
ISO27001:2022
A new era is dawning for ISO27001.
Are you ready for it?
BY GARY HIBBERD

What?!

ISO27001 is changing in 2022. What do you need to know?

By Gary.Hibberd@ConsultantsLikeUs.com

INTRODUCTION

THE TIME HAS COME FOR 27001 TO CHANGE

There is little doubt that ISO27001 is an important standard in the world of Information Security and Data Protection.

It has been around for some considerable time, with its origins lying in Government Security Standards, through to becoming a commercially accepted British Standard (BS7799-1) and finally, an International Standard (ISO27001:2005).

Although there were some minor changes in 2017, it hasn't seen a major update or release since 2013..

.Until now.

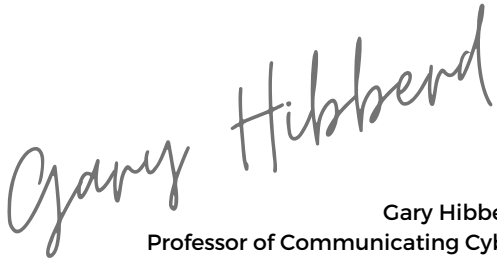
Set to be released by March 2022, the new standard is as close to a 're-write' as you can imagine. Therefore, I'm here to say to you that you shouldn't be fooled into thinking this is going to be a walk in the park. It's a significant change.

Consider this your 'primer' and your 'call to action'.

If you want to 'cut to the chase', then I suggest you do these two things;

- Get in touch with me and I'll guide you on what needs to be done
- Read the standard for your self, and make a plan.

Either approach is good. Just don't ignore it.



Gary Hibberd
Professor of Communicating Cyber


What you
need to
know!

STANDARD NUMBERS

Want to look like an ISO27001 rockstar? Here are the headlines you need to be aware of in relation to the new standard.

4

Clauses

These Clauses are;

5. Organizational Controls (37 Controls)
6. ·People Controls (8 Controls)
7. ·Physical Controls (14 Controls)
8. ·Technological Controls (34 Controls)

Gary.Hibberd@ConsultantsLikeUs.com

STANDARD NUMBERS

93

Controls

Reduced from the current 114 in Annex A

Gary.Hibberd@ConsultantsLikeUs.com

STANDARD NUMBERS

11

New Controls

5.7 - Threat intelligence
5.30 - ICT Readiness for Business continuity
5.23 - Information security for use of cloud services
7.4 - Physical security monitoring
8.9 - Configuration management
8.10 - Information deletion
8.11 - Data Masking
8.12 - Data Leakage Prevention
8.16 - Monitoring Activities
8.23 - Web filtering
8.28 - Secure coding

Gary.Hibberd@ConsultantsLikeUs.com

STANDARD NUMBERS

58

Updated Controls

Introduction of 'attributes' for each control, and a focus on 'purpose', instead of 'objective'.

Atrribute types;

- Control Type
- Information Security Properties
- Cybersecurity concepts
- Operational Capabilities
- Security Domains

Gary.Hibberd@ConsultantsLikeUs.com

STANDARD NUMBERS

24

Merged Controls

Organisations will need to see how their current controls can be merged and evidenced in the new standard.

Gary.Hibberd@ConsultantsLikeUs.com


Need some help?

ISO27001

BRACE YOURSELF...
THE 27001 EXPERTS ARE COMING!

Do you remember what LinkedIn was like back in 2017 and 2018? It was crammed packed full of GDPR (General Data Protection Regulation) Gurus!

It seemed as though you could open a window (virtual or real) and throw a rock, and you would hit a GDPR expert!

Everyone from Marketing companies and business coaches to IT Companies were proclaiming themselves as the saviours of your business in the face of this new 'terrifying' regulation.

But come 26th May 2018, they all disappeared!

Gary.Hibberd@ConsultantsLikeUs.com

ISO27001

BRACE YOURSELF...
THE 27001 EXPERTS ARE COMING!

I have a feeling we're about to see them reappear in the guise of ISO27001 'transformation' and 'transitional' experts, as this new standard begins to dominate headlines in 2022.

Of course, I could be wrong... but I'm already seeing more and more companies proclaiming to be ISO27001 'specialists', yet have no credentials or experience to back this up.

I've created a short checklist for you to follow so that you can separate those who claim to be specialists (aka 'experts') from those who know what they're doing.

Gary.Hibberd@ConsultantsLikeUs.com

27001 CHECKLIST
GETTING HELP

INSTRUCTION: There are a lot of Consultants and companies willing to help. But here's a nice checklist for you, so you know what you're getting and who might land you in hot water (remember; Snake oil is cheap, but intoxicating stuff!)

Ask these questions and score them 0 (VERY Bad) to 10 (Excellent!).

- [ ] HOW MANY ISO27001 IMPLEMENTATIONS HAVE YOU PERSONALLY COMPLETED?

Hint: Knowing is not the same as 'doing'. Many people will 'know' the standard, but what practical experience do they have?

27001 CHECKLIST

- [ ] HOW LONG HAVE YOU BEEN WORKING WITH ISO STANDARDS?

Hint: As before, the more experience someone has with security standards, the better and easier it will be for you.

- [ ] WHAT EXPERIENCE HAVE YOU IN TRANSITIONING ORGANISATIONS FROM ONE ISO TO ANOTHER?

Hint: This is a significant change, and so it would be great to have someone onboard who knows how to plan this for you.

Have they done it before? What went well? what didn't?

27001 CHECKLIST

- [ ] HOW WOULD YOU GO ABOUT CONDUCTING THE TRANSITION?

Hint: Look for a simple approach that is relevant to you and your business. This is a complex change, but it still doesn't need to be complicated!

- [ ] WHAT IS YOUR EXPERIENCE OF OTHER FRAMEWORKS AND REGULATIONS, LIKE NIST, SANS, DPA2018 & GDPR?

Hint: There are many forms of good and best practice in relation to Information Security. Having someone on board to help you, who has knowledge and experience in GDPR, Data Protection and other security frameworks will be a great benefit to you.

FINALLY!

Remember, there is no need to panic! There will be a transition period of around two years to the new standard.

Only people who should be getting excited, are Security Consultants like me (and I'm VERY excited about it!)

But you do need a plan! Don't leave this until the last minute.

If you are already certified, speak to your auditor about this new standard at your next Surveillance Audit.

They can guide you.

If you're just starting out on the journey, then follow the current ISO27001:2013 standard ask the person guiding you how you can prepare for the new version.

If they can't guide you... Please get in touch and I'll be happy to be your guide.

HAVE QUESTIONS?

You can contact me at
gary.hibberd@consultantslikeus.co.uk

HTTPS://WWW.LINKEDIN.COM/IN/GARYHIBBERD/


Good luck!