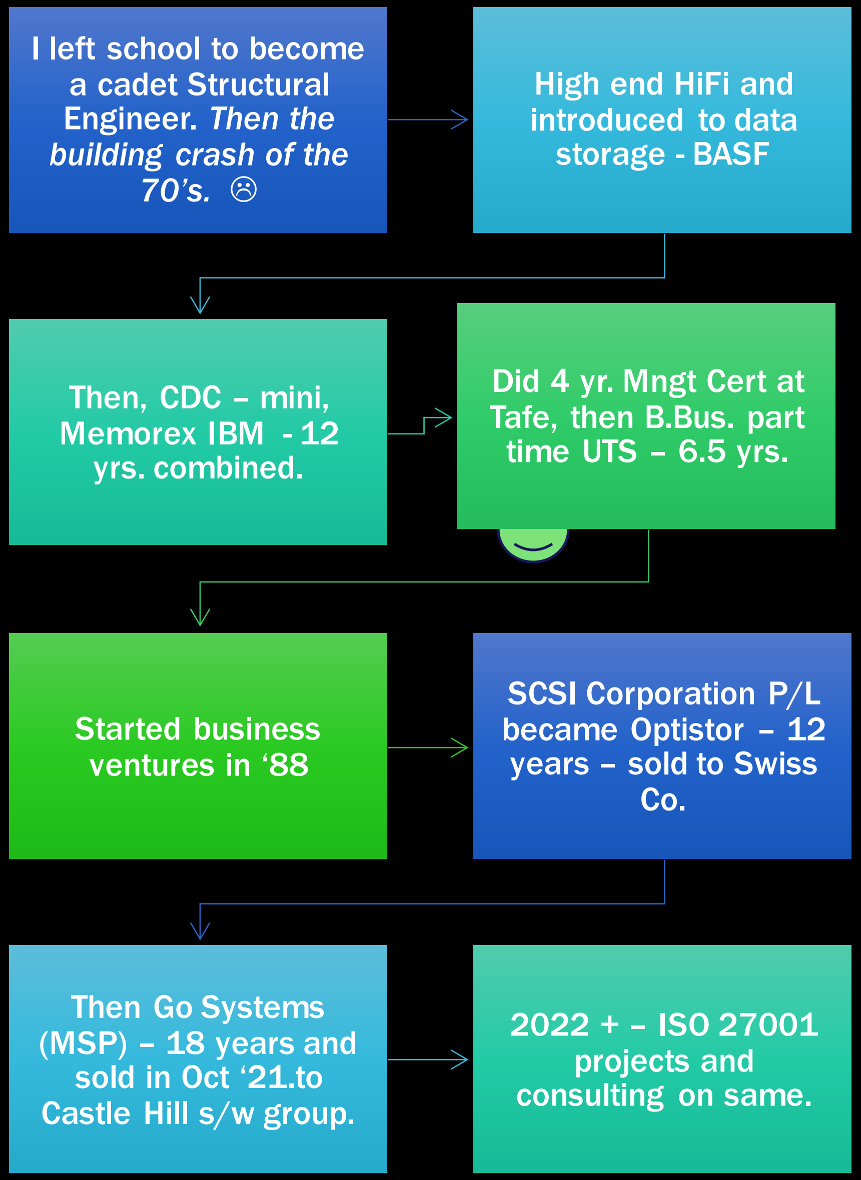
THE ISO 27001 CERTIFICATION – HOW TO UNDERTAKE AND ACHIEVE YOUR JOURNEY IN A TIMELY AND EFFECTIVE MANNER?

ISO27001 Certification – Information Security Management System (ISMS)

Information Security Management ISO 27001 Certified

SO, WHOM AM I TO PRESENT THIS TOPIC TO YOU TODAY?



I left school to become a cadet Structural Engineer. *Then the building crash of the 70's.* ☹

High end HiFi and introduced to data storage - BASF

Then, CDC – mini, Memorex IBM - 12 yrs. combined.

Did 4 yr. Mngt Cert at Tafe, then B.Bus. part time UTS – 6.5 yrs.

Started business ventures in '88

SCSI Corporation P/L became Optistor – 12 years – sold to Swiss Co.

Then Go Systems (MSP) – 18 years and sold in Oct '21.to Castle Hill s/w group.

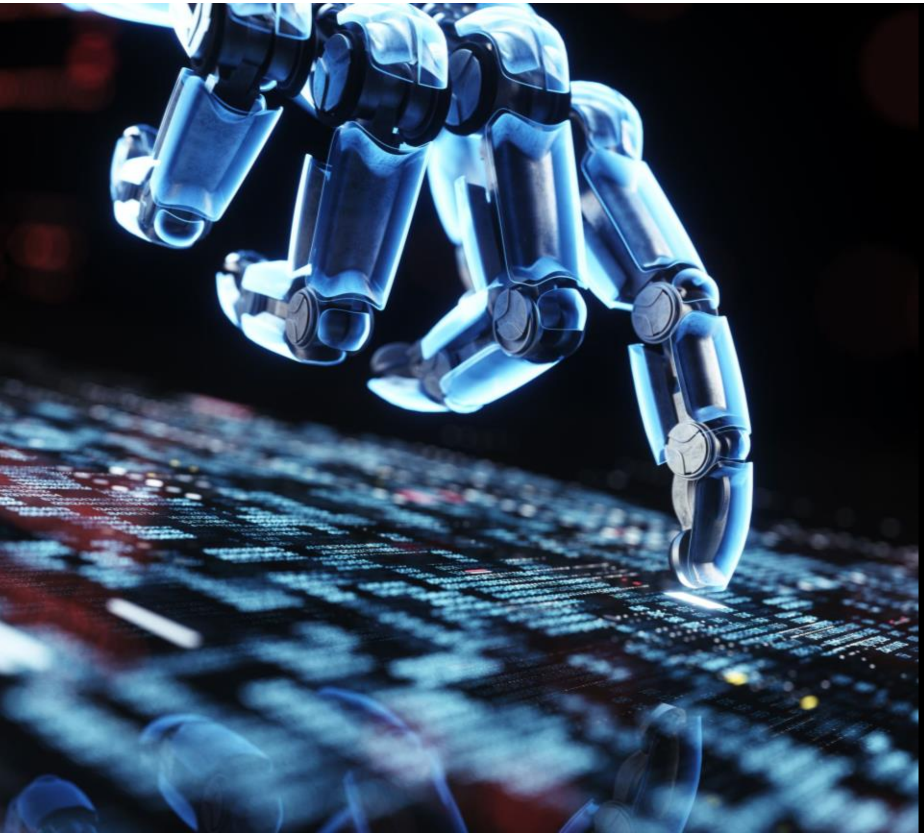
2022 + – ISO 27001 projects and consulting on same.

PROOF WILL BRING CONFIDENCE

Information Security Management
ISO
27001
Certified

ISO27001 (ISMS) Certification provides the robust framework for implementing and managing your ISMS.

IS ISO27001 STATIC?



- No, the standard continues to evolve as the tech evolves.
- We are now into version 2022.
- The gaps between versions will get tighter as time goes on.
- The previous version was 2013.
- The versions update themselves for where security is at in this ever-changing world.

SECURITY - SOME OF THE MANY AUSSIE HACKS

Millions of names and details stolen; including mine with Medibank (3.9m) and Latitude.

😠

Latitude Financial Services 😠

medibank

DYMOCKS FOR BOOKLOVERS

'yes' OPTUS

HWL EBSWORTH LAWYERS

SOME RECENT HACKS

City of Onkaparinga Council (Adelaide) – Ryuk ransomware.

As of 18th Sept 2023 - 65 Aust Govt agencies caught up in HWL Ebsworth cyber-attack. Most did not suffer a cyber incident, however Insurance Commission of WA may have.

In SA 38,000 government employees and potentially up to 80,000 workers were exposed. Frontier Payroll was hacked.

The list goes on.

EVEN MSPS ARE GETTING HACKED.

The Russian cybercriminal group AlphaV also known as.

Hacked a Melb MSP in Sept '23 and also their customers. Stole 4.9TB of data. – Real Estate, Medical, Legal Firm, Strata Group etc.

SECURITY – RMM PLATFORMS

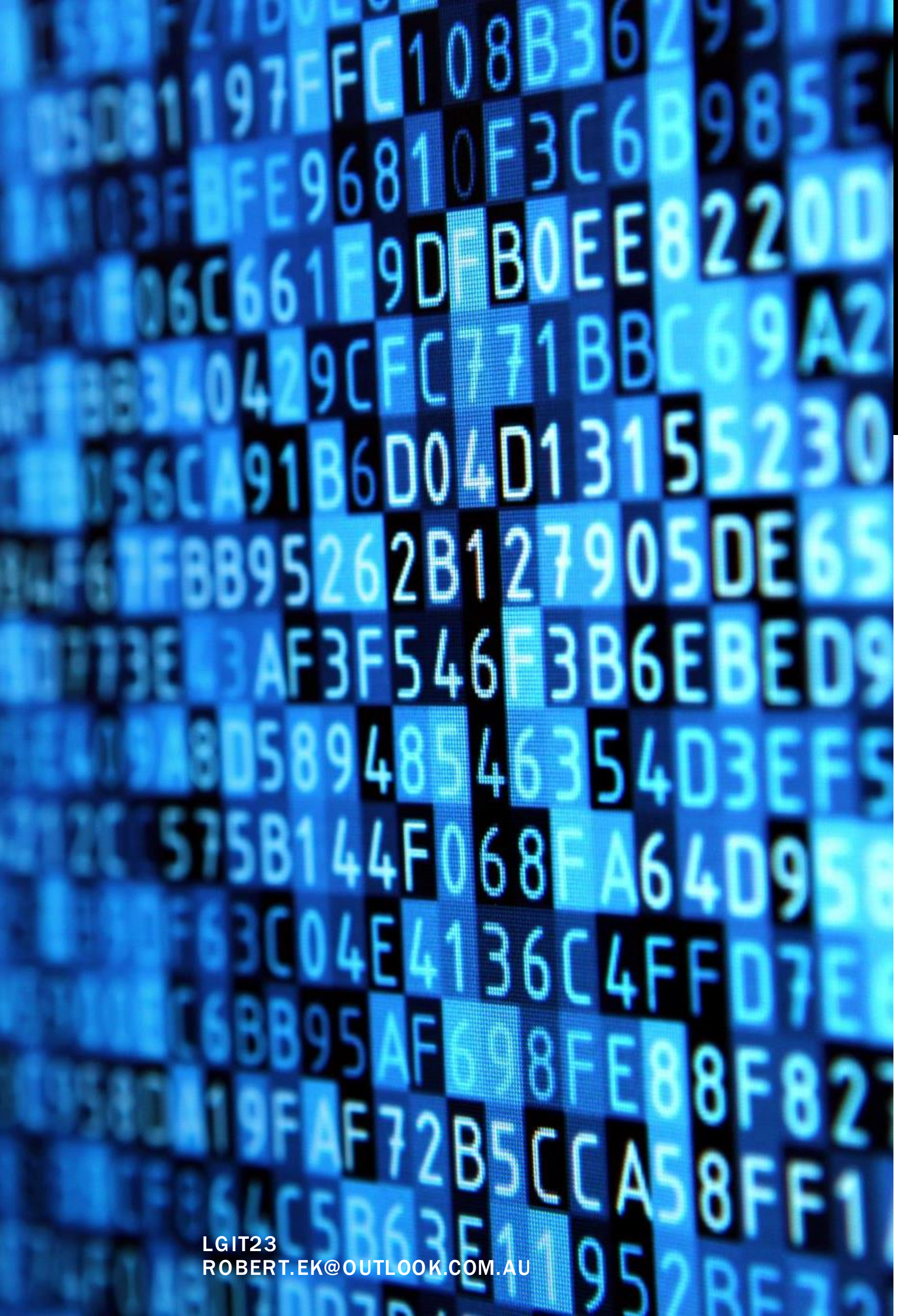
- Kaseya hack July ‘21 affected 50 MSPs and between 800-1500 businesses. One of largest security breaches in recent history
- SolarWinds n-Central hack in January ’20

MSPs should consider whether they continue to rely on RMM software.

MODERN ATTACKS ON ORGANISATIONS.

- 62% increase in ransomware attacks on financial institutions.
- 34% increase in number of reported phishing attacks.
- 300% increase in number of supply chain attacks. Who does the council interact with?

Sophos ENSIA, FBI, 2021/22



Impactful hacking stats (2022)

- 50% or all cyber-attacks are done on SMBs <100 staff. What about the other 50%
- 32%/65% - out of ransomware victims 32% pay, but only get 65% of their data back.
- 62% of incidents in the System Intrusion pattern involved threat actors compromising managers and partners.
- 77% of organisations do not have a cyber security incident response plan.

Sources: Purplesec, Cloudwards, Data Breach Investigation Report, Trend Micro, IBM, CSO.

WHY DO ATTACKS HAPPEN?

1. Lack of security awareness.
2. System vulnerabilities
3. Wrong risk assessment
4. Issues in the processes and negligence.
5. Your choice.

NEW SOUTH WALES LOCAL **COUNCILS – 2022 RISK LANDSCAPE AND WHAT LIES AHEAD**

Grant Thornton 14th Dec 2022 - NSW 128 local Councils

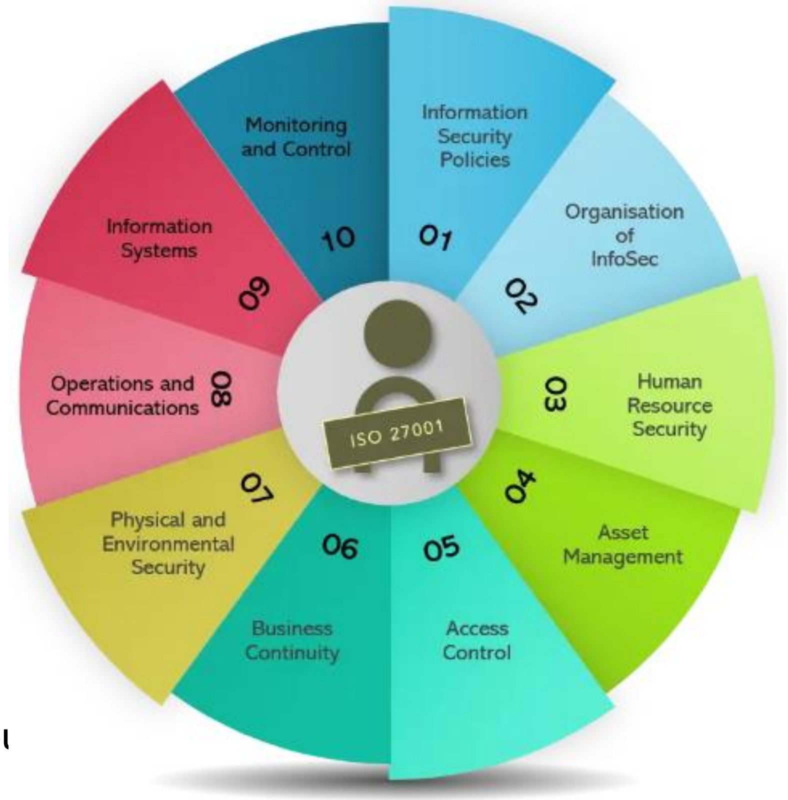
1. Talent retention and attraction
2. Cybersecurity and data governance
3. Environmental/natural disasters
4. Asset Management
5. Financial Stability

The skills gap has more than doubled since 2019.

In its Dec 2022 Cybersecurity Workforce study, ISC2 found that 3.4 million more skilled cybersecurity professionals are currently needed globally.

SO HOW DO YOU PROVIDE THE PROOF?

Become ISO 27001 Information Security Management System (ISMS) certified.



ISO 27001
01 Information Security Policies
02 Organisation of InfoSec
03 Human Resource Security
04 Asset Management
05 Access Control
06 Business Continuity
07 Physical and Environmental Security
08 Operations and Communications
09 Information Systems
10 Monitoring and Control

Information Security Management ISO 27001 Certified

AND..... WHAT DOES THIS MEAN?

Having the ISO27001 ISMS certification in place is a critical component for both your council profile as well as your financial stability.

When achieved you can broadcast this achievement to all your residents and supply chain. You can prove that you now have the International Best Practice for security on all levels in place protecting you, them and your supply chain.

Information Security Management
ISO
27001
Certified

UH OH - INSURANCE

Here is the good news from the ‘Council of Insurance for Agents and Brokers’ – average increase in cyber insurance prices fell below 10% for the 1st time in 10 quarters in the 1st qtr. 2023.

Uh oh – a Panseer survey states that 82% of global insurers expect the rise in cyber insurance premiums to continue.

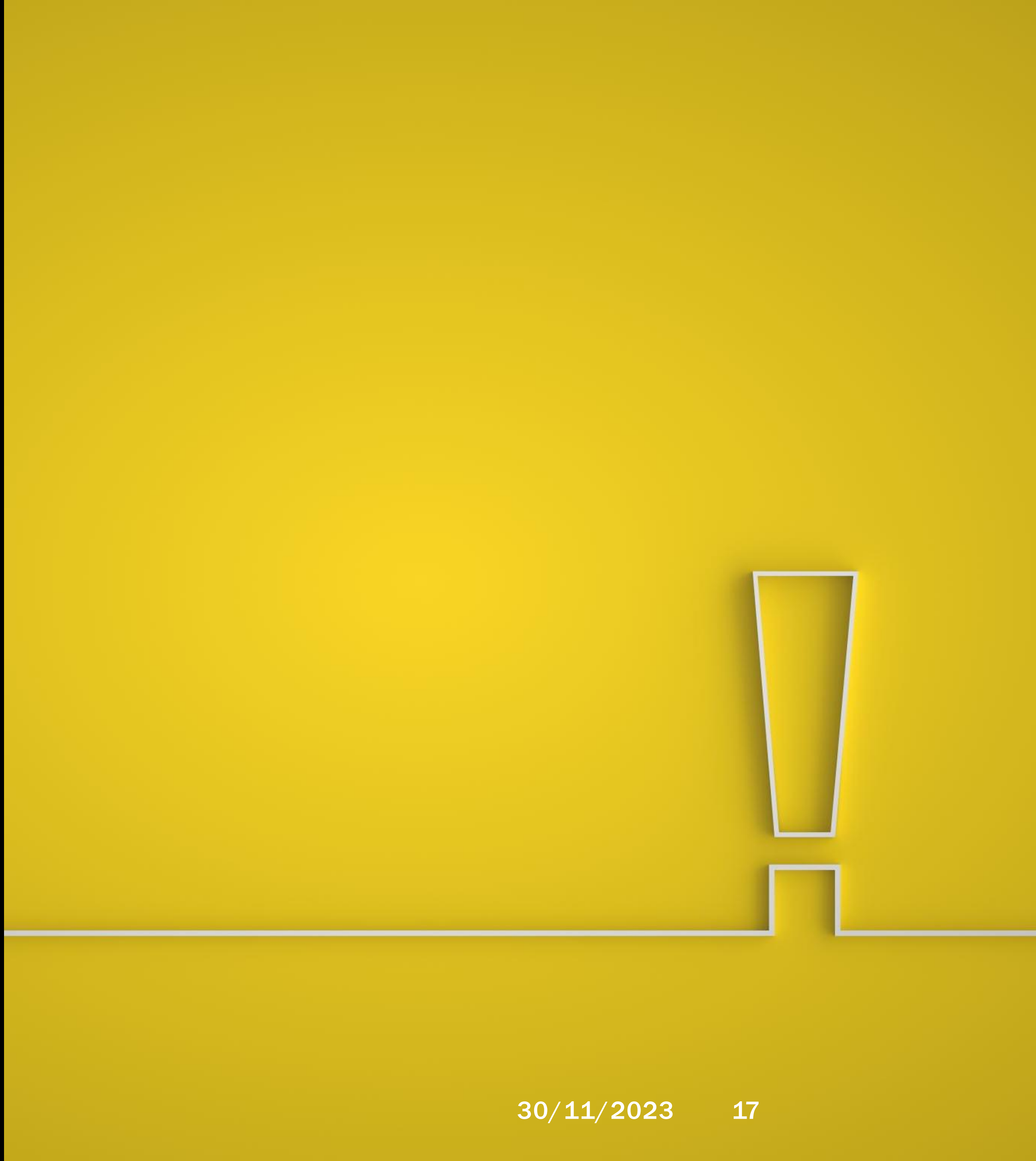
Plus, their questionnaires have become intense.

Great for the insurance guys but sucks for us. *However, if you can show them your 27001 Certification all the questions can disappear, and premiums drop.*

GOVT REGULATIONS ARE GETTING STRICTER BY THE MONTH.

In the USA you now need to advise their regulatory body if you have been breached within 4 days. If not, heavy fines apply, and your reputation gets smashed. The same will happen here.

Australia's new Cyber Security Strategy. Announced Dec 2022. Expert Advisory Board appointed as development of new Cyber Security Strategy begins (homeaffairs.gov.au)



OK SO WHAT NEXT?

My suggestion is that you become ISO27001 certified

- So that the Council stays trusted and safe.
- Plus, maintain resident and supply chain data securely.
- Plus, introduce ISO to the Council as an ongoing process. A security aware culture.
- Plus, better, Insurance Premiums

ISO27001 PROJECTS

1st ISO project I did was clunky and very manual and annoying and took quite some time to achieve.

I then had a good look at about 50 International ISO27001 platforms.

Resulted in other ISO projects not being clunky providing a clear intuitive path through the process.

WHAT NEEDS TO BE DONE

- Develop a project plan.
- Perform an independent risk assessment.
- Design and Implement controls based on your security roadmap.
- Document what you are doing.
- Monitor and remediate.

HOW DO YOU DO THIS?

- Get a coach.
- Do a Security Audit by independent specialised firm.
- Choose an intuitive platform.
- Choose Certification firm.

THE 9 PROJECT MANAGEMENT TIPS. (FIRST 5)

- Secure executive buy-in in the beginning – may need a presentation by coach to the executive team.
- Hire the outside security audit expert to conduct a gap analysis.
- Appoint a Project Leader.
- Be careful about scoping the ISMS.
- Establish a risk management framework that meets the requirements of ISO27001.

THE 9 PROJECT MANAGEMENT TIPS. (CONTINUED - NEXT 4)

6. Break down control implementation work into smaller pieces.
7. Map existing controls to ISO27001 requirements.
8. Document items as you go so preparing the risk treatment plan and statement of applicability (SOA) takes less effort.
9. Consider scheduling multiple audits at the same time.

IS THIS GOING TO COST YOU A FORTUNE?

No.

I coach organisations getting their ISO27001 done.

I will show you how and assist with minimal involvement as the components are all in place and ready for you if you need them.

One of them is an intuitive platform to work on and is easily maintained. + Independent Security audit + National Certifiers.

Information Security Management ISO 27001 Certified

YOUR VALUE WITH YOUR RESIDENTS AND SUPPLY CHAIN WILL …….

BIGGEST MISTAKES WITH ISO27001?

1. Not having a coach.
2. People writing too many documents on policies and procedures – as just having good quality policies and procedures will not control your risks.

Well trained competent and motivated people will help you control and manage your risks.- ISO27001 is continuous.

YOU WILL HAVE THE PROOF

You will be valued – *as you will have high standards along with the* *__credibility of being certified.__*

Information Security Management ISO 27001 Certified

Why do it?

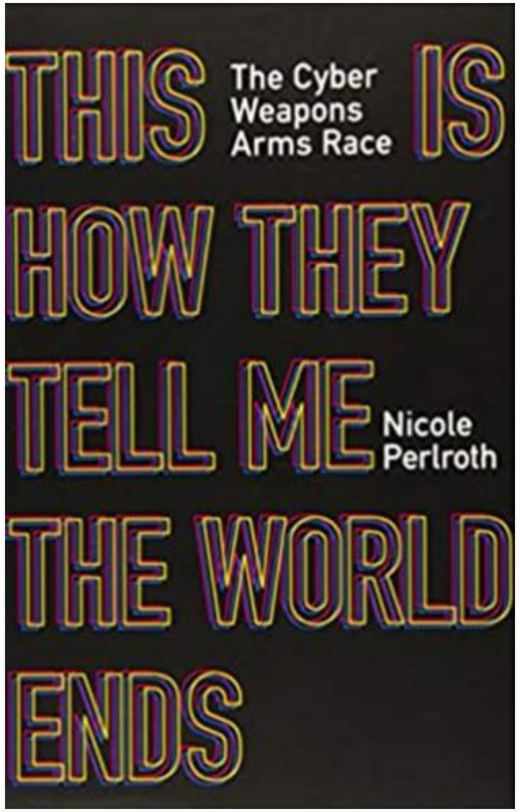
Be	Your council will be far more secure.
Have	Your council will have far better processes and procedures.
Keep	You will continue to keep your internal standards high.
Engaged	Your fellow workers will be engaged with your security and learn.
Budgets	Your finance team will be less stressed, and budgets will be met.
Complete	Complete security.

THANKS FOR LISTENING AND THANKS TO SMBIT

IF YOU WOULD LIKE TO FIND OUT MORE, PLEASE FEEL FREE TO HAVE A CONVERSATION.

YOU CAN CONTACT ME VIA EMAIL @ robert.ek@outlook.com.au

BKB - BUILDING KNOWLEDGEABLE BUSINESSES.



THIS IS HOW THEY TELL ME THE WORLD ENDS
The Cyber Weapons Arms Race
Nicole Perlroth

Great Christmas read.

Paula Januszkiewicz | CQURE – https://cqureacademy.com

ADVANCED WINDOWS SECURITY COURSE
ARE YOU READY TO OUTPERFORM IN 2024?
CQURE
ACADEMY

Paula did 6 live hacks in 1 hour in Melb 1 month ago at a national conference of Managed Services Providers ☹