



Building a better working world

Cyber and privacy risk management

Responding to the Cayman 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.

Cayman regulatory landscape: what's changing?

CIMA's Rule and Statement of Guidance - Cybersecurity

- ▶ The code sets out risk management principles and leading-practice standards to make sure that regulated entities:
 - ▶ Establish a sound and robust cyber risk management program
 - ▶ Implement a minimum standard of technical and business process controls
 - ▶ Make every effort to improve their level of resilience to cyber attacks, as well as their ability to respond and recover from any actual cyber incidents
 - ▶ Put measures in place to ensure the confidentiality, integrity and availability of their data and systems
- ▶ CIMA incorporates cybersecurity and IT system reviews in its examination/inspection procedures

Cayman Islands Data Protection Law (DPL), 2017

- ▶ On **30 September 2019**, the long-awaited Data Protection Law, 2017 came into force in the Cayman Islands.
- ▶ The DPL 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 almost all organizations, businesses (including investment funds) and the government that process personal information in Cayman.

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 CIMA's Cybersecurity for Regulated Entities? 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?

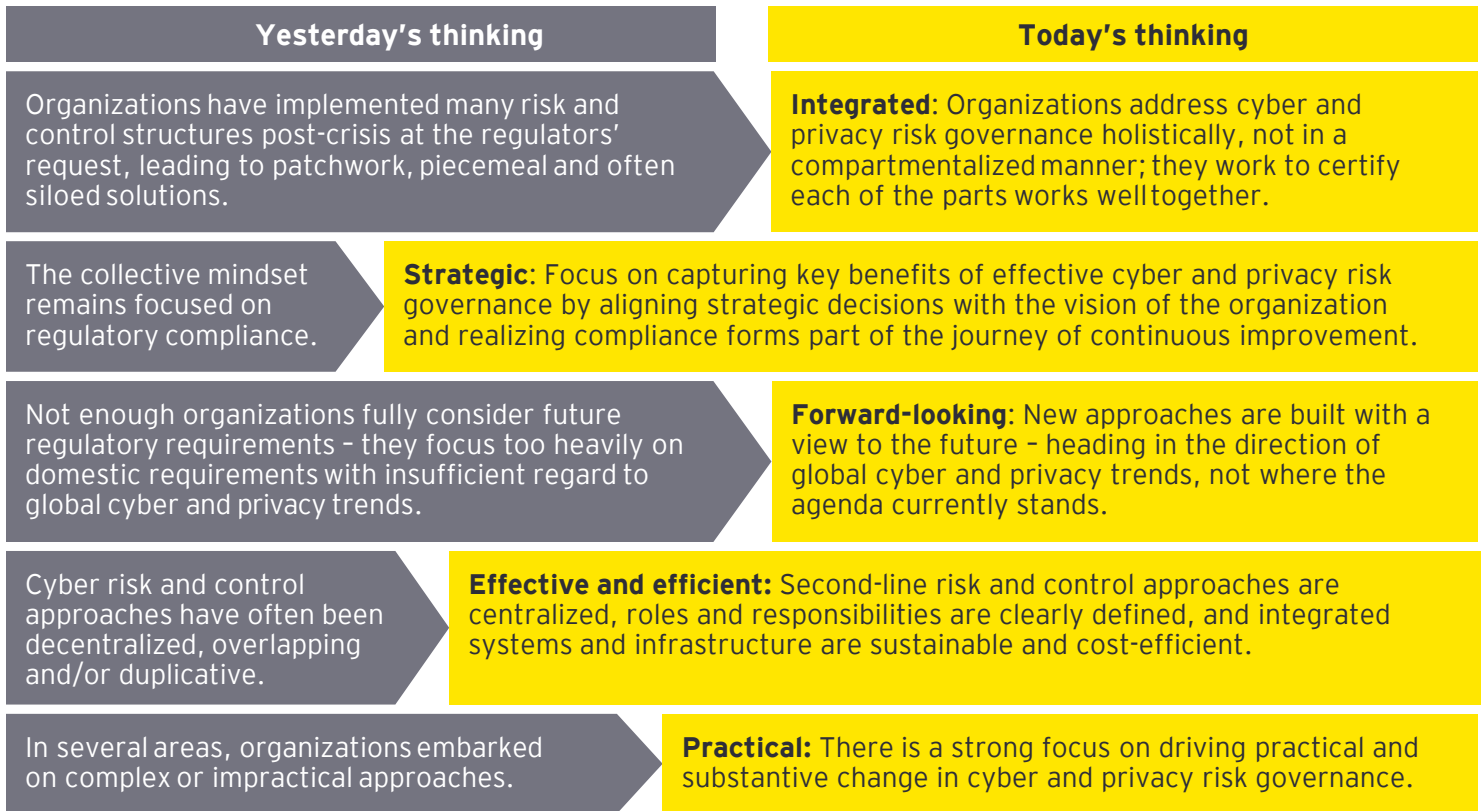
Internal audit
Are controls documented? Do we have evidence of cyber defense and privacy compliance?

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

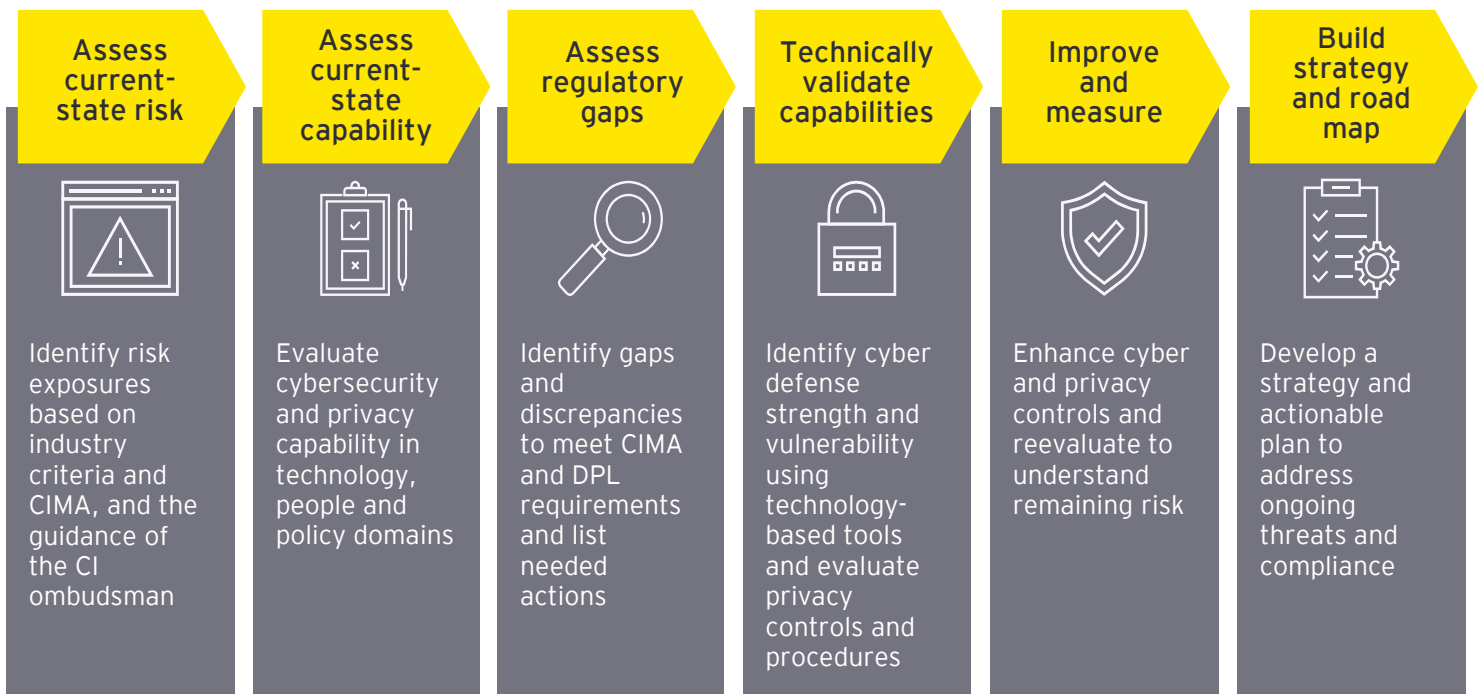


An effective approach to compliance

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 CIMA cyber regulation

Impacted area	Key considerations	
	<p>Framework and cyber risk management</p>	<ul style="list-style-type: none"> ▶ Ensure appropriate governance mechanisms are in place to address cyber security risk across the enterprise, including: <ul style="list-style-type: none"> ▶ Establish, implement, maintain and document cybersecurity framework ▶ Approve cybersecurity risk management strategy ▶ Maintain adequate IT security policies and procedures ▶ Identify managerial responsibilities ▶ Review the emerging cybersecurity threats
	<p>Role of the governing body</p>	<ul style="list-style-type: none"> ▶ Approve written cybersecurity risk management strategy ▶ Approve cybersecurity risk assessment ▶ Approve comprehensive cybersecurity framework
	<p>Cybersecurity awareness, training and resources</p>	<ul style="list-style-type: none"> ▶ Establish a comprehensive training and awareness program which needs to be reviewed and updated. Adopt a security-by-design approach ▶ Appoint sufficient and suitable personnel to maintain their cybersecurity framework
	<p>Third-party risk management</p>	<ul style="list-style-type: none"> ▶ Ensure oversight and clear accountability for all outsourced functions ▶ Identify and evaluate the risks associated with third parties ▶ Define contractual terms and conditions that would enable you to manage appropriate risks ▶ Request third parties to implement security policies, procedures and controls that are at least as stringent as the ones established within your own organization
	<p>Data protection</p>	<ul style="list-style-type: none"> ▶ Demonstrate that data protection is part of their strategy and cybersecurity framework, taking into consideration the provisions of the Data Protection Law and the guidance issued by the ombudsman on data protection
	<p>Notification requirements</p>	<ul style="list-style-type: none"> ▶ Immediately notify the Authority in writing of an incident when it is deemed to have a material impact or has the potential to become a material incident, and no later than 72 hours following the discovery of said incident
	<p>Enforcement</p>	<ul style="list-style-type: none"> ▶ Whenever there has been a breach of these rules, the Authority's policies and procedures as contained in its Enforcement Manual will apply, in addition to any other powers provided in the regulatory laws and the Monetary Authority Law (MAL)

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

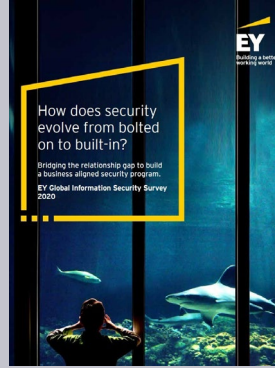
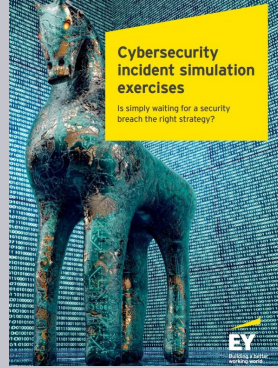
Impacted area	Key considerations
 <p>Data protection policy and data classification</p>	<ul style="list-style-type: none"> ▶ Classify personally identifiable information (PII) ▶ Develop mechanisms to enforce policies and standards
<p>Privacy risk and controls</p>	<ul style="list-style-type: none"> ▶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

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

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 the field of cyber risk management. Our experience in the financial services industry, 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 proposed requirements of CIMA's Rule on Cybersecurity for Regulated Entities and Cayman Islands Data Protection Law (DPL), 2017.



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



Kerr Kennedy
Associate Partner, IT Risk Consulting
EY Bermuda Ltd.
+1 441 294 5380
kerr.kennedy@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. For more information about our organization, please visit 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. 006457-20Gb1
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