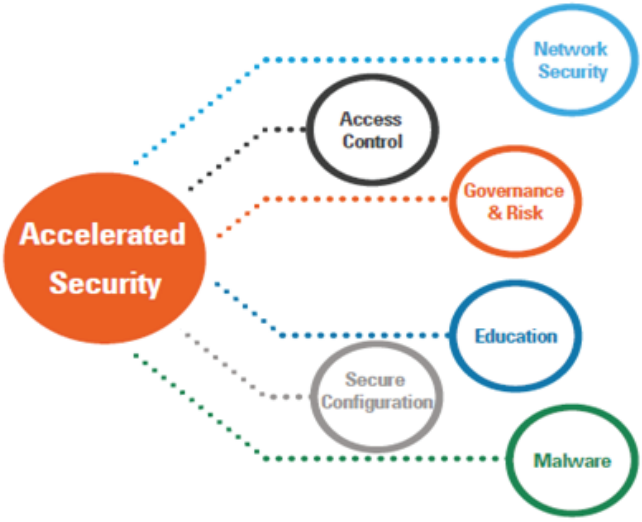
KPMG

Fast-track to cyber security

ACCELERATED SECURITY

Cyber attack is often viewed as a risk which only affects high-profile, asset-rich businesses, but as traditional targets for cyber attack enhance their protection, attackers are increasingly focusing on organizations with a lower level of cyber maturity. Furthermore, many governments and businesses demand that their suppliers and partners engage in cyber security best practice. Regardless of industry or size, all organizations are potential victims and must endeavor to develop strong, resilient cyber defenses.

According to the UK Government's Department for Business, Innovation and Skills, 60% of small firms were hit by Cybercrime in 2013 alone. Research by the Federation of Small Business (UK's leading business organization representing small and medium sized businesses) identified that nearly a third of businesses wouldn't know what to do if they had a security breach with 40% saying they would struggle to recover all lost data.



What is a Accelerated Security?

The Accelerated Security service is designed to help small and mid-tier companies to protect themselves from cyber attack, through a series of cyber pre-packaged defense controls that don't require significant IT resources to implement.

KPMG will help Accelerated Security clients to implement policies, procedures and tools which will help the organization to develop basic cyber defenses.

"Any organization that holds valuable data is a target for hackers, which can be hard to stomach for a business that has previously stayed below the radar. This realization can leave some companies struggling to achieve their aspirations without feeling exposed to cybersecurity risk – a concern our new package addresses."

What's on your mind?

- **How do I effectively manage** cyber risk, in proportion to the risk to my organization?
- **How do I make** our employees our first line of defense?
- **How can I be confident** that our systems and devices are secure?
- **How can I demonstrate** to our customers that we are managing cyber security appropriately and not exposing them to risk?
- **How can I ensure** our management of cyber security is effective, appropriate and in-line with best practice?

Potential benefits to you

- Alignment with 'Cyber Essentials' and the '10 Steps to Cyber Security', demonstrating a commitment to managing cyber risk to customers and stakeholders.
- Confidence that the appropriate cyber security controls have been selected and implemented in line with industry best-practice and expert advice.
- Choice between a six domain 'Cyber Essentials' package or a 10 domain 'Accelerated Security' package, allowing you to choose the level of protection that your business needs.
- Exceptional Value – A complete package of basic cyber controls, implemented quickly and for a fixed price.

We focus on the areas important to you

The development of Accelerated Security has drawn on the knowledge of a combination of KPMG specialists in information protection, technical security, risk infrastructure, organizational design, user education and security operations. These combined skills have been utilized to create an approach which is designed to respond to the cyber threats your organization faces every day. The areas and the materials we offer are as follows:

01 | Governance & Risk

- Build a framework for the governance of Information Security.
- You can manage risks effectively and in line with organizational risk appetite.
- Report on the existing risk position in a clear and concise format.

02 | Network Security

- Implement a Network Security Policy.
- Set standards for secure network design and operation.
- You can manage and track the operation of network security controls.

03 | Education & Awareness

- Educate users about their responsibilities.
- Maintain awareness of security risks, trends and issues within the organization and sector.
- Deliver Information Security training.

04 | Malware Defense

- Implement a policy to support the prevention of malware infection within the organization.
- Define an effective process for the detection and management of malware incidents.
- Support understanding of malware risk and the controls required to manage it.

05 | Secure Configuration

- Enabling IT assets to be configured securely and do not present an unacceptable risk.
- Implement the correct secure technical configurations for a range of devices and systems.
- You can manage and track the process of device configuration.

06 | Access Controls

- The definition of the access requirements of users within the organization.
- You can manage access to systems in line with leading practice.
- You can manage passwords appropriately and securely.

Contact us:

Diveane Bowe
Partner
Audit and IT Advisory Services

T: +1 (242) 393-2007
E: dbowe@kpmg.com.bs

Shavonne Thompson
Senior Manager
IT Advisory Services

T: +1 (242) 393-2007
E: slthompson@kpmg.com.bs

kpmg.com.bs **kpmg.com/app**