POLICY & COMPLIANCE

“COMPLY OR DIE TRYING”

Or “How I Learned to Stop Worrying and Love Standards”

A PowerPoint Slide Presentation

By Andrew Kelly

OWASP Day 2012

Abstract

We all have to comply with something: Laws or bylaws - regulations or recommendations - industry standards or industry best-practice.

This OWASP talk will focus on the 'real-world' application of security policy and compliance in IT and business.

How policy and compliance can actually be very useful when it comes to securing your job, your company - and your company's future. Both from an IT - and a business/commercial prospective.

And - along the way - some common myths, misconceptions and downright misunderstandings around policy and compliance may well be busted.

Come and listen to a guy who actually thinks compliance and policy ... are fun!

All About Me

Telecom Ltd., Auckland, NZ [2012 on]; Lateral Security (IT) Services Ltd., Auckland, NZ [2010-2012]; Security-Assessment.com Ltd., Auckland, NZ [2007-2009]; Transpower Ltd., Wellington, NZ [2006-2007]; BT Syntegra Ltd., London, UK [2006]; Fonterra Co-operative Group Ltd., Auckland, NZ [2004-2005]; BT Syntegra Ltd., Leeds, UK [2004]; Insight Consulting Ltd., Walton-on-Thames, UK [2003]; National Bank of NZ Ltd., Wellington, NZ [2003-2004]; Royal Bank of Scotland Group, Edinburgh, UK [2002]; Halifax/Bank of Scotland, Leeds, UK [2001]; Banque Nationale de Belgique, Brussels, Belgium [2001]; Deutsche Bank Ltd., London, UK [2000-2001]; Lloyds/TSB Bank Ltd., Southend-on-Sea & London, UK [2000]; Bank One International/First USA Bank, Cardiff, UK [1999]; Générale de Banque, Brussels, Belgium [1998-1999]; Perot Systems Europe Ltd., Nottingham, UK [1997-1998]; Chartered Trust Plc (Standard Chartered Bank), Cardiff, UK [1996-1997]; Legal & General Assurance, Kingswood, Surrey, UK [1996]; Sun Life Assurance Company of Canada (UK) Ltd., Basingstoke, UK [1989-1993]; Databank Systems Ltd., Wellington, NZ [1988-1989]

All About Me

You saw right: Telecom Ltd., Auckland, NZ [2012 on]

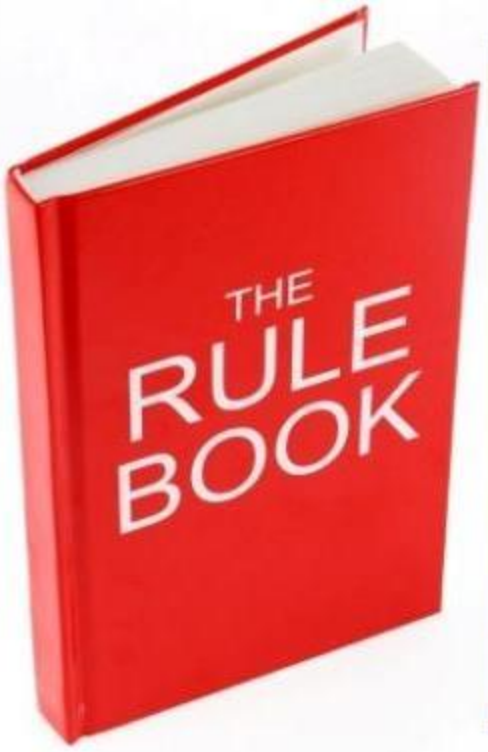
Yes! Resistance ***was*** futile ... and I have been ... absorbed!

A Favourite Quote

“If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.”

Bruce Schneier

“PEOPLE, PROCESS, TECHNOLOGY”



“People, Process, Technology”

“People … Process … Technology”

Organisations often apply technology (first) to solve security problems - only to find the ‘solution’ ends up worse than the original problem (remember Schneier?).

A 'technology-first' - tactical - mindset often provides only a temporary fix.

The goal *should* be to define a ‘fit-for-purpose’ environment - by first making the people and processes more efficient: *Then* giving employees the tools and technology to make them more effective.

“People, Process, Technology”

“We’ve got this new-and-awesome monitoring system…”

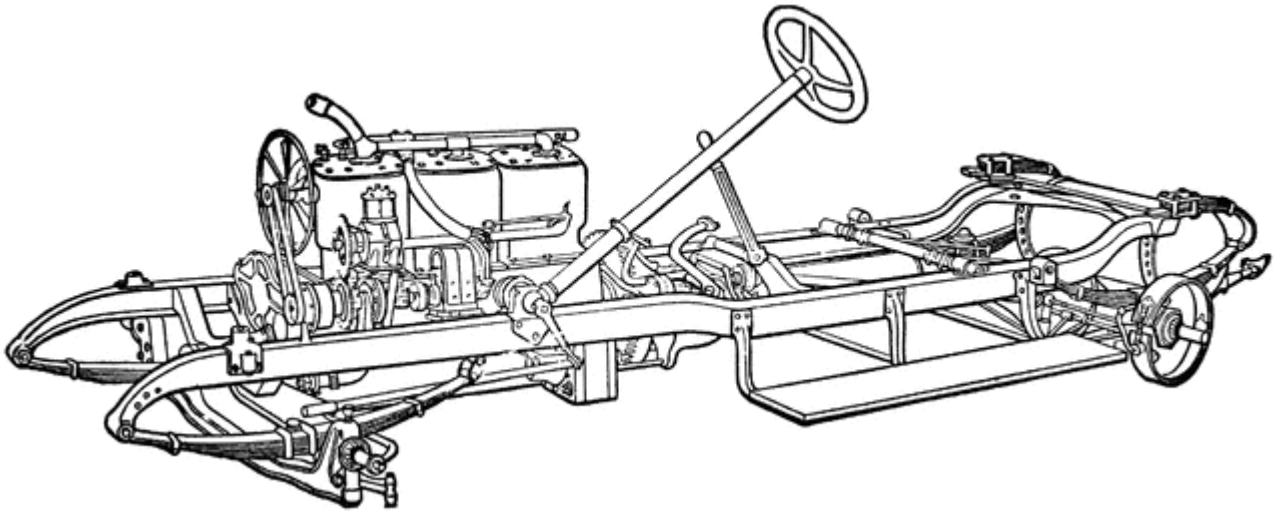
AN ANALOGY

Why information Security policy and governance should be important to you…

No, really…

An Analogy

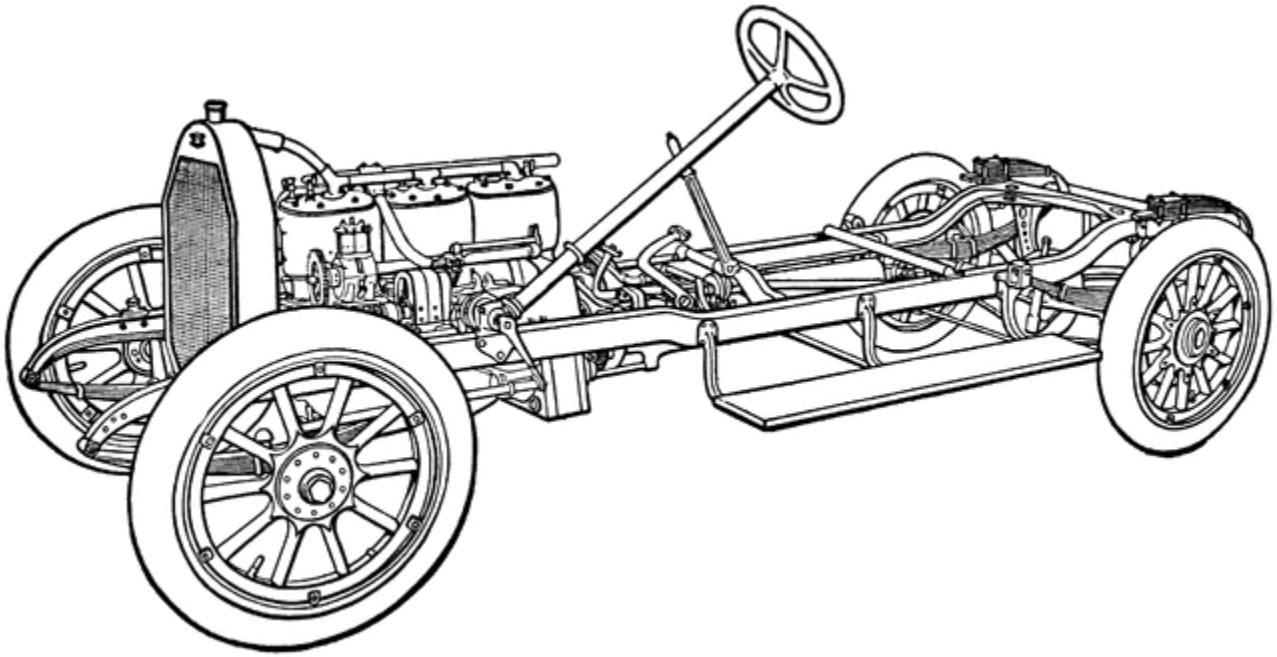
Think of technology as the … engine … of information security...



Lots of constantly moving parts, thingies going up and down; it's always being improved, updated and uprated. It's always striving to drive information security forward...

An Analogy

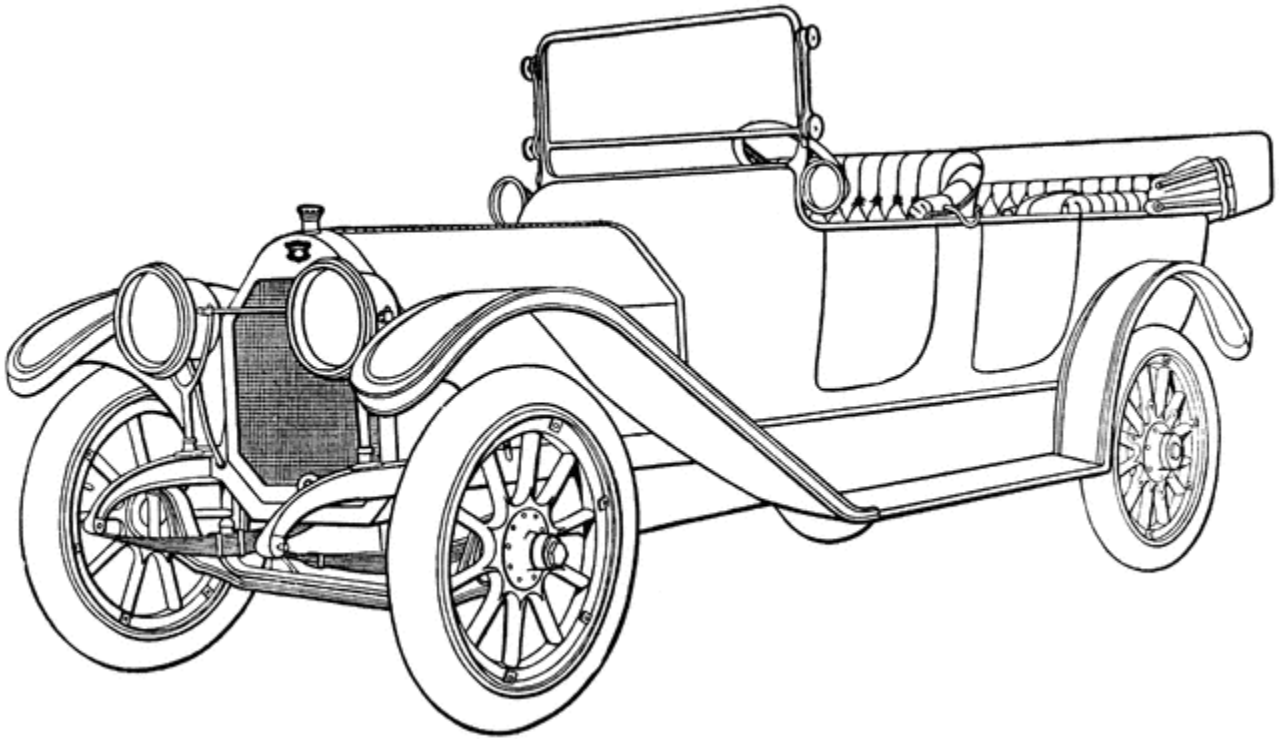
Think of an information security policy as providing the framework around that technology...



Because technology without a framework - with no context - is like a car with no wheels: Lotsa noise alright ... but it ain't going nowhere fast!

An Analogy

Then think of information security governance then as the wrapping around the whole thing…



Because technology and policy without governance - without a management mandate - is fine. But it can get a little drafty … and wet!

An Analogy

“We’ve contracted you to create an Information Security Policy...”

‘LEFT-FIELD’ THINKING

‘Left-Field’ Thinking

Do you have problems?

Are you finding the youth of today simply can’t be asked when it comes to slicing noodles - because the job is ‘exhausting’?

Don’t want to spend the 30,000 yuan a year - plus - it takes to hire a qualified noodle chef … if you can find one anyway?

Is noodle-uniformity a ‘must-have’?

Are you a closet fan of Anime and/or 1950’s kitsch?

Then … does ex-Chef Cui Runguan have just the product for *YOU!*

‘Left-Field’ Thinking

“Chef Cui” - the 10,000 yuan noodle-slicing robot!

A ‘bot with only one thing on its tiny electronic mind: Slicing uniform noodles into a boiling pot of water for hour after hour!

First revealed in March 2011 - more than 3,000 *“Chef Cui”* robots have been sold since.

‘Left-Field’ Thinking

‘The Uninvited Guest: Chinese Sub Pops up in Middle of U.S. Navy Exercise, Leaving Military Chiefs Red-faced’

Daily Mail (UK), November 2007

When the US Navy deploys a battle fleet on exercises, it takes the security of its aircraft carriers very seriously indeed…

‘Left-Field’ Thinking

The uninvited guest: A Chinese Song Class submarine.

Like the one that surfaced by the *USS Kitty Hawk…*

‘Left-Field’ Thinking

Password Strength

All passwords must contain at least:

1. Eight (8) characters;
2. One (1) special character; and
3. One (1) capital.

‘Left-Field’ Thinking

Resulting password:

mickeyminniedonalddaisyhueydeweylouiegoofyquasimodowellington

‘Left-Field’ Thinking

Resulting password:

mickeyminniedonalddaisyhueydeweylouiegoofyquasimodowellington

1. Eight (8) characters?

   Check: mickey, minnie, donald, daisy, huey, dewey, louie & goofy

2. One (1) special character?

   Check: quasimodo

3. One (1) capital?

   Check: wellington

IT'S COMPLIANCE TIME

We all have to comply with *something*…

Laws or bylaws - regulations or recommendations - industry standards or industry best-practice.

It’s Compliance Time

Information Security:
ISO/IEC 27001 ‘IT - Security Techniques - IS Management Systems - Requirements' (ISO 27001);
ISO/IEC 27002 ‘IT - Security Techniques - Code of Practice for IS Management' (ISO 27002);
'New Zealand Information Security Manual' (NZISM);
'Australian Government Information Security Manual' (AGISM);
'Payment Card Industry Data Security Standard' (PCI DSS);
ISF 'Standard of Good Practice' (SoGP); and
National Institute of Standards and Technology Special Publications (NIST 800-series).

Governance:
ITGI 'Control Objectives for Information and Related Technologies' (COBIT); and
HM Government 'Information Technology Infrastructure Library' (ITIL).

Assurance:
ISAE 3402 'Assurance Reports on Controls at a Service Organisation' (ISAE 3402); and
SSAE 16 'Reporting on Controls at a Service Organisation' (SSAE 3402).

Legislation:
Official Information Act 1982;
Privacy Act 1993;
Protected Disclosures Act 2000; and
Sarbanes-Oxley Act 2002.

It’s Compliance Time

OWASP Code Review Requirements

From OWASP's *'Code Review Introduction'* page:

“Code review is probably the single-most effective technique for identifying security flaws. When used together with automated tools and manual penetration testing, code review can significantly increase the cost effectiveness of an application security verification effort.”

So ... what do we have to - or can we - comply with here?

It’s Compliance Time

ISO/IEC 27002:

5.1.2 Review of the information security policy

6.1.8 Independent review of information security

10.4.1 Controls against malicious code

11.1.1 Access control policy

11.2.4 Review of user access rights

11.6.1 Information access restriction

12.1.1 Security requirements analysis and specification

12.2.1 Input data validation

12.5.1 Change control procedures

12.5.2 Technical review of applications after operating system changes

12.5.5 Outsourced software development

12.6.1 Control of technical vulnerability

15.2.1 Compliance with security policies and standards

15.2.2 Technical compliance checking

It's Compliance Time

NZISM:

2.2 'Outsourcing information technology services and functions' (2)

6.1 'Conducting cyber security reviews'

6.2 'Vulnerability analysis strategy'

6.2 'Resolving vulnerabilities'

12.4 'When security patches are not available'

14.1 'Automated outbound connections by software' (2)

14.5 'Secure programming'

14.5 'Software testing' (2)

14.6 'Agency website content'

PCI DSS:

Requirement 6: Develop and maintain secure systems and applications [specifically subsections 6.3, 6.3.1, 6.3.2, 6.5, 6.5.1 to 6.5.9]

COBIT:

AI2.4 Application security and availability

AI2.6 Major upgrades to existing systems

AI2.7 Development of application software

It’s Compliance Time

COBIT (continued):

AI3.2 Infrastructure resource protection and availability

AI6.2 Impact assessment, prioritisation and authorisation

AI7.2 Test plan

AI7.4 Test environment

AI7.6 Testing of changes

AI7.7 Final acceptance test

DS5.5 Security testing, surveillance and monitoring

DS5.7 Protection of security technology

DS5.9 Malicious software prevention detection and correction

DS9.2 Identification and maintenance of configuration items

DS9.3 Configuration integrity review

ME2.2 Supervisory review

ME2.3 Control exceptions

ME2.4 Control self-assessment

ME2.5 Assurance of internal control

ME2.7 Remedial actions

It's Compliance Time

COBIT (continued):

ME4.7 Independent assurance

PO2.3 Data classification scheme

PO3.1 Technological direction planning

PO8.3 Development and acquisition standards

ITIL:

SD 2.4.2 Scope

SD 3.11 Service design models

SD 3.6 Design aspects

SD 3.6.1 Designing service solutions

SD 3.7.3 Develop the service solution

SD 4.6.4 Policies, principles, basic concepts

SD 4.6.5.1 Security controls

SD 5.3 Application management

SO 4.4.5.11 Errors detected in the development environment

SO 5.11 Internet/web management

SO 5.13 Information security management and service operation

It’s Compliance Time

ITIL (continued):

SS 6.5 Sourcing strategy

SS 8 Technology and strategy

SS 9.5 Risks

ST 3.2.3 Adopt a common framework and standards

ST 4.1.4 Policies, principles and basic concepts

ST 4.1.5.1 Transition strategy

ST 4.1.5.2 Prepare for service transition

ST 4.3.5.3 Configuration identification

ST 4.3.5.4 Configuration control

ST 4.4.5.3 Build and test

ST 4.4.5.4 Service testing and plans

ST 4.5.5.1 Validation and test management

ST 4.5.5.5 Perform tests

ST 4.6 Evaluation

It’s Compliance Time

“I know this company that’s spent $2 million on getting itself PCI DSS certified...”

SELLING SECURITY POLICY

Narrator: Chicken Little was in the woods one day when an acorn fell on her head.

Chicken Little: "Help! Help! The sky is falling! I have to go tell the king!"

Selling Security Policy

The advantages of a technology-independent, business-focused and -aligned Information Security Policy:

1. High-level, easy-to-understand language bridges the divide between the business, IT professionals - and clients;

Selling Security Policy

The advantages of a technology-independent, business-focused and -aligned Information Security Policy:

1. High-level, easy-to-understand language bridges the divide between the business, IT professionals - and clients;
2. Focuses on desired outcomes - not on the means of implementation;

Selling Security Policy

The advantages of a technology-independent, business-focused and -aligned Information Security Policy:

1. High-level, easy-to-understand language bridges the divide between the business, IT professionals - and clients;
2. Focuses on desired outcomes - not on the means of implementation;
3. Simplifies the corporate compliance process - positioning your company to quickly and efficiently adapt to new requirements;

Selling Security Policy

The advantages of a technology-independent, business-focused and -aligned Information Security Policy:

1. High-level, easy-to-understand language bridges the divide between the business, IT professionals - and clients;
2. Focuses on desired outcomes - not on the means of implementation;
3. Simplifies the corporate compliance process - positioning your company to quickly and efficiently adapt to new requirements;
4. Provides commercial advantage in a competitive market place;

Selling Security Policy

The advantages of a technology-independent, business-focused and -aligned Information Security Policy:

1. High-level, easy-to-understand language bridges the divide between the business, IT professionals - and clients;
2. Focuses on desired outcomes - not on the means of implementation;
3. Simplifies the corporate compliance process - positioning your company to quickly and efficiently adapt to new requirements;
4. Provides commercial advantage in a competitive market place;
5. Security becomes a matter of compliance with agreed requirements - as opposed to the ‘best-practise’ or ‘opinion’ approach; and

Selling Security Policy

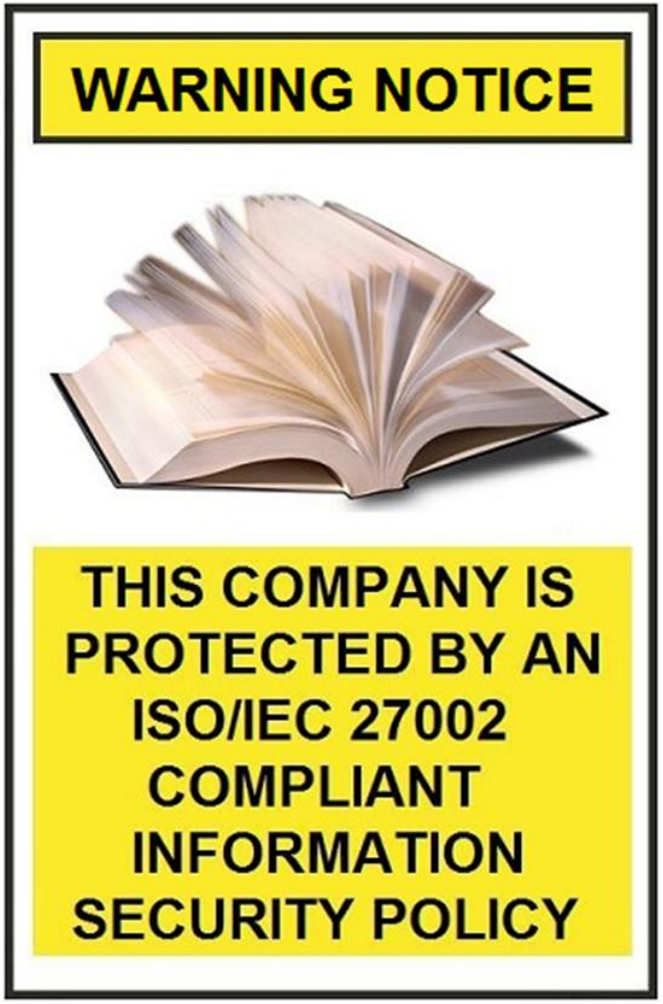
The advantages of a technology-independent, business-focused and -aligned Information Security Policy:

1. High-level, easy-to-understand language bridges the divide between the business, IT professionals - and clients;
2. Focuses on desired outcomes - not on the means of implementation;
3. Simplifies the corporate compliance process - positioning your company to quickly and efficiently adapt to new requirements;
4. Provides commercial advantage in a competitive market place;
5. Security becomes a matter of compliance with agreed requirements - as opposed to the ‘best-practise’ or ‘opinion’ approach; and
6. Policy objectives provide a viable framework within which to implement more detailed and/or technical standards and procedures.

Selling Security Policy

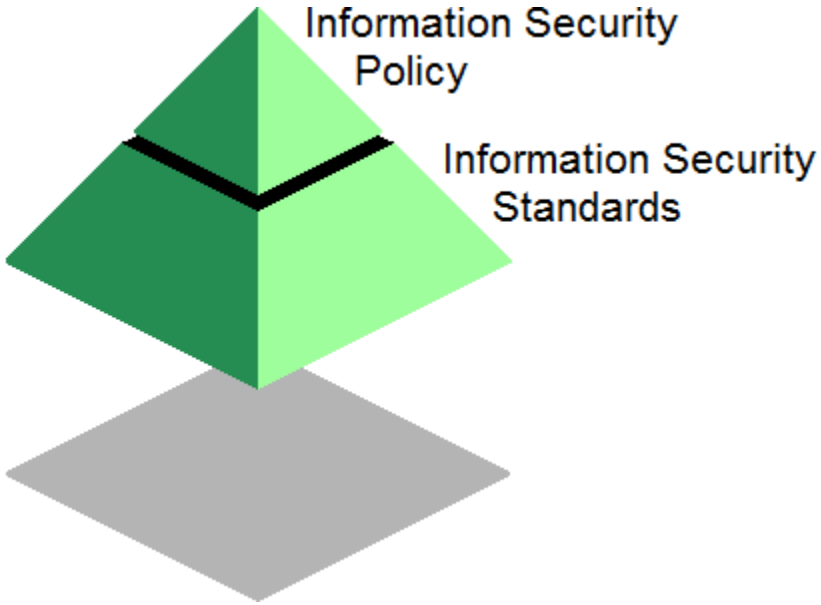
“But you haven’t mentioned the fact it’ll make us more secure...”

INFORMATION SECURITY POLICY 101

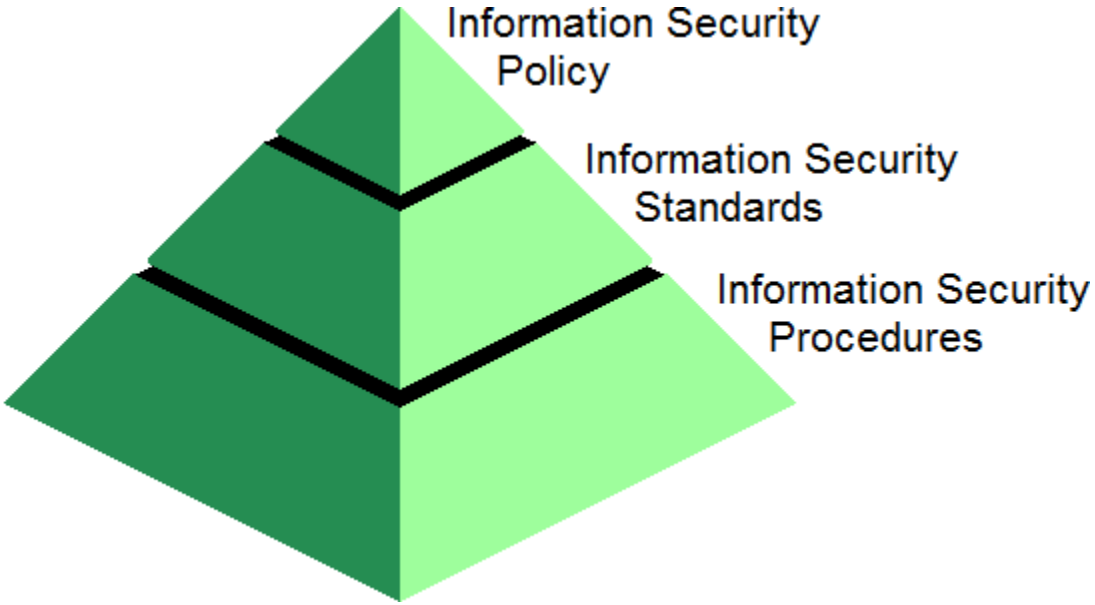


Information Security Policy 101

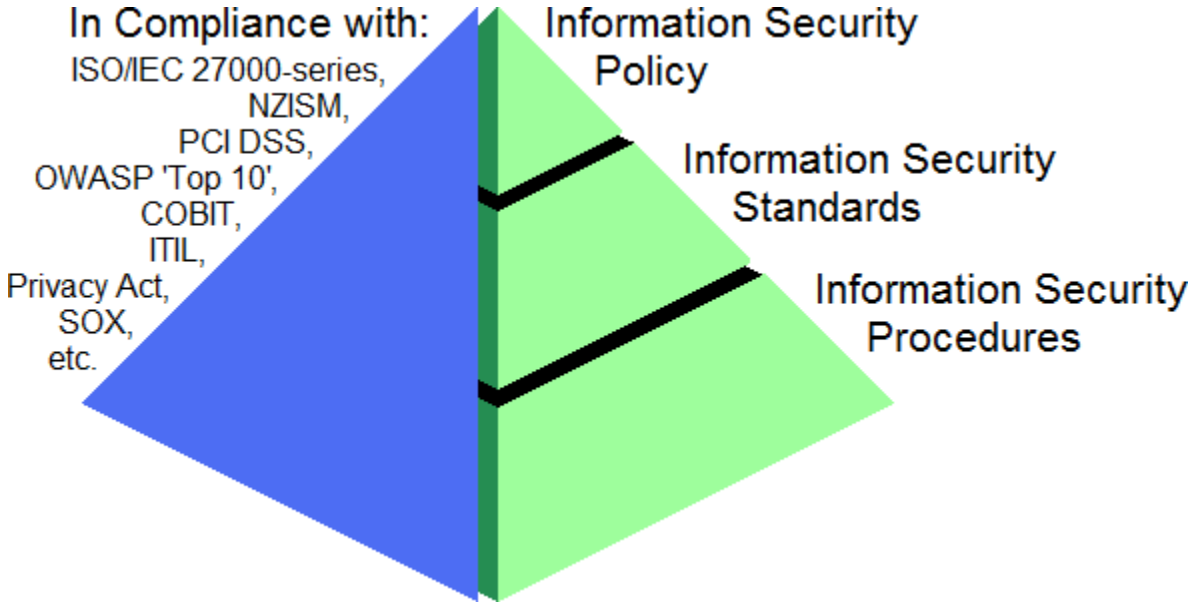
Information Security Policy 101



Information Security Policy 101

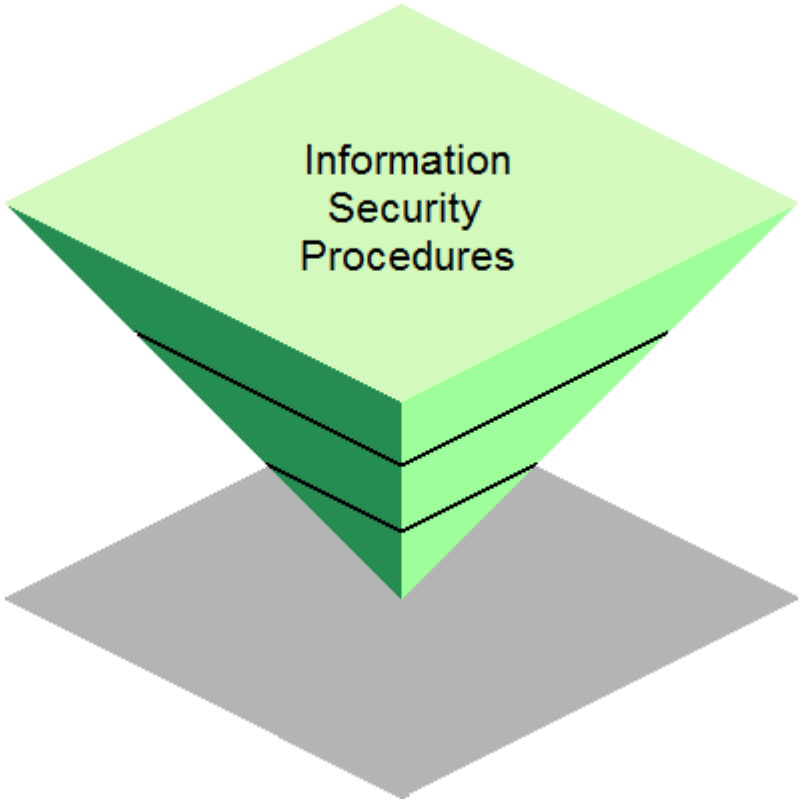


Information Security Policy 101



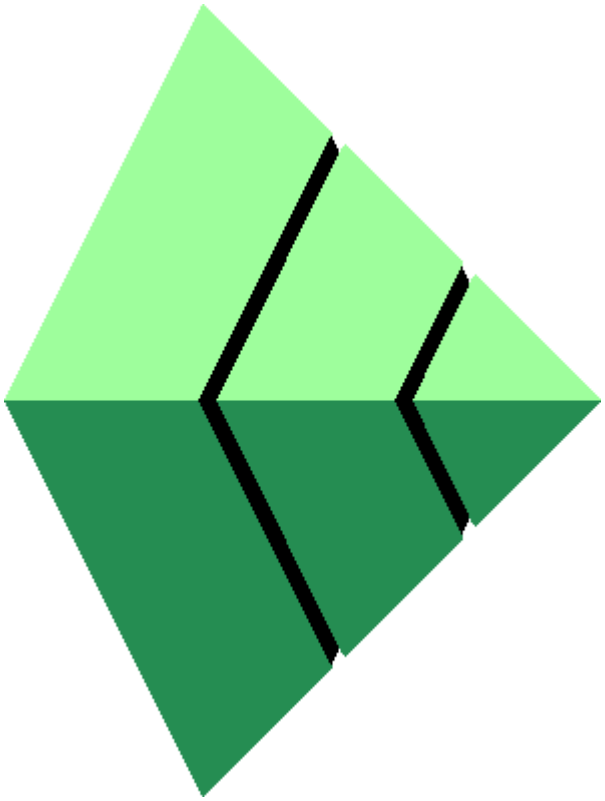
Information Security Policy 101

Some do it the wrong way about...



Information Security Policy 101

And some like it sideways...



Information Security Policy 101

“No problem! I’ll get on and create another policy...”

MYTHS, MISCONCEPTIONS AND MISUNDERSTANDINGS

Myths, Misconceptions & Misunderstandings

“Compliance plus/minus certification equals security”

Compliance can’t ensure security - only attesting to the state of security at a specific moment in time.

Most often compliance relies on people continuously adhering to policies and standards.

Myths, Misconceptions & Misunderstandings

“To solve our compliance issues, we need product *x*”

Technology - alone - can’t meet your compliance needs: It’s always been about aligning the right technologies with people and process.

Remember Schneier’s quote?

Myths, Misconceptions & Misunderstandings

“Security compliance is too hard”

Every time a new compliance mandate comes out, it’s more about rearranging already generally accepted controls: The underlying and fundamental objectives won’t change.

Myths, Misconceptions & Misunderstandings

“Security compliance is an IT project”

IT may implement the technical and operational aspects - but compliance is an on-going process of assessment, remediation and reporting.

Compliance is a *business* issue best addressed using a multi-disciplinary approach.

Myths, Misconceptions & Misunderstandings

“Non-compliance is bad”

Can non-compliance actually be useful when it comes to securing your job, your company - and your company's future?

ADVERTISEMENT

“Anatomy Of Fraud: A Study Of Fraud In New Zealand”

http://abkaye.blogspot.co.nz/

ANY QUESTIONS?

None? Most excellent...!