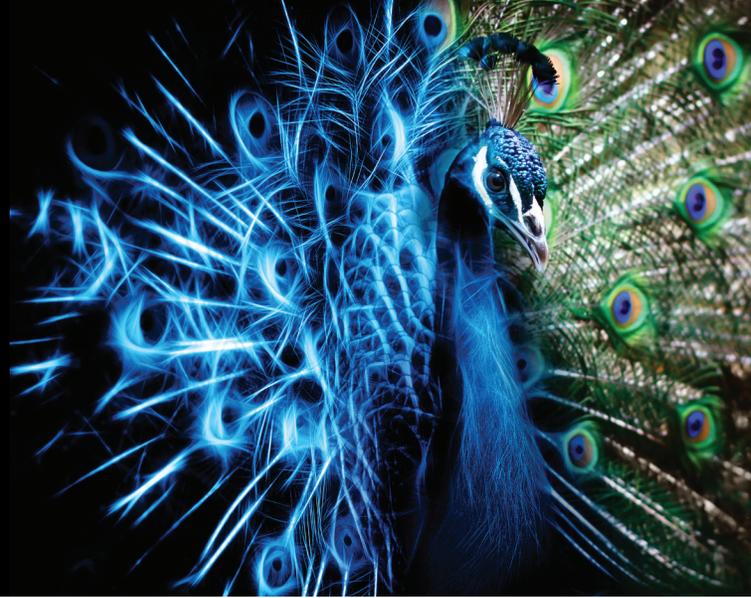




# Feel free to flourish

## CYBER MATURITY ASSESSMENT



Organizations are subject to increasing amounts of legislative, corporate and regulatory requirements to show that they are managing and protecting their information appropriately. Simultaneously, the threats from cyber criminals and hacktivists are growing in scale and sophistication. Organizations need to continually evolve their cyber security architecture to respond to the changing digital environment. By working with your team we can help you take a positive approach to managing cyber risk. This can enable you to take control of uncertainty and turn the digital environment into a genuine strategic advantage.

The cyber security landscape and associated threats are not something new – the speed of evolution is what is changing. The focus on cyber security is increasing rapidly due to many high profile and highly disruptive/damaging security breaches threatening financial and physical damage across critical national and corporate infrastructures.

It is also increasingly common for government buyers and large corporates to demand confidence in information management as a qualifier for lucrative contracts or partnerships. With the stakes so high, organizations must decide on their cyber risk appetite and how they will respond. There is a significant responsibility on executives to assure customers, stakeholders and employees that appropriate cyber security architecture is in place. We can work with you giving you the advice and challenge you need to make decisions with confidence.

### What is a Cyber Maturity Assessment?

KPMG’s Cyber Maturity Assessment (CMA) provides an in-depth review of an organization’s ability to protect its information assets and its preparedness against cyber threats.

We believe that it is unique in the market in that it looks beyond pure technical preparedness for cyber threats. It takes a rounded view of people, process

and technology to enable clients to understand areas of vulnerability, to identify and prioritize areas for remediation and to demonstrate both corporate and operational compliance, turning information risk to business advantage.

In developing the assessment, KPMG has combined international information security standards with global insight of best practice in risk management, cyber security, governance and people processes. The approach addresses six key dimensions at three levels of maturity that together provide an in-depth view of an organization’s cyber maturity, as shown below.

#### Leadership and Governance

Board demonstration of due diligence, ownership and effective management of risk

#### Human Factors

The level and integration of a security culture that empowers and helps to ensure the right people, skills, culture and knowledge

#### Information Risk Management

The approach is designed to achieve effective risk management of information throughout the organisation and its delivery and supply partners

#### Business Continuity and Crisis Management

Preparations for a security event and ability to prevent or reduce the impact through successful crisis and stakeholder management

#### Operations and Technology

The level of control measures implemented to address identified risks and reduce the impact of compromise

#### Legal and Compliance

Regulatory and international certification standards as relevant

## What's on your mind?

**Do I need help assessing** whether the mechanisms to manage our risks are mature?

**Am I looking to create** a stronger security culture within my organization?

**Do I need a better understanding** of whether I comply with the varied regulatory requirements?

**Am I looking to take greater control**, ensuring that my organization is prepared for the evolving cyber security landscape?

**What should I be considering** as part of a cyber security strategy?

## Our approach

Working with your team and conducting a combination of interviews, workshops, policy and process reviews and technical testing, KPMG's IT Advisory team takes a positive view to managing cyber security, and the program rapidly:

- Identifies current gaps in compliance and risk management of information assets;
- Assesses the scale of cyber vulnerabilities;
- Sets out prioritized areas for a management action plan.

The assessment provides the flexibility to assess the level of cyber maturity on a site by site basis or at a company level. It helps to identify best practice within an organization and provides comparative information against peer groups and competitors.

In turn, allowing businesses to feel free to navigate the cyber security landscape and achieve their business aspirations.

Contact us:

**Diveane Bowe**  
Partner  
Audit and IT Advisory Services

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

[kpmg.com.bs](http://kpmg.com.bs)

[kpmg.com/app](http://kpmg.com/app)



© 2016 KPMG Advisory Services Ltd., a Bahamian limited company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

## WE BELIEVE CYBER SECURITY SHOULD BE ABOUT WHAT YOU CAN DO – NOT WHAT YOU CAN'T

### WHY KPMG?

#### INDEPENDENT

KPMG is not tied to any technology or software vendor. Our recommendations and technical strategies are based solely on what is fit and appropriate for your business.



#### COLLABORATIVE

We facilitate and work with collaborative forums with the aim of bringing together the best minds in the industry to collectively solve shared challenges.



#### TRUSTED

KPMG member firms have a long list of certifications to work on engagements for the world's leading organizations.



#### GLOBAL, LOCAL

KPMG is a global network of member firms with over 174,000 people working in 155 countries. We have over 2,000 security practitioners globally, giving member firms the ability to orchestrate and deliver to consistently high standards worldwide. KPMG's regional practices can service your local needs from information security strategy and change programmes, to low level technical assessments, forensic investigations, incident response, training and ISO27001 certification.

