SUPPORTING DATA SECURITY IN YOUR BUSINESS – HELPING YOU TO ADOPT ISO 27001 STANDARDS

ISO 27001

Definition: “*ISO/IEC 27001:2013 (also known as* ***ISO27001****) is the international standard that sets out the specification for an Information Security Management System (ISMS). Its best-practice approach helps organisations manage their information security by addressing people and processes as well as technology*” (IT Governance, 2021, p.1).

History and Context: In common with all ISO standards, ISO 27001 is voluntary, but certification can be achieved. ISO 27001 was developed over a number of years in conjunction with the ISO/IEC *Joint Technical Committee* known as JTC 1, who have produced a number of standards over the years reflecting the rapidly chaining information security environment.

Protect Against Cyber Attack: Many national governments have recognised the crucial role that data security plays in organisational functionality and strategy. The devastating ‘wannacry’ ransomware attack on the NHS in 2017 (Chen and Bridges, 2017, p.455) illustrated how dangerous it can be to have weak IT security control. Several other large commercial organisations have also fallen prey to hackers and scammers, highlighting the critical necessity of IT security processes and controls for simple day-to-day operations.

GPDR: In 2018, after very considerable consultation the General Data Protection Regulations – GPDR – were formally enacted. A pan-European Regulation which remains in force post-Brexit requires that all businesses which handle personal data can demonstrate robust integrity and security measures (ISO, 2020, p.1). Fines for breaches of GDPR are punitive, and so even if the executive board remain unconvinced by IT security risk, at the very least there is a business case for ISO 27001

WHY DATA SECURITY MATTERS

Build Good Customer Relationships: A survey conducted by IT Governance (2020, p.1) found that increasing numbers of clients are asking for evidence of data security protocols – 68% of clients of the firms surveyed asked to see evidence of ISO 27001 (***Fig. 1***).

Strengthen the Supply Chain: Data has become integral to supply chains for all types of business. More than 44% of organisations now expect their suppliers to show evidence of data security.

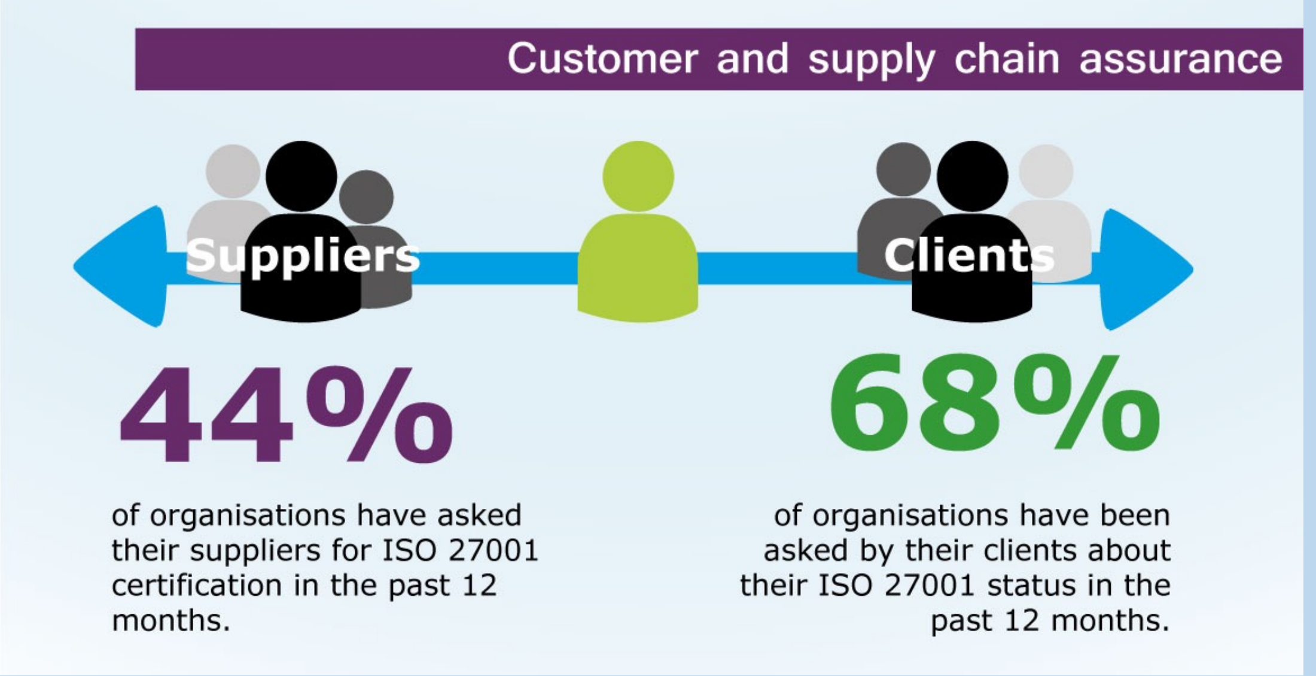

Fig. 1 *ISO 27001 Provides Supply Chain Assurance*

MAIN BENEFITS OF ISO 27001 TO YOUR BUSINESS

The Main Benefits

ISO27001 is designed to help businesses ensure that they have controls in place to manage data security. With more data than ever before, and increasing numbers of staff working remotely, data integrity and security has neve been more important. The risks of a failure to ensure data is secure are considerable. Breach of GDPR regulations, loss of sensitive commercial data and reputational damage to name just three (***Fig. 2***). Let us help you begin the process of ISO 27001 implementation today to ensure that you have the right controls in place to keep your data secure.

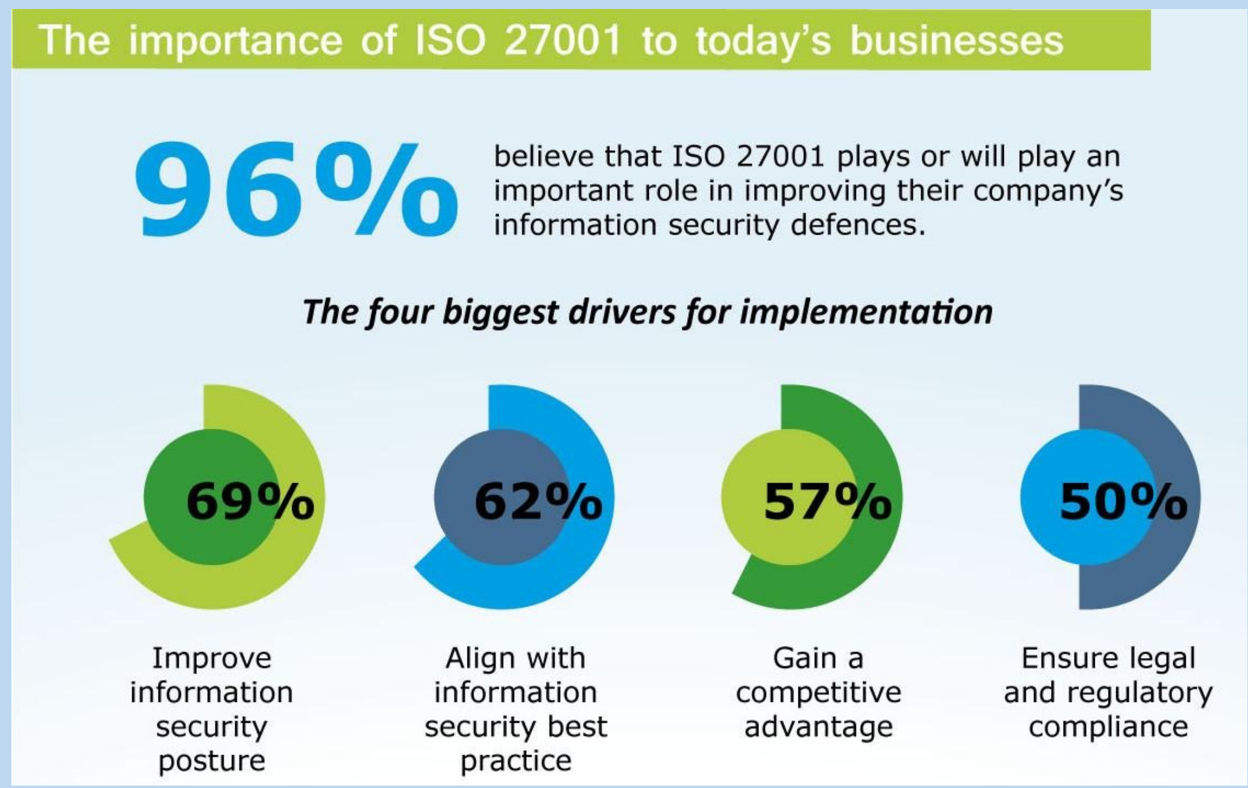

Fig. 2 *Importance of ISO27001 for Today’s Business*

ISO 27001 can potentially:

- ❖ Significantly increase data security, reassuring clients and suppliers and supporting confidential and commercially sensitive information
- ❖ Ensure that best practice has been adopted – the world of IT security moves fast and ISO 27001 can help you stay ahead
- ❖ Reduce costs associated with data management and containment of breaches
- ❖ Secure competitive advantage, demonstrating a proven commitment to data security
- ❖ Encourage a process driven mindset within the organisation which increases efficiency for routine tasks
- ❖ Ensure legal and regulatory compliance – which can in some circumstances positively impact insurance premiums because you are seen as a reduced risk

Research Evidence of ISO 27001 Benefits

Empirical evidence gathered from current academic research shows that:

- Positive relationship between implementation of ISO 27001 and organisational performance, but costs take longer to payback than anticipated (Hsu et al., 2016, p.4842)
- When paired with other IT/IS tools such as PDCA the positive effects of ISO2700 are magnified (Velasco et al., 2018, p.298)
- In a study of 152 firms, ISO 27001 was proven to be the most effect framework for ensuring GDPR compliance (Lopes et al., 2019, p.5).

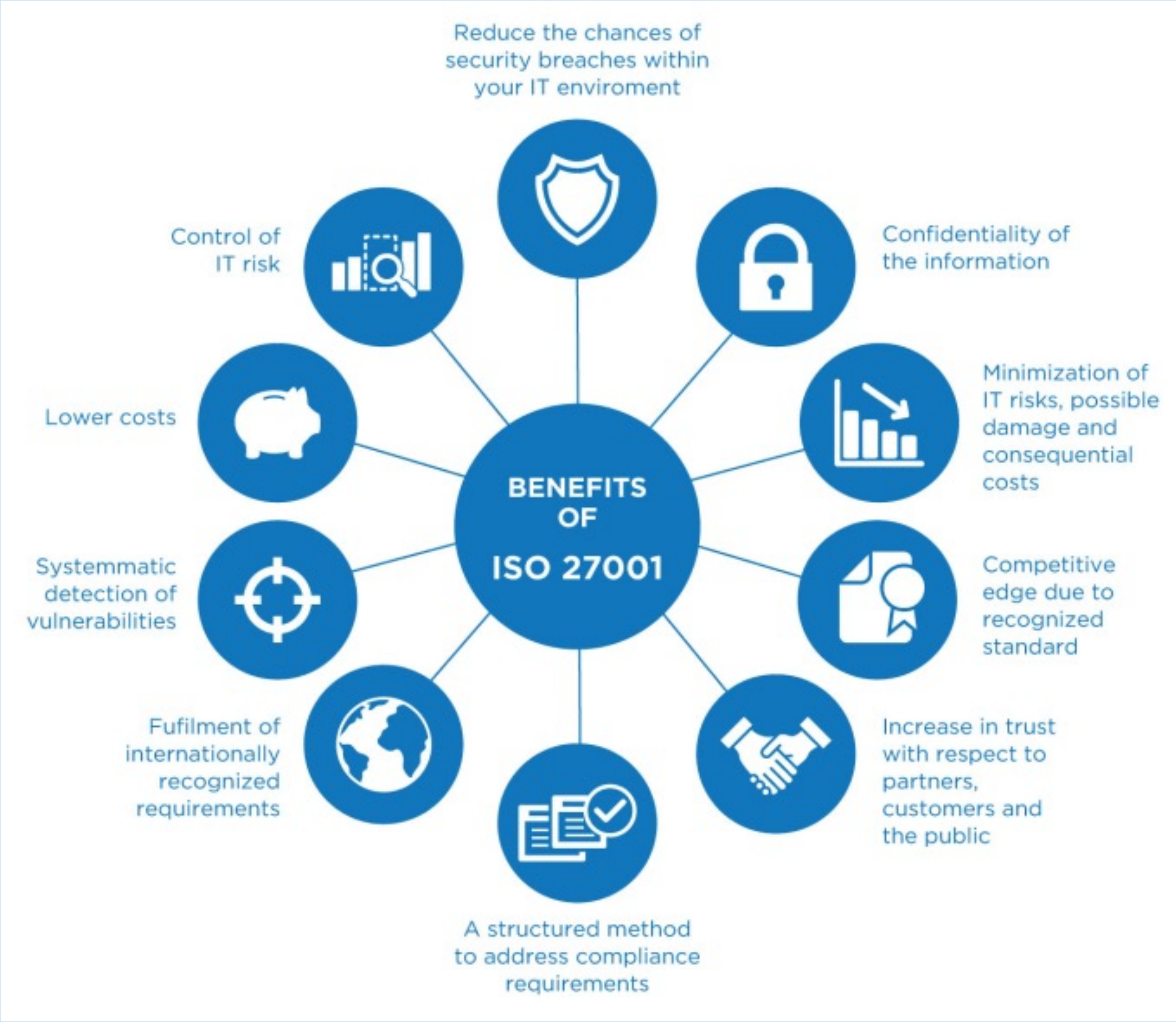
Reduce the chances of security breaches within your IT enviroment
Confidentiality of the information
Minimization of IT risks, possible damage and consequential costs
Competitive edge due to recognized standard
Increase in trust with respect to partners, customers and the public
A structured method to address compliance requirements
Fufilment of internationally recognized requirements
Systemmatic detection of vulnerabilities
Lower costs
Control of IT risk
BENEFITS OF ISO 27001

Fig. 3 *Benefits of the ISO 27001 Standard*

SUGGESTIONS FOR IMPLEMENTATION

Focus on: (1) process control; (2) building competitive advantage through increased efficiency and risk reduction; and (3) strengthening stakeholder/supply chain relationships.

Recommendations

1. **Conduct a full IT security and process review.** Undertake a top-to-bottom review of IT and data security protocols – use white hat hackers if deemed appropriate
2. **Establish where process improvements can be made internally.** Engage employees in establishing data security improvements – especially behavioural ones such as sharing passwords and emailing data to personal accounts for ‘catch-up’ work. The intentions may be good, but this can be dangerous.
3. **Collaborate with suppliers to improve data security protocols.** Work with suppliers to ensure that any data exchange is not the ‘weak link’ in your data security protocols – highlight the benefits to suppliers to secure buy-in
4. **Publish internally evidence of improvements to data security** . Share improvements and business gains internally to sustain momentum.
5. **Continually monitor and review.** Continually monitor and review to ensure that best practice is being followed.

REFERENCES

Chen, Q. and Bridges, R.A., 2017, December. Automated behavioral analysis of malware: A case study of wannacry ransomware. In *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)* (pp. 454-460). IEEE.

Hsu, C., Wang, T. and Lu, A., 2016, January. The impact of ISO 27001 certification on firm performance. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 4842-4848). IEEE.

ISMS Online. *2021. Why is ISO 27001 Important?* [online][https://www.isms.online/iso-27001/4-key-benefits-of-iso-27001-implementation/] accessed 2nd Feb 2021.

ISO. 2021. *Information Security*. [online] [https://www.iso.org/isoiec-27001-information-security.html] accessed 2nd Feb 2021.

IT Governance. 2020. *ISO 27001 Challenges and Drivers.* [online][https://blog.itgovernance.co.uk/blog/iso-27001-infographic-challenges-and-drivers?] accessed 2nd Feb 2021.

IT Governance. 2021. *What is ISO 27001?* [online] [https://www.itgovernance.co.uk/iso27001.] accessed 2nd Feb 2021.

Lopes, I.M., Guarda, T. and Oliveira, P., 2019. Implementation of ISO 27001 standards as GDPR compliance facilitator. *Journal of Information Systems Engineering & Management*, *4*(2), pp.1-8.

Velasco, J., Ullauri, R., Pilicita, L., Jácome, B., Saa, P. and Moscoso-Zea, O., 2018, November. Benefits of implementing an ISMS according to the ISO 27001 standard in the ecuadorian manufacturing industry. In *2018 International Conference on Information Systems and Computer Science (INCISCOS)* (pp. 294-300). IEEE.