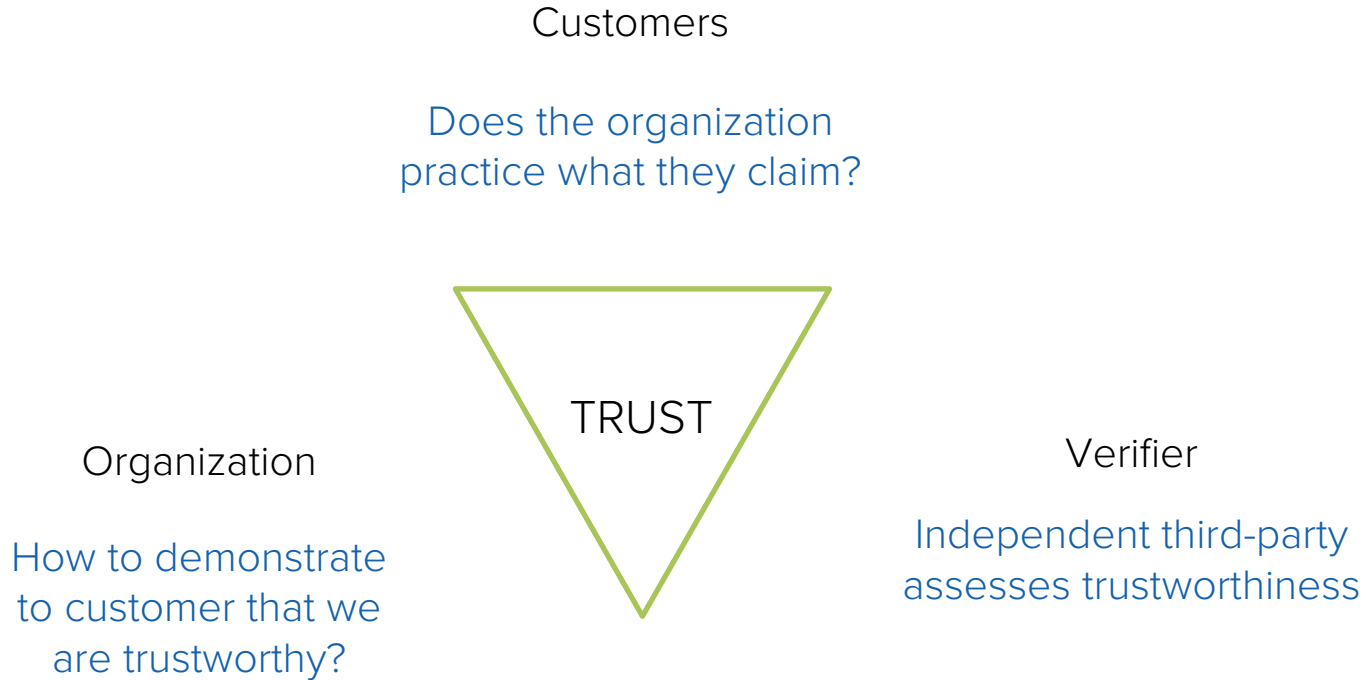
- Do not engage until completed ISO/IEC 27001 training.
- Training helps you understand what a consultant does and how they can help.
- Without training, you can't differentiate between apples and oranges: consultant can give you anything.
- Consultants can bring experience that helps “implement”, but no one knows your business as well as yourself.
- Understand your business processes first instead of adhering to consultant's best practices.

## Templates

- Do not rely on templates because it can make the ISMS too burdensome to maintain. A process that works for another company may not work for yours.
- Perpetuation of bad practices: e.g., the “master document list”, which was never part of the standard, but templates have encouraged this.
- Only consider templates for reference after being trained to prevent confusion.
- More crucial for SMEs to get it right early on to prevent diversions and extra costs.

The goal is to reap benefits of an ISMS and certify on the way, NOT just getting certified.

# CERTIFIED ASSURANCE EXISTS TO PROMOTE TRUST



# A LOGICAL STEP IN ENSURING PROPER IMPLEMENTATION AND BRINGS MULTIPLE BENEFITS

## Rationale

- Measureable, verifiable, then improvable
- Third-party assurance is (more) impartial
- Ensures implementation of framework is adequate and complete
- Cost of audit
  - Minimal compared to cost of training and implementation
- 3-year cycle
  - First year initial audit
  - 2 subsequent annual surveillance audits

## Benefits

- Customer (external)
  - Trust
  - Transparency
  - Differentiation
  - Third-party audit obsoletes need for your customer's second-party audits
- Internal
  - Operational effectiveness
  - Transparency: management knows ISMS is indeed performing

# ACHIEVING CERTIFICATION IS AN ACHIEVEMENT – MAXIMIZE YOUR RETURN BY USING A REPUTABLE CERTIFICATION BODY

- Not all certification bodies (CBs) are equal.
- Using a reputable CB allows your customers to further trust your certification.
- Maximize your return by considering their reputation:
  - Using a CB that “sells” certificates not only can destroy the value of the certification, but also your reputation.
- Recognition matters:
  - If you operate internationally or deal with international customers, consider a reputable CB with an international reach for global recognition.
- CBs have different strengths
  - Some are stronger in certain areas / management system standards than others.
  - Choose one with experience in your sector for better auditing results
- It's not (just) about the price:
  - A lower price may mean lower cost / more junior auditors
  - Quality of auditing affects the quality of your ISMS
  - Reputation to customers
- Contact more than one CB to compare!

# ACHIEVING CERTIFICATION IS AN ACHIEVEMENT – ALWAYS USE AN ACCREDITED CERTIFICATION BODY

- Accreditation bodies (AB) accredit (“certify”) a CB’s ability to perform certifications.
  - ABs audit the CBs to make sure they operate properly.
  - Management system certifications are governed by ISO/IEC 17021.
- Choose a CB whose program (e.g., ISO/IEC 27001) is accredited in your sector. e.g., [BSI, ISO 9001, Pharmaceuticals]
  - Always ask the CB – even reputable ones may not be accredited in certain standards!
  - A certification can carry multiple accreditations (e.g., HKAS, UKAS)
- Follow business requirements: some tender requirements dictate accreditation requirements (e.g., Housing Authority requires HKAS-accredited ISO 50001).
- Brand names and where you do business matter: UK businesses obviously trust UKAS.



[1] [List of HKAS accredited certification bodies](#)

# THE CERTIFICATION PROCESS IS ALWAYS SMOOTHER WITH PROPER PREPARATION AND RESPECT

## Gap assessment

- Do a gap-assessment before/during implementation of the ISMS
- Tells you what needs to be improved to align the ISMS with the standard, and whether it is ready for certification
- Can be done internally, by a consultant or CB

## Pre-assessment (strongly recommended)

- Prior to the certification audit, ask the CB to perform a pre-assessment
- Mock-exam gives you a taste of how audits work and which areas need improvement
- Like a certification audit except examined areas is a subset

## Internal audits

- Some CBs require an internal audit done before certification audits
- Do it yourself with the proper training

## External auditors are your best friend

- Friends, not foes: bring lots of experience and can deliver lots of value (not consultants but allowed to opine)
- They always find something which your internal auditors won't.
- Trained to be impartial and transparent with issues to the auditee.
- Don't get discouraged by findings. Every finding is an opportunity to improve!



# ADDRESS THE RISKS NOW

## Governance gaps

### Cloud

47% use cloud services, but 62% of these have no policies governing cloud services<sup>[1]</sup>

### Mobile

58% do not have a mobile security strategy<sup>[1]</sup>

## Ask yourself

- Will our trade secrets / customer data be leaked?
- Will we get hacked and end up on the front page?
- Will our intellectual property get stolen?

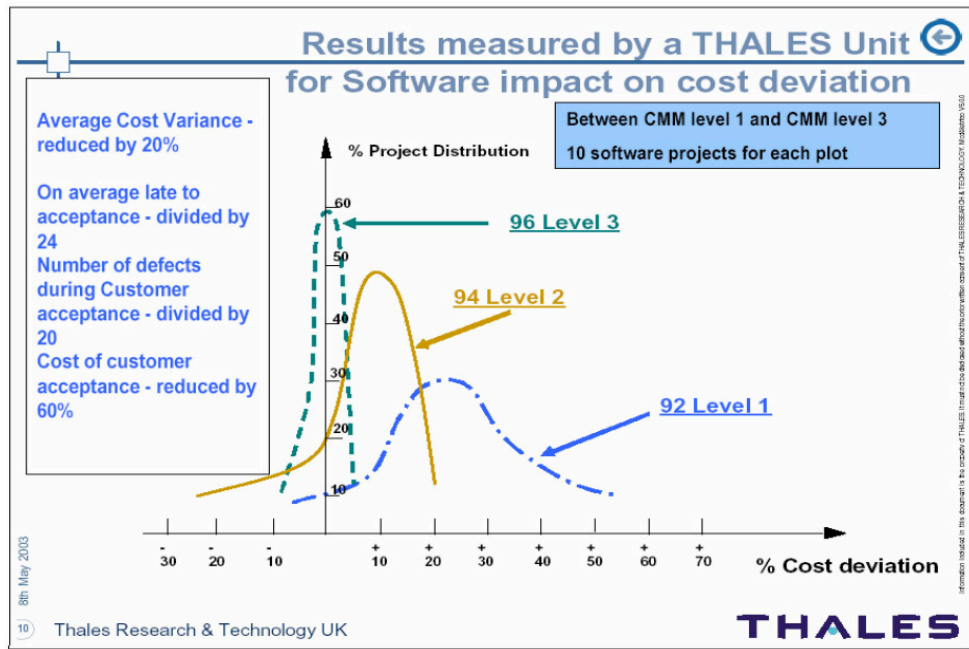
Issues above already covered in the ISO/IEC 27001 standard – the ISMS approach really works.  
Protect your organization now!

[1] “Defending yesterday: Key findings from The Global State of Information Security® Survey 2014”, 2014, PwC

# Appendix

# IMPROVE BUSINESS PROCESS PERFORMANCE ONLY POSSIBLE AFTER BEING MEASURED

- Concept demonstration (software project example from CMMI)
- ISMS helps your organization do this on information security performance
- Provides solid ground to apply the same concept to continually improve other aspects :
  - Quality (ISO 9001)
  - Environmental (ISO 14001)
  - Business continuity (ISO 22301)
  - ...



Getting Started with Process Improvement Using the CMMI®. Carol Marsh, Patrick Vigier. ESEPG 2003.