



Building a better working world

# Cyber and privacy risk management

Responding to the Bermuda cyber and privacy regulatory requirements

## What we are seeing in the market

The cyber threat landscape is increasing and expanding. As we move to an experience-led economy powered by data, there is also an increased focus on data privacy, underpinned by rising customer expectations and increased regulatory scrutiny. The pace and scale of regulatory change over the last five years have greatly impacted organizations' approach to cyber and privacy risk management both locally and globally.

only **7%** of organizations would describe cybersecurity as enabling innovation; most choose terms such as "compliance-driven" and "risk-averse."

**86%** of organizations say that crisis prevention and compliance remain the top drivers of new or increased security spending.



2019 saw the **highest-ever** fines issued by privacy regulators; meanwhile, data breaches reported under the General Data Protection Regulation (GDPR) more than **doubled** over the prior year.

**6 in 10** businesses only consider cybersecurity after it's already too late.

# Bermuda regulatory landscape: what's changing?

## BMA Insurance Cyber Risk Management Code of Practice 2019

- ▶ The code sets out risk management principles and leading-practice standards to make sure that regulated insurers:
  - ▶ Establish a sound and robust cyber risk management program
  - ▶ Implement a minimum set of requirements for technical and business process controls
- ▶ Failure to comply with the provisions will be a factor taken into account when determining whether a licensed insurer is meeting its obligation to conduct business in a sound and prudent manner.
- ▶ Insurers must regularly assess cyber risks arising from their business model and implement higher standards than those outlined in the code, where leading practice warrants it.
- ▶ The BMA will assess compliance in a proportionate manner relative to the insurer's nature, scale and complexity.

## Personal Information Protection Act (PIPA), 2016

- ▶ The PIPA outlines the requirements for organizations that process personal information, as well as the rights granted to individuals regarding the use of their personal information by such organizations.
- ▶ This legislation, which follows international best practice, applies to all organizations, businesses and the government that process personal information in Bermuda.

## What does this mean for you?

### Board

What are we doing about cyber and privacy risk?

### Chief executive officer

Are our cybersecurity and data strategies aligned with our business strategy?

### Audit committee

Do we have the right IT and operational controls to address cyber and privacy risk?

### Chief compliance officer

Is the organization complying with the BMA's Insurance Cyber Risk Management Code of Practice? Are we compliant with data privacy regulation?

### Chief information security officer

Is there a cyber risk management program in place? Are responsibilities known? Are mature data governance and protection programs in place?

### Chief risk officer

Do we know our cyber vulnerabilities? Do we know our privacy risk? How are we managing them?

### Internal audit

Are controls documented? Do we have evidence of cyber defense and privacy compliance?

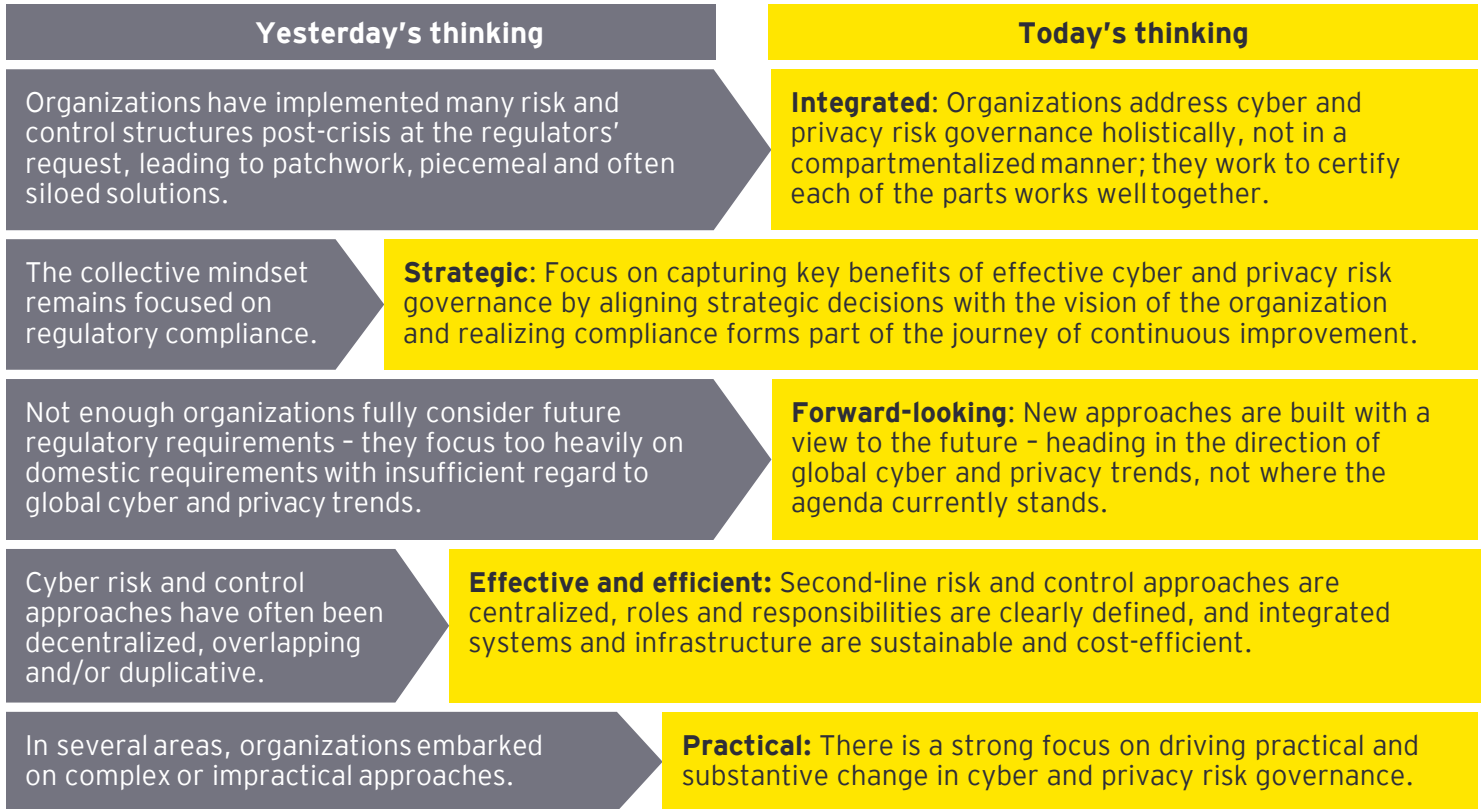
### Functional leads

Do I have the proper lines of defense for cyber and privacy?

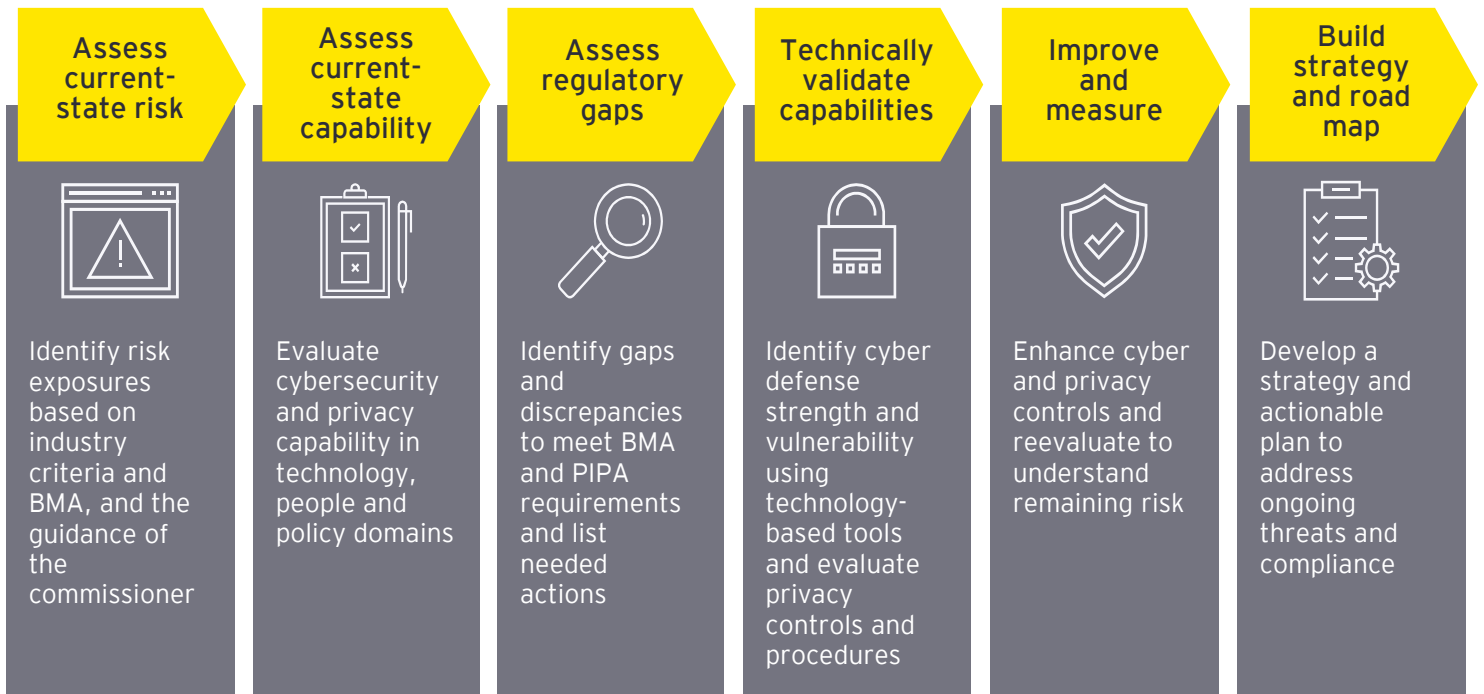


# An effective approach to compliance

A new mindset is required to meet new and broader regulatory expectations and to enable the drive for change in a way that delivers real value to the business.




## Mapping out your compliance journey



# EY's insights on the key areas to comply with BMA cyber regulation

Impacted area	Key considerations
 <p data-bbox="456 254 695 583">Governance and cyber risk management</p>	<ul data-bbox="722 296 1528 548" style="list-style-type: none"> <li>▶ Define and document <b>Cyber Risk Policy</b> and approve it with the board of directors at least annually</li> <li>▶ Appoint a <b>Chief Information Security Officer (CISO)</b> role to an appropriately qualified member of staff or outsourced resource</li> <li>▶ Develop a cyber risk plan and approve it with the board</li> <li>▶ Perform <b>regular cyber risk assessments</b> and retain the reports to be ready to be provided to the Authority upon request</li> </ul>
<p data-bbox="456 590 695 982">Cybersecurity</p>	<ul data-bbox="722 632 1502 940" style="list-style-type: none"> <li>▶ Develop a cyber incident management procedure, including incident identification, containment and reporting to the Authority</li> <li>▶ Perform staff cyber risk awareness trainings at least annually and adopt a <b>security-by-design</b> approach</li> <li>▶ Implement appropriate security controls to protect desktop, mobile and network devices</li> <li>▶ <b>Perform regular cybersecurity testing</b>, including penetration testing and vulnerability assessments</li> </ul>
<p data-bbox="456 989 695 1234">Third-party risk management</p>	<ul data-bbox="722 1010 1528 1213" style="list-style-type: none"> <li>▶ Identify and evaluate the risks associated with <b>third parties</b></li> <li>▶ Define contractual terms and conditions that would enable you to manage appropriate risks</li> <li>▶ Request for outsourced service providers to implement security policies, procedures and controls that are at least as stringent as the ones established within your own organization</li> </ul>
<p data-bbox="456 1241 695 1486">Data security</p>	<ul data-bbox="722 1262 1502 1451" style="list-style-type: none"> <li>▶ Classify the information you hold in terms of its sensitivity, value and criticality</li> <li>▶ Develop and implement a <b>data protection policy</b> including the requirements for data loss prevention, data retention, data sanitation and data backup in accordance with the data classification levels</li> </ul>
<p data-bbox="456 1493 695 1640">IT operations</p>	<ul data-bbox="722 1503 1528 1619" style="list-style-type: none"> <li>▶ Document and implement the following processes to ensure the ongoing security and stability of <b>IT operations</b>: change management, incident management, access management, patch management, security events logging and monitoring</li> </ul>
<p data-bbox="456 1646 695 1772">Cloud security</p>	<ul data-bbox="722 1667 1458 1751" style="list-style-type: none"> <li>▶ Assess the risks of the use of <b>cloud environments</b> and implement appropriate controls to address identified risks depending on cloud architecture</li> </ul>
<p data-bbox="456 1778 695 2022">Business continuity</p>	<ul data-bbox="722 1839 1490 1965" style="list-style-type: none"> <li>▶ Develop and implement <b>business continuity planning (BCP)</b> and <b>disaster recovery (DR)</b> planning policies and procedures</li> <li>▶ Perform regular tests of BCP and DR plans to ensure the recovery and availability of the systems</li> </ul>

# EY's insights on the key areas to comply with the PIPA regulation

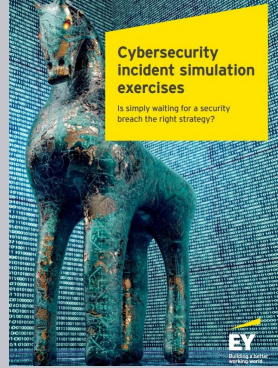
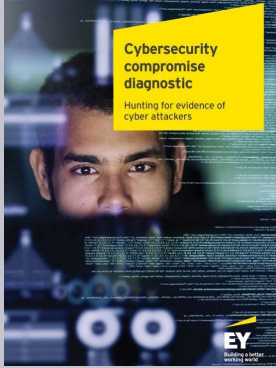
Impacted area	Key considerations	
	<b>Data protection policy and data classification</b>	<ul style="list-style-type: none"> <li>▶ <b>Classify</b> personally identifiable information (PII)</li> <li>▶ Develop <b>mechanisms</b> to enforce policies and standards</li> </ul>
	<b>Privacy risk and controls</b>	<ul style="list-style-type: none"> <li>▶ <b>Integrate privacy controls</b> in existing control framework and risk assessments</li> <li>▶ Conduct <b>risk assessments</b> on processes and data flows</li> </ul>
	<b>Data life cycle management</b>	<ul style="list-style-type: none"> <li>▶ <b>Maintain data flows</b> and privacy register</li> <li>▶ Document conditions for processing (i.e., legal ground, data minimization, information provision, purpose limitation)</li> </ul>
	<b>Data subject rights</b>	<ul style="list-style-type: none"> <li>▶ Set up procedures to support <b>rights of data subjects</b>, i.e., to access, modify and erase their PII; transfer PII to another organization (data portability); and object to the processing</li> </ul>
	<b>Privacy by design and architecture</b>	<ul style="list-style-type: none"> <li>▶ Update security architecture to support <b>privacy by design</b></li> <li>▶ Conduct <b>privacy impact assessment</b> for new projects and systems</li> </ul>
	<b>Data security</b>	<ul style="list-style-type: none"> <li>▶ <b>Identify technical security measures</b> to protect PII in line</li> <li>▶ Consider <b>data encryption</b> (rest, use motion)</li> <li>▶ Ensure identity access management with appropriate use in line with PIPA</li> </ul>
	<b>Data retention and disposal</b>	<ul style="list-style-type: none"> <li>▶ Document <b>data retention and disposal</b> policy</li> <li>▶ Identify retention periods for each category of PII</li> </ul>
	<b>Monitoring</b>	<ul style="list-style-type: none"> <li>▶ Ensure that PII is used in line with policies, standards and PIPA</li> <li>▶ Set up mechanisms to <b>detect deviations</b>, i.e., unauthorized disclosures</li> </ul>
	<b>Incident response and breach notification</b>	<ul style="list-style-type: none"> <li>▶ <b>Integrate</b> personal data breaches within <b>incident response</b></li> <li>▶ Identify stakeholders to be notified after a data breach</li> </ul>
	<b>Vendor management</b>	<ul style="list-style-type: none"> <li>▶ Gain <b>visibility on vendors</b> that process PII</li> <li>▶ Set up mechanism to ensure vendors only process PII in line with policies, standards and PIPA (e.g., monitoring vendors and performing audits)</li> </ul>

# How we can help

Our portfolio of high-demand services is designed to address your cyber and privacy regulatory compliance requirements in a holistic and impactful way.

	Cyber	Privacy
Key compliance services	<ul style="list-style-type: none"><li>▶ Cyber compliance gap analysis and road map exercise</li><li>▶ Cyber maturity benchmarking and performance analysis</li><li>▶ Compliance program readiness and remediation exercise</li><li>▶ Board-level cybersecurity training and awareness sessions</li><li>▶ Cyber strategy and road map support</li><li>▶ Cyber risk management and board reporting</li><li>▶ Policies, standards, processes and guidelines</li><li>▶ Attack-and-penetration testing</li><li>▶ Targeted cybersecurity audits</li><li>▶ Secure business continuity management and disaster recovery assessment strategy, planning and testing</li><li>▶ Crisis management program design and implementation</li><li>▶ Supply chain security and third-party risk assessment</li></ul>	<ul style="list-style-type: none"><li>▶ Privacy compliance gap analysis and road map exercise</li><li>▶ Privacy maturity assessment and benchmarking</li><li>▶ Privacy strategy, road map and architecture design</li><li>▶ Personal data compliance assessment through data analytics</li><li>▶ Assessment and remediation services related to regional, national, industry data protection and privacy regulations</li><li>▶ Policies, procedures, notices and consent management</li><li>▶ Privacy training and awareness sessions</li><li>▶ Program risk assessment and remediation</li><li>▶ Targeted privacy audits</li><li>▶ Incident response planning and design</li><li>▶ Data governance and ownership review</li><li>▶ Data classification models and strategies</li><li>▶ Data handling methods and approaches</li><li>▶ Third-party privacy and data-sharing risk assessment</li></ul>
Supporting services	<ul style="list-style-type: none"><li>▶ Cyber attestation</li><li>▶ Compliance-as-a-service</li><li>▶ Cyber operating model and organizational design</li><li>▶ Cyber risk quantification</li><li>▶ Physical security assessment</li><li>▶ Product security assessment and program management</li><li>▶ Insider threat assessment and remediation exercise</li></ul>	<ul style="list-style-type: none"><li>▶ Program governance and business alignment</li><li>▶ Personal data asset register creation</li><li>▶ Privacy metrics and program reporting</li><li>▶ Cloud strategy</li><li>▶ PCI compliance services</li><li>▶ Data governance strategy</li><li>▶ Data management</li><li>▶ Data discovery scanning</li></ul>

# EY cybersecurity and privacy thought leadership



## EY Global Information Security Survey 2020

### Bridging the relationship gap to build a business-aligned security program

EY's Global Information Security Survey 2020 captures the responses of nearly 1,300 C-suite leaders and information security and IT executives. Most of the world's largest and most recognized global companies are represented, covering a variety of industries.



For more insights

Cyber

Privacy

## Meet our team

EY is a global leader in cyber risk management, with deep experience in the Bermuda insurance market. This, combined with our market-leading services in cyber risk and our close relationship with regulators, positions EY as the service provider of choice to help you meet the requirements of the BMA's Insurance Cyber Risk Management Code of Practice 2019 and Personal Information Protection Act (PIPA), 2016.



**Kerr Kennedy**  
Associate Partner, IT Risk Consulting  
EY Bermuda Ltd.  
+1 441 294 5380  
kerr.kennedy@bm.ey.com



**Chris Maiato**  
Principal, Regional Consulting Leader  
EY Bermuda Ltd.  
+1 441 294 5346  
chris.maiato@bm.ey.com



**David Brown**  
Senior Partner, Regional Insurance Leader  
EY Bermuda Ltd.  
+1 441 294 5401  
david.l.brown@bm.ey.com

EY | Assurance | Tax | Strategy and Transactions | Consulting

### About EY

EY is a global leader in assurance, tax, strategy, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via [ey.com/privacy](http://ey.com/privacy). For more information about our organization, please visit [ey.com](http://ey.com).

### About the EY region of the Bahamas, Bermuda, British Virgin Islands and Cayman Islands

The EY region of member firms in the Bahamas, Bermuda, British Virgin Islands and Cayman Islands is aligned with EY's Americas Financial Services Organization, headquartered in New York. We serve the banking and capital markets, insurance, and wealth and asset management sectors providing a full suite of assurance, tax, strategy, transaction and consulting services with a focus on providing seamless, exceptional client service.

© 2020 EYGM Limited.  
All Rights Reserved.  
EYG no. 006456-20Gb1  
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

[ey.com](http://ey.com)