KPMG

# The wider digital offer

***We strive to create high-quality solutions*** with innovation at their core, while building genuine relationships to deliver real value to our clients

***Bryan Beesley***

Senior Manager, KPMG in the Isle of Man

14 March 2019

KPMG

# Our Expertise

## Cyber Security

- Cyber Maturity Assessment
- C-Suite Awareness
- Maritime Cyber Security

## Privacy

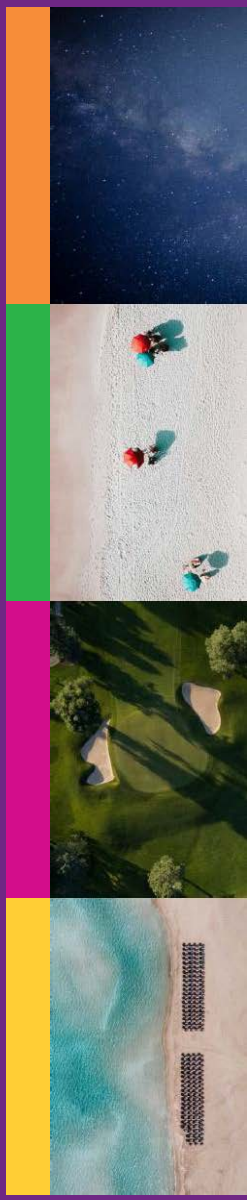
- Privacy Maturity Assessments
- DPO as a Service

## Robotic Process Automation

Accurate automation of predictable and repetitive tasks

## Blockchain

- Solution Maturity Assessment

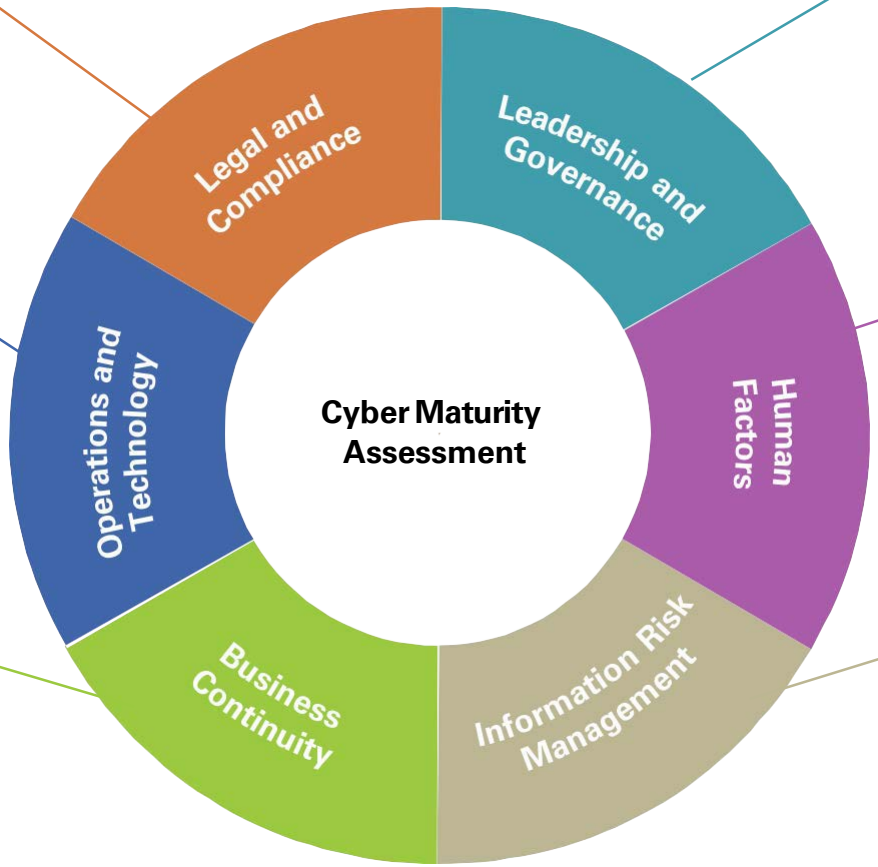


KPMG

# Cyber Maturity

Determining and supporting the awareness and development within the organisation of its Crown Jewels and wider level of maturity in relation cyber security, including business continuity and privacy.

# KPMG's Global Cyber Maturity Assessment framework




**LEGAL AND COMPLIANCE**

Regulatory and international certification standards as relevant

**OPERATIONS AND TECHNOLOGY**

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

**BUSINESS CONTINUITY AND CRISIS MANAGEMENT**

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

**LEADERSHIP AND GOVERNANCE**

Board demonstrating due diligence, ownership and effective management of risk

**HUMAN FACTORS**

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

**INFORMATION RISK MANAGEMENT**

The approach to achieve comprehensive and effective risk management of information throughout the organization and its delivery and supply partners

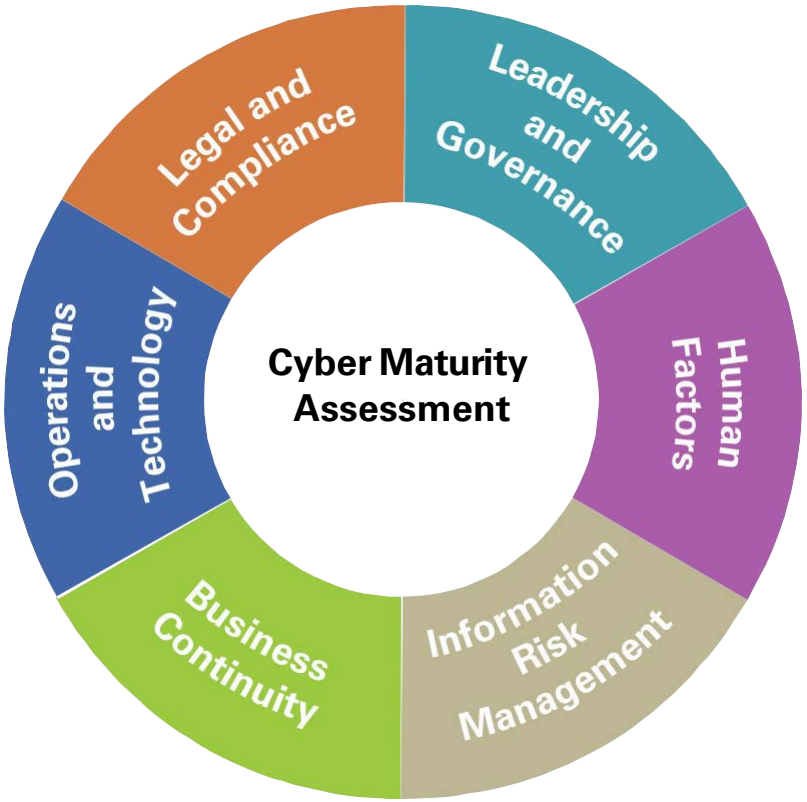
# The Six dimensions- KPMG Cyber Maturity Framework

**Technology alone is not the answer to Cyber risk issues. The answer lies in an integrated approach, focusing on all elements identified below.**

### Legal and compliance
- Three Lines of Defence
- Financial RiskTransfer
- Legislative Compliance

### Operations and technology
- Personnel Security
- Physical Security
- Identity &Access Management
- Threat &Vulnerability
- Network Security
- Cyber Hygiene
- Service Delivery
- Logging & Monitoring
- Remote, Mobile &Wireless Security

### Business continuity
- BCP with Cyber
- Stakeholder Management
- BIA & Disaster Recovery
- Incident Response




### Leadership and governance
- Cyber Understanding and Vision
- Leadership/Board Responsibilities
- Policies

### Human factors
- Culture
- Training & awareness
- Talent management
- Specialist Skills and Capabilities

### Information risk management
- Information Sharing
- Architecture
- Risk Appetite
- Asset Management
- Information Risk Management Processes and Policy
- Third Parties

# The Six dimensions- KPMG Cyber Maturity Framework

**Technology alone is not the answer to Cyber risk issues. The answer lies in an integrated approach, focusing on all elements identified below.**

**Legal and Compliance**

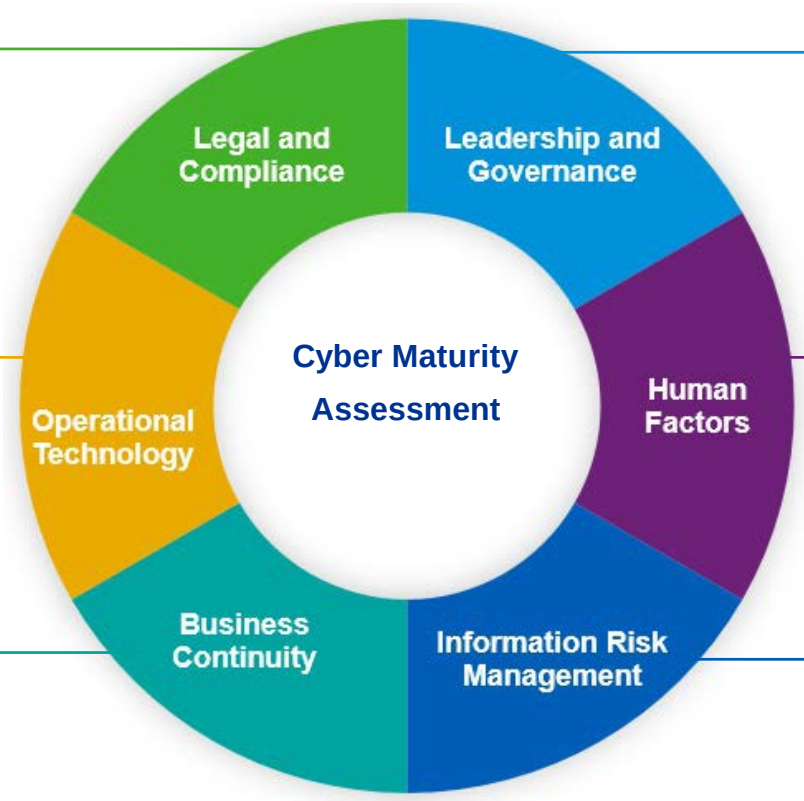
Regulatory and international certification standards as relevant

**Operational Technology**

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

**Business Continuity**

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




**Leadership and Governance**

Board demonstrating due diligence, ownership and effective management of risk

**Human Factors**

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

**Information Risk Management**

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

KPMG

# Maritime Cyber Risk

***Enabling a step-change in risk management for the maritime and super yacht industry***

# A new generation of pirates

58%

Think shipping is on the verge of a technological/ digital revolution

12%

of crew hadreceived any form of **cyber security training**

56%

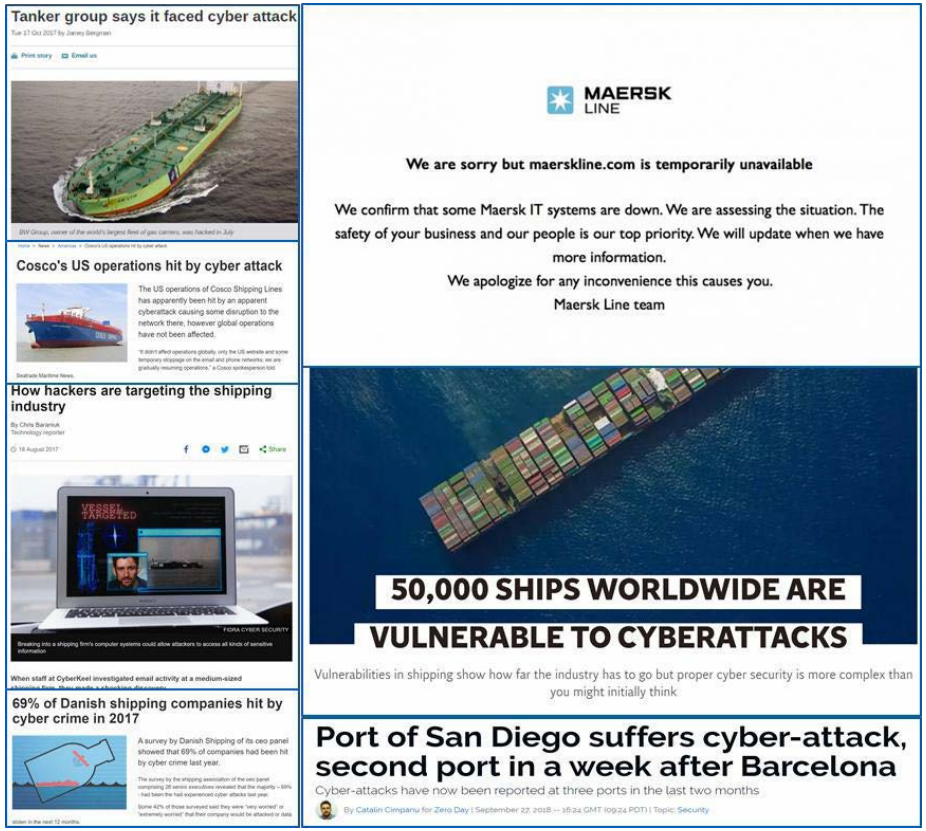
ofbusinesses do not havea **plan** to tackle cybersecurity

As crews get **smaller** and ships get **bigger**, more reliance on **automation** and remote monitoring, meaning key components, including navigational systems, can be **hacked.**

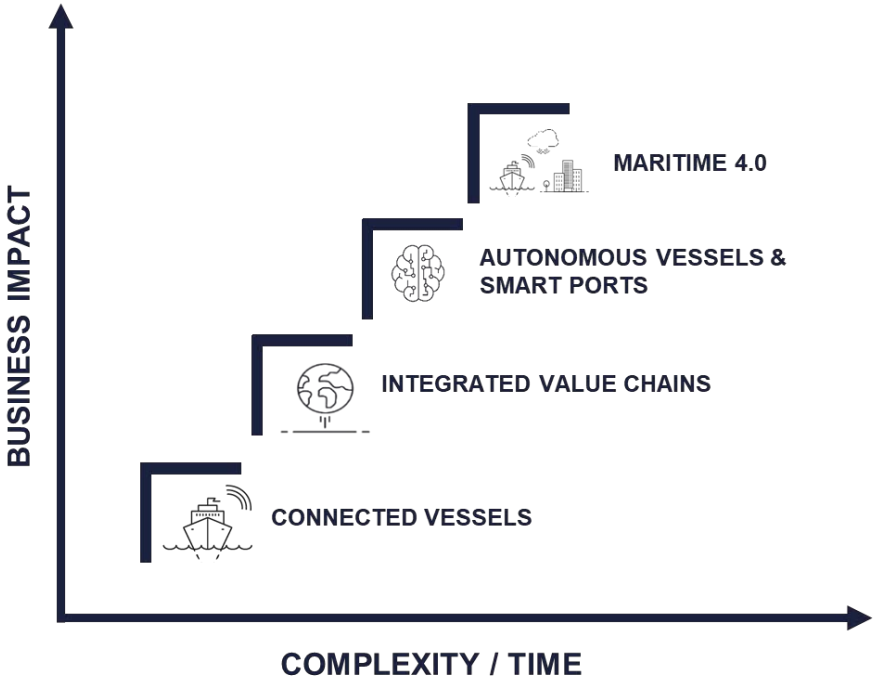
90%

Think there should be more done to prevent **cyber risks**

Sources: Crew Connectivity 2015 survey, IBM & SeaAsia Survey2017



# Changes on the horizon for the maritime sector




**The Human Factor**

Cyber awareness

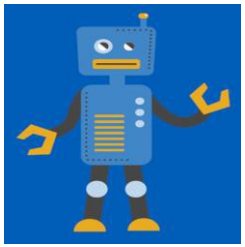
Digital skills

**Technology implications**

Digitalization

Interconnectivity

Complexity



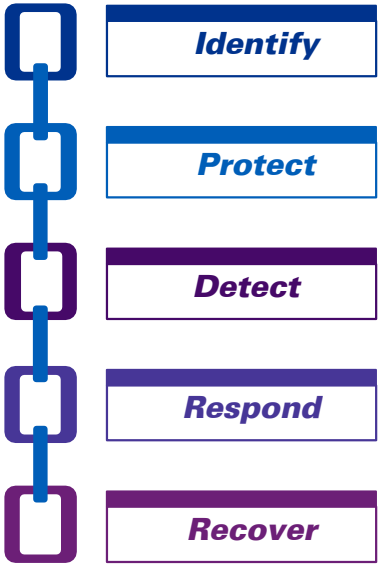
**Compliance**

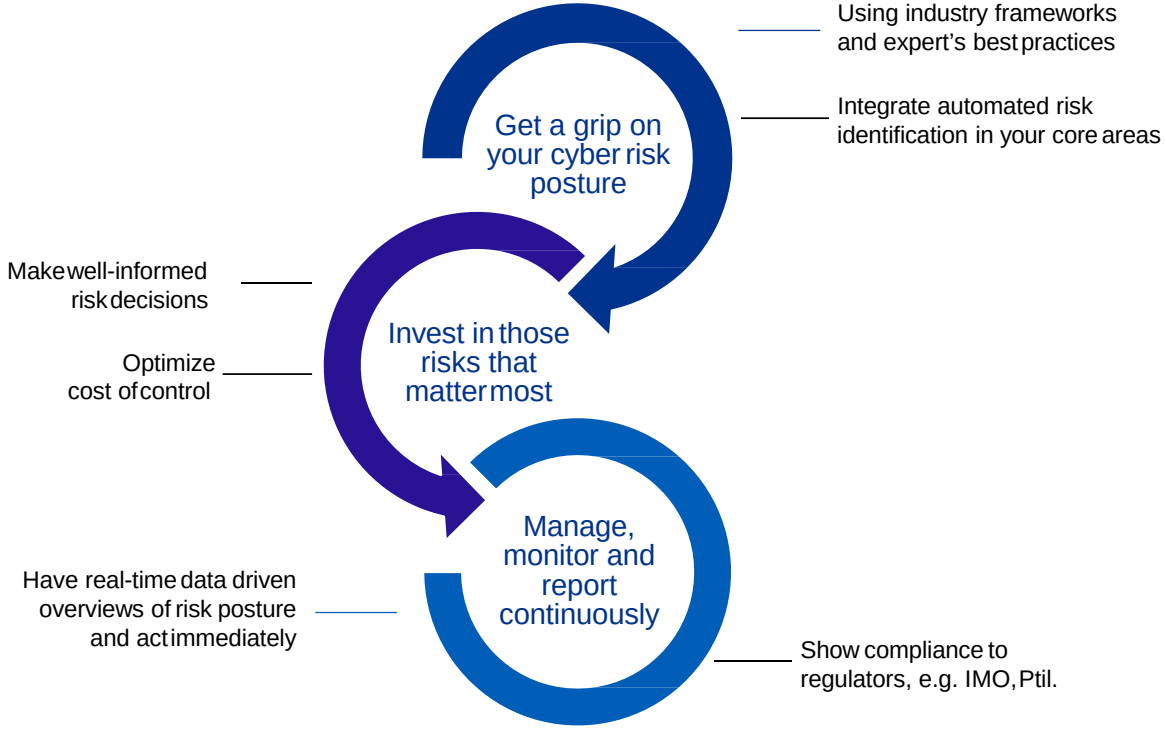
IMO guidelines

BIMCO requirements

Cyber risk management

# An integrated approach



# Solutions

***For those that are setting sail ...***

- ***Cyber Risk Quickscan***
- ***Full CyberAssessment***
- ***Control Deep Dives***
- ***Staff Cyber SecurityTraining***

***... and for those that are sailing high wind.***

- ***Fleet Risk Management***
- ***Continuous Control and Compliance Monitoring***
- ***Advanced Resilience Assessments***
- ***Incident Response Simulation andAssistance***

# Setting Sail with Cyber Risk

| What you need to set sail | What we do to help you |
|---|---|
| **Cyber Risk Quickscan**<br>To be able to turn risks into business advantages, you first need to understand your connected IT and OT landscape and identify the most relevant threats and highest risks for your environment. Several regulators will be enforcing cyber risk management soon. | • Perform assessments to identify crown jewels and relevant threat actors for your organization<br>• Finding potential attack paths towards your crown jewels<br>• Identify important components in your environment by determining potential impacts and risks<br>• Assess the cyber maturity of your most important environments |
| **Full Cyber Assessment**<br>Once you understand your connected IT and OT landscape, it is important to assess the current security measures within your fleet on areas where they are relevant. A full assessment gives you a better sense of the robustness of your overall security posture, and enables you to perform deep dives where they are relevant. | • Perform crown jewels and threat actor assessments<br>• Conduct a detailed risk assessment based on procedural, human and technological factors<br>• Assess the cyber maturity of your entire environment<br>• Provide recommendation on improvements and further deep dives |
| **Control Deep Dives**<br>Having designed and implemented controls and measures to protect your environment, it is important to monitor them and test them frequently. A deep dive on your cyber controls gives you a better sense of the robustness of your countermeasures and identifies gaps for improvement. | • Assess protective measures by performing configuration reviews, controls designs and performing on-site inspections of physical security related to critical systems and processes<br>• Analyze IT and OT network traffic for malicious behavior<br>• Assess protective and detective measures by performing penetration tests and red teaming exercises |
| **Staff Cyber Security Training**<br>The staff on board is one of the most important factors in both defense and response. Proper education on cyber risks, do's and don'ts as well as indicators of potential cyber incidents will help you staff in safeguarding your valuable vessels and systems. | • Train staff on becoming more security aware<br>• Provide awareness courses, games and tests to provide, activate and validate security awareness<br>• Train staff to identify and respond to cyber incidents using our real simulated environment |

# Sailing High Wind with Cyber Risk

| What you need to set sail | What we do to help you |
|---|---|
| **Fleet Risk Management**<br>As you try to balance investment with actual risk reduction, a comprehensive and quantified method to consistently assess and address the main risks across your portfolio of ships will justify the cost of control. In addition, it helps you in complying with mandatory cyber risk management regulations (e.g. IMO). | • Provide an easy to use set of tools to identify, assess and control risks on your fleet in a consistent manner<br>• Integrate all your control frameworks, in order to prove compliance to the regulators you may be subject to.<br>• Real-time control dashboards and exception handling functionality |
| **Continuous Control and Compliance Monitoring**<br>Real-time insight in any emerging cyber risks on board, plus timely notification when follow-up is needed. Automated control monitoring increases the level of control and compliance while leveraging the stream of data that your systems generate. | • Assess protective measures by performing configuration reviews, controls designs and performing on-site inspections of physical security related to critical systems and processes<br>• Analyze IT and OT network traffic for malicious behavior<br>• Assess protective and detective measures by performing penetration tests and red teaming exercises |
| **Advanced Resilience Assessments**<br>A thorough understanding of the quality of your protection, detection and recovery capabilities. As you may be subject to threats that have a high persistence, you will need to validate you resilience in a way that is going deeper than the deep dive. | • Perform full resilience assessments<br>• Perform red team exercise on selected attack vectors<br>• Test and exploit like an advanced and persistent threat actor would do. |
| **Incident Response Simulation and Assistance**<br>When an incident happens, getting back to business as usual is key for your business continuity and safety. To achieve this, cyber response processes should be 'second nature' for your organization. | • Train staff on becoming more security aware<br>• Provide awareness courses, games and tests to provide, activate and validate security awareness<br>• Train staff to identify and respond to cyber incidents using our real simulated environment |

KPMG

# Privacy Management

# KPMG's Privacy Management Framework

### *Privacy Principles*

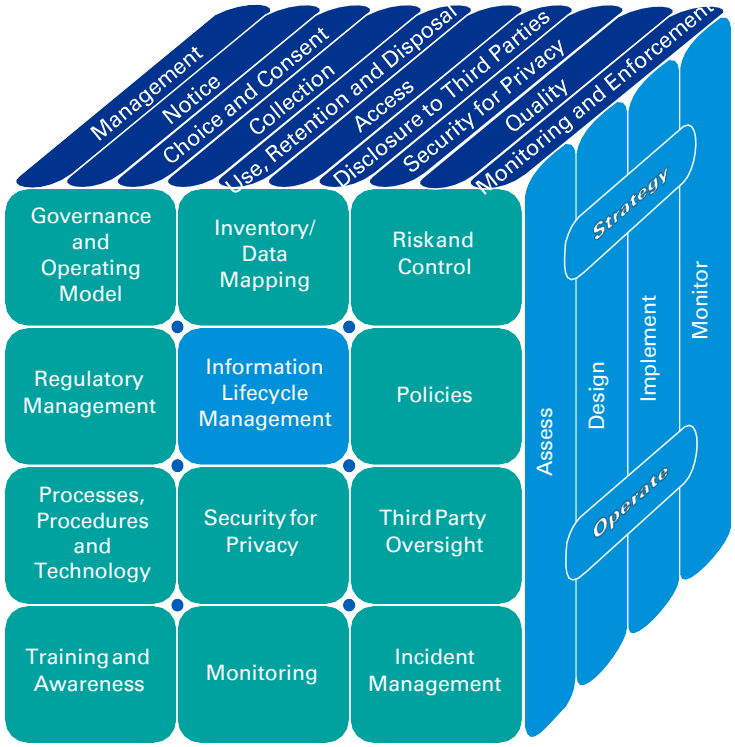
Privacy components are viewed against the internationally-recognised 'Generally Accepted Privacy Principles', which provide the foundation for our privacy management framework.

### *Privacy Management Framework*

Our framework elements are the distinct components that organisations employ to help ensure compliance with applicable Privacy laws and regulations. They provide a practical and pragmatic structure for organising the day-to-day management and oversight required to mitigate Privacy risk exposures.

### *KPMG Support*

Our Privacy Service has been designed on the basis that organisations need tailored risk based solutions to address their individual Privacy needs, risk appetite and future business strategy. Its modular and layered structure enables targeted and tailored solutions to be designed, developed, implemented and monitored consistently, cutting through the complexity of Privacy and complex global organisations.



# Privacy Maturity Stages -Overview

The following table outlines the levels of maturity used within the Privacy Maturity Model for each Privacy Management Framework component:
For each component and sub-component of the Privacy Management Framework, a detailed maturity level is defined – the table below generalises what each of these maturity levels look like for each of the 40 maturity models.

| Level | Description |
|---|---|
| 1 Adhoc | — Evidence that the organisation has recognised that the issues exist and need to be addressed.<br>— Processes notdocumented.<br>— No standardised processes; instead, there are adhoc approaches that tend to be applied on an individual or case-by-case basis.<br>— In a state of dynamic change — driven in an ad hoc, uncontrolled, or reactive manner. |
| 2 Initial | — Minimal documentation.<br>— Repeatable, possibly with consistent results by different people undertaking the same task.<br>— Lacks rigorous process discipline — high degree of reliance on the knowledge of individuals and, therefore, errors are likely.<br>— No formal training or communication of standard procedures — responsibility is left to the individual. |
| 3 Controlled | — Defined and documented standard procedures communicated through training.<br>— Formal controls operate to ensure effective operation of processes.<br>— Activities are consistently performed within key functions and business groups, but are not yet coordinated consistently across theorganisation. |
| 4 Monitored | — Formal processes with review and approval built in, where appropriate, and that are communicated consistently across the organisation.<br>— Activities are consistent and well coordinated across the organisation. |
| 5 Optimised | — Efficiency and effectiveness of processes assessed using formal measures andprocedures.<br>— Changes made to maintain efficiency over time.<br>— Process seamlessly integrated across enterprise boundaries. |

# Why is privacy so important?

***It remains a high priority for companies***

"The government's recent cyber risk survey found that while 69 per cent of businesses say their senior management consider cyber security is a very or fairly high priority for their organization only half of businesses have actually taken recommended actions to identify cyber risks."

~ Elizabeth Denham, UK Information Commissioner

***We are all at risk of non-compliance***

You may think you are not a tech or internet based company but the chances are you still manage an significant amount of data.

- Staff records
- Customers
- Contractors

***A range of operations are implicated***

Operations that are considered "processing" include, but are not limited to: "*Collecting, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*"

# Increasingly regulatory pressure and complexity

The regulatory landscape is ever evolving – remains increasingly fragmented and complex – and this represents a key driver of change. Managing Privacy regulatory requirements requires a careful strategy in line with a businesses risk appetite and future commercial objectives. Ownership of the regulatory risk is increasingly transitioning upwards to C-Suite level.

### EU REGULATIONS

- The EU General Data Protection Regulation (GDPR)

### US REGULATIONS

- State level regulation such as California Consumer Privacy Act of 2018
- Federal legislation such as the health Insurance Portability and Accountability Act (HIPAA)

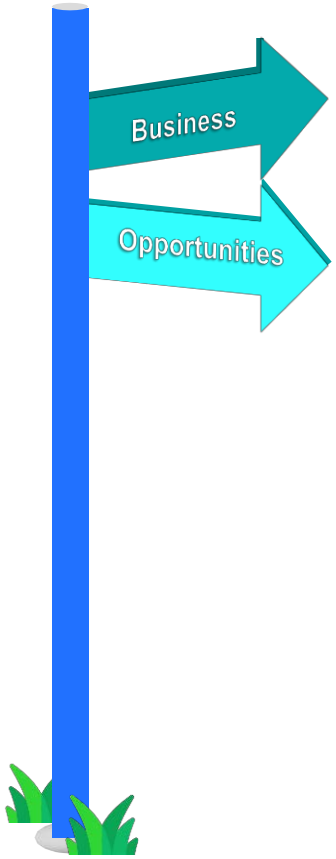
### BERMUDIAN REGULATIONS

- The Personal Information Protection Act (PIPA)

### ASIAN REGULATIONS

- Singapore – Personal Data Protection Act
- South Korea – Personal Information Protection and IT Network Act

# Opportunities beyond GDPR compliance




**Strengthen data security and cyber-resilience**
(in terms of confidentiality, integrity and availability)

**Minimizing risk**
Minimizing privacy and security risks will reduce risks to reputation, brand and business relationships.

**Improve brand image by ethical behavior**
(including Corporate Social and Environmental Responsibility activities)

**Ensure continued development of data initiatives**
(digital marketing, profiling, e-commerce, big data,…)

**Improve operational efficiency**

**Reduce cost**
Aligning your compliance efforts with existing or planned process or technology changes and projects will decrease the cost of these.

**Increase data value**
(better knowledge, improved quality, cross-group exchange)

**Build trust**
Managing privacy risks will build the trust of data subjects (customers, suppliers, partners and employees)

**Enhance customers' will to consent**
A transparent privacy approach will enhance customers' willingness to consent.

**Improve control over outsourced activities**

**Control legal liability**
Adherence to compliance requirements limits legal liability and reduces the risk of sanctions

**New income generation through new business revenue opportunities**

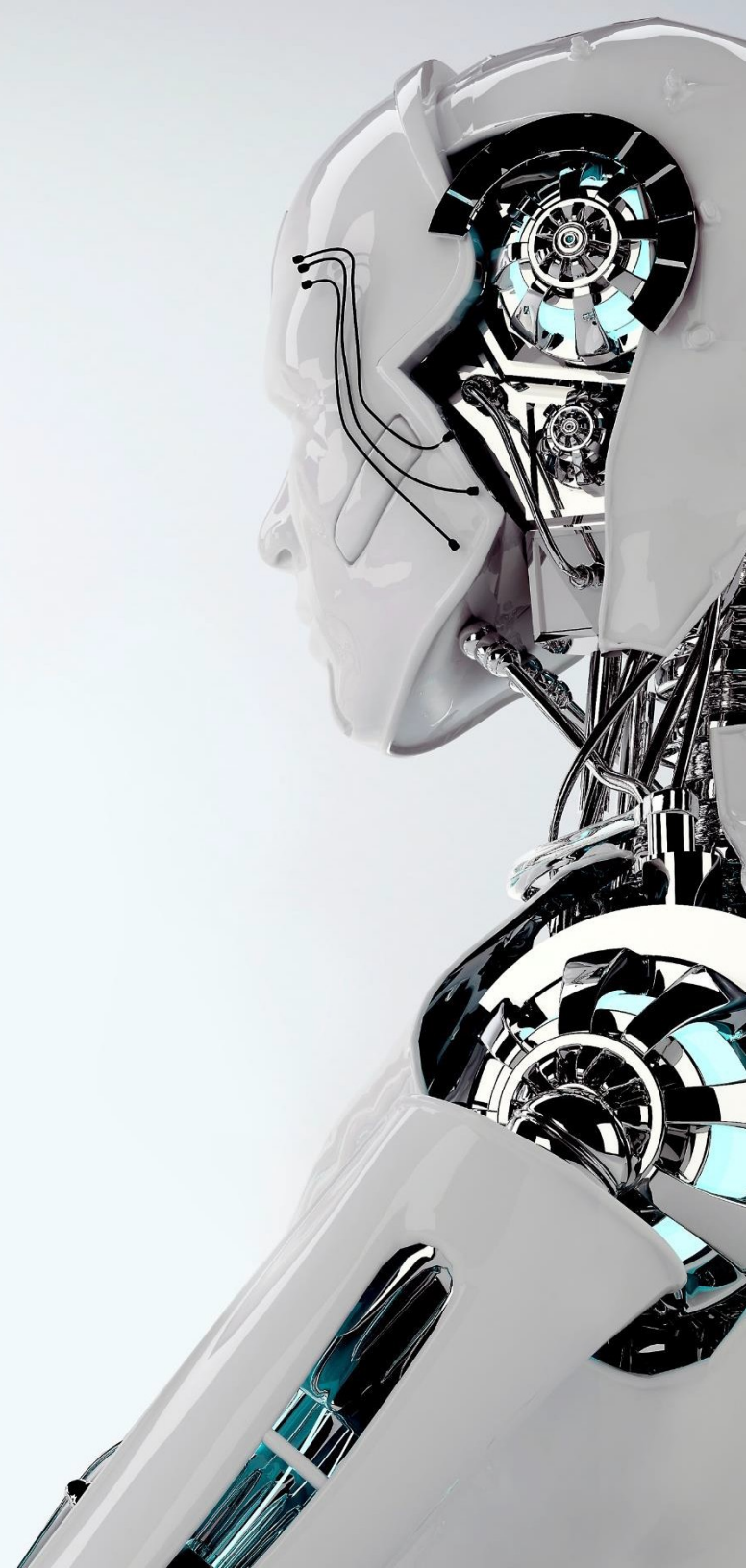
**Accelerated market-readiness**
Getting privacy right so that new, differentiating products can be marketed quickly.

KPMG

# Robotic Process Automation

***Also referred to as digital labour, Robotic Process Automation (RPA) is a method used to automate predictable, repetitive, mundane and unappealing processes and tasks that were considered to be achievable only by human employees.***

Software can be used to emulate and automate the steps usually performed by people in an organisation in a much faster and more accurate way.



# How does Robotic Process Automation work?

https://www.youtube.com/watch?v=xW95yb6J1eU

# Intelligent Automation supports both front-office and back-office activities

***The different parts of IA can be integrated to provide an automated transaction system for functions & Enterprise.***

**Automation skills**

- **Rule-based Automation**
- **Dialogue Automation**
- **Analytical Automation**
- **Cognitive Automation**

Automation Skills are applied within different channels and mixed with human contact.

Combination of skills in order to handle different formats and exchanges of information

Dialogue drvien - Dynamic

Input driven - Static

**Chat**

***Automated Customer Dialogue (Chat-bot/VA)***

– Self-service customer automation for standard customer requests

– Log-in and authentication to support individual requests

– Hand over to human chat for non-standard requests

**Chat**

***Human Chat + RDA***

– Support customers over chat

– Combine w/RDA for better activity efficiency & quality

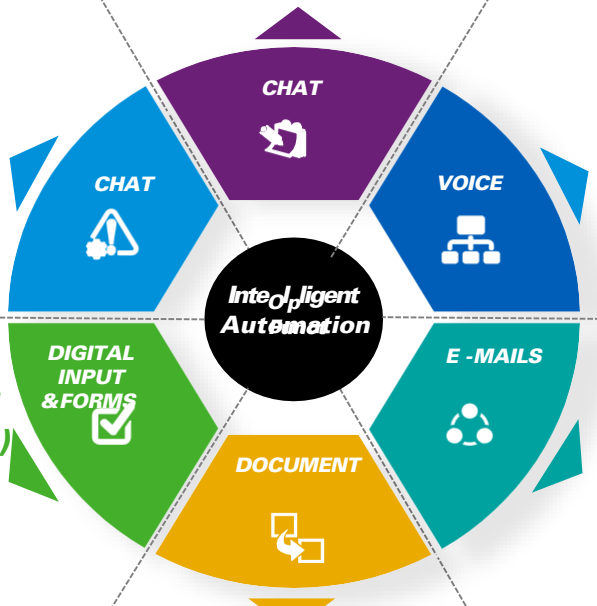
**Voice**

***Human + RDA & Cognitive Support***

– Support customers over voice

– Improved efficiency using RDA for standard activities

– Improved customers service w/cognitive support by giving the case worker better insight and automatic live recommendations




**Structured data**

***Automated rule-based (RPA + Human except.)***

– Read structured input data or send to interpretation

– Automated processing according to standard workflow

– Auomated decision according to business rules

– Send to human processing for business exceptions

**E-mails**

***Interpret, structure and respond (AnA)***

– Interpret emails and content

– Classify content and structure data when possible

– Auto-respond when possible due to e-mail classification/ interpretation

– Generate response based on template and forward to human response with proposal

**Documents**

***Monitor/Receive & Forward (AnA)***

– Interpret, classifiy and structure cocument

– Forward data for to automated processing

– Manual processsing for remaining

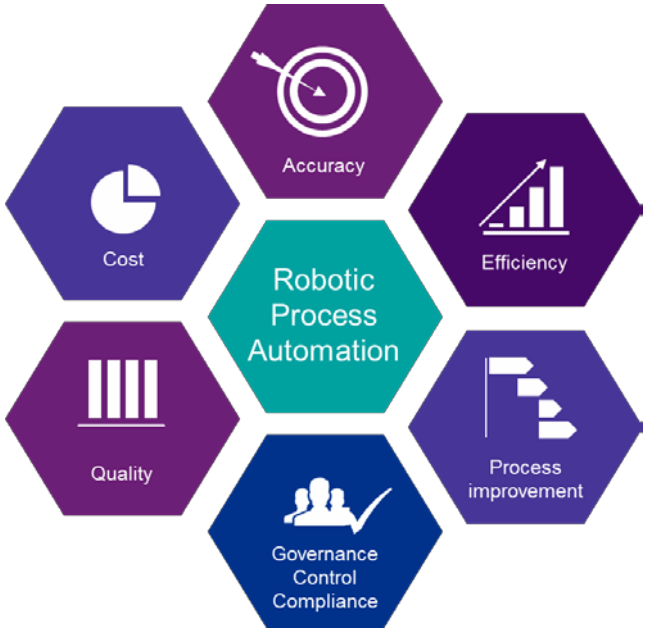
# Benefits of Robotic Process Automation

## Accuracy

- Eliminates human error rate resulting in greater performance, consistency & accuracy of processes
- Reduces manual journal entries
- Detects transaction exceptions

## Costs

- No change in existing IT systems is required
- Implementations for Process Robotics take from several days up to several weeks
- Cost reduction for relevant processes generally are between 40-75%
- Payback period typically is between 6 and 12 months




## Efficiency

- Reduces FTEs resulting in significant cost reductions
- Automates rules-based processes enabling resources to focus on more value-add activities
- Reduces cycle time
- Performs tasks 365 days a year at 24/7 availability

## Quality

- Detects poor data integrity
- Monitors system stats and starts troubleshooting efforts
- Enables scheduled maintenance and interface checks

## Process improvement

- Provides platform for continuous improvement
- Increases visibility and transparency of financial processes
- Enables standardisation of processes across entities
- Enables ability to scale up rapidly for increases in transaction volume

## Governance, control & compliance

- Eliminates fraud
- Performs policy updates and performance during down times
- Maintains record of tasks completed for compliance record keeping

# Benefits of RPA

**Privacy and Compliance**

—Reduce error in transactional tasks

—Increase security and governance tasks

—Limits exposure to sensitive data

**Quality and Accuracy**

—Reduce quality issues associated with manual data entry

—Deploy new "no-labour" data integrity routines

—Reduce the need for re-work

—Fully auditable & traceable

**Process Efficiency**

—Lower cost and increased speed of implementation

—Non-invasive, can work with existing IT systems

—Can perform tasks 365 days a year at 24/7 availability

**Speed**

—Leverage digitised process data to increase the speed and accuracy of service delivery

—Accelerate completion rates of certain tasks

—Rapidly scale up / scale down operations

—Respond quickly to regulatory and policy changes

**Employee Satisfaction**

—Enable resources to focus on higher, value-added activities

—Reduce amount of repetitive, administrative tasks

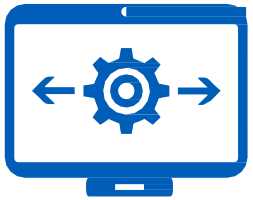
—Automation tools can be employees' personal assistants

**Customer Engagement**

—Reduce application processing and call centre wait times

—Provide accurate and prompt answers to customer inquiries

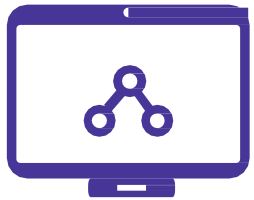
# Robotic Process Automation (RPA) is the first step towards cognitive automation



## Robotic Process Automation (RPA)

**Rules engine** + **Screen scraping** + **Work flow** +

- Macro-based applets
- Screen level data collection
- Workflow automation
- Visio®-type building blocks
- Process mapping
- Business process management

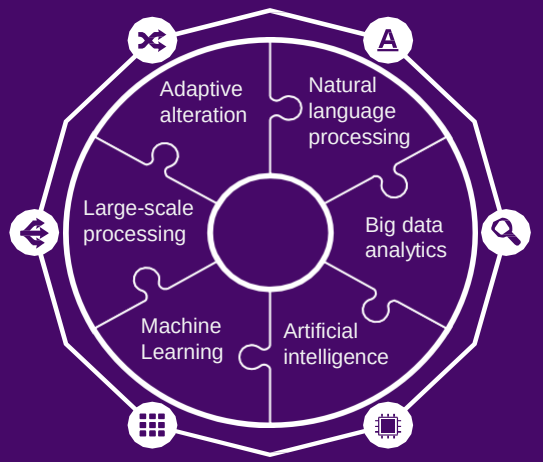


## Enhanced process automation

**Processing of unstructured data and base knowledge** +

- Built-in knowledge repository
- Learning capabilities
- Ability to work with unstructured data
- Pattern recognition
- Reading source data manuals
- Natural language processing

## Cognitive automation




- Artificial intelligence
- Natural language recognition and processing
- Self-optimisation/self-learning
- Digestion of super data sets
- Predictive analytics/hypothesis generation
- Evidence-based learning

KPMG

# Blockchain

***Blockchain is a peer-to-peer distributed digital ledger that initially served as the technology behind cryptocurrencies. It has since evolved to serve as a platform that allows multiple untrusted parties to transact with each other without having to rely on trusted third parties.***

While the most common use case for Blockchain has been publically available ledgers, there has recently been a rise in ledgers that are available to a small group of entities (consortiums), allowing them to conduct their inter-business operations more efficiently within the organisation of its Crown Jewels and wider level of maturity in relation cyber security, including business continuity and privacy.

# What is the blockchain maturity model?

***Quick Scan***

— KPMG has developed a blockchain maturity model which helps to get a grip on the specific risks associated with blockchain implementations.

— This framework helps you to get an understanding of the IT risk maturity of the blockchain implementation in all eight risk areas.

— The assessment enables you to identify weak points and to spot opportunities for improvement.The overall report provides you with concrete pointers as to how to improve and raise your blockchain maturitylevel.

# The benefits of the maturity model

***Clear insight into blockchain risks***

This framework helps you to get an understanding of the IT riskmaturity of the DLT implementation from eight risk areas.

***From proof-of-concept to production***

Going from proof-of-concept to a production ready system requires a good view on IT risks. The maturity model identifies weaknesses in your existing blockchainsolution.

***Concrete action plan***

The assessment gives concrete pointers to risk areas for improvement and concrete recommendations how to improve and raise to the next blockchain maturity level.

***Unique and validated model***

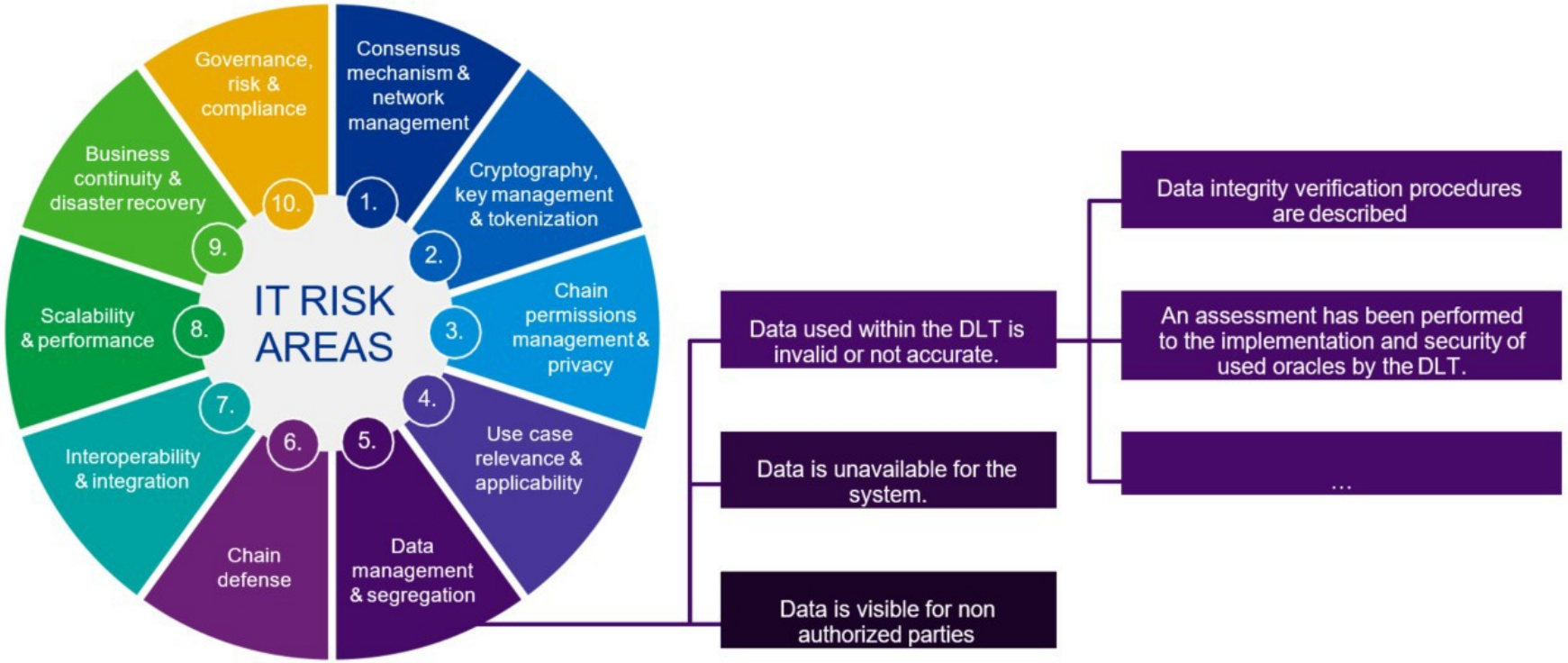
This assessment with its specific blockchain focus is unique in the current market and is based upon solid research, IT risk standards and years of experience and was validated with clients.

# How does the maturity model scoring work?

The model contains blockchain specific risks grouped in eight IT risk areas.

Each of these risk areas contains multiple risks.

For each risk a number of controls have been defined to allow KPMG to assess the maturity on the specific risk.

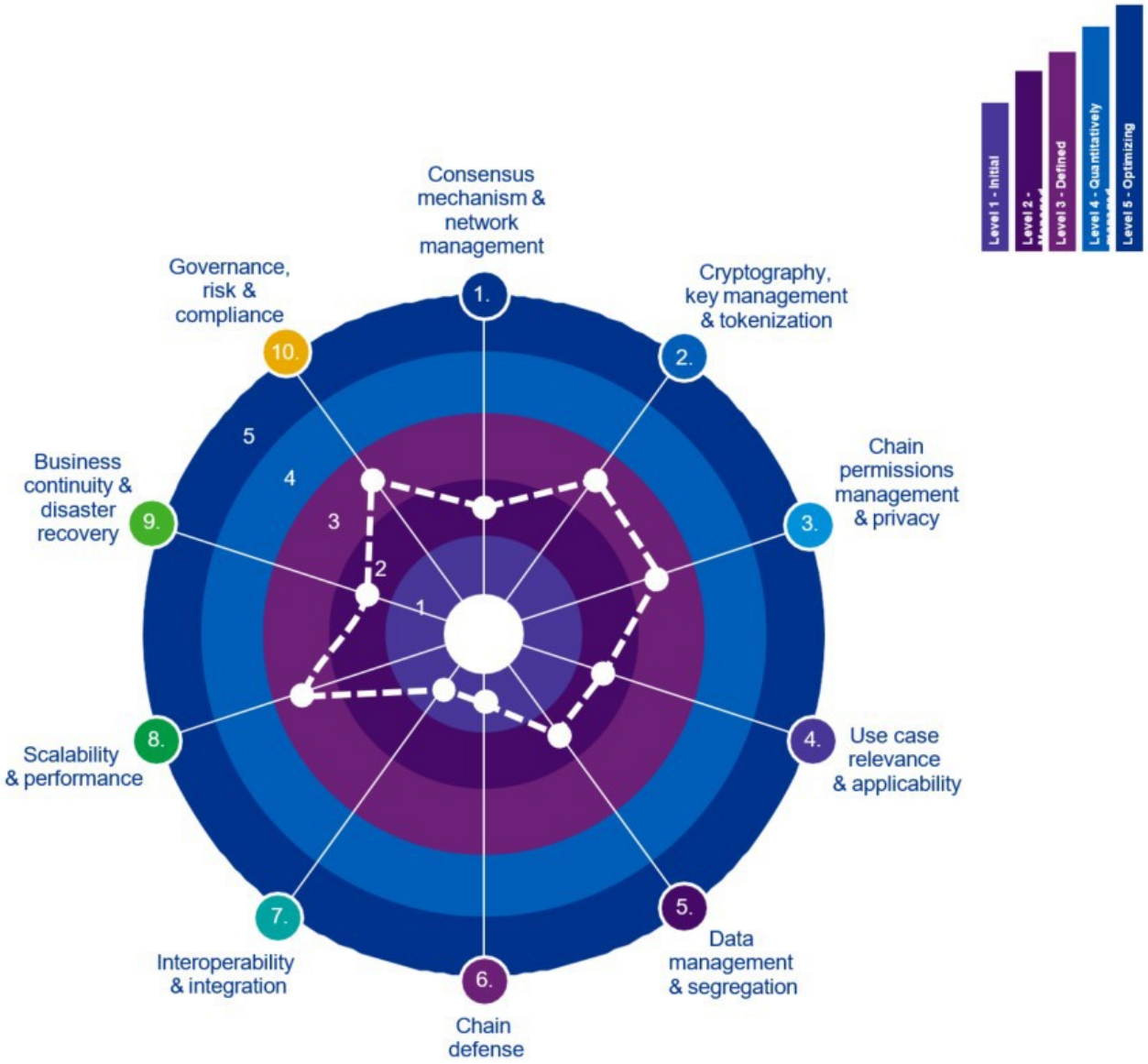


# Blockchain maturity model assessment findings

## Overall score

— After the assessment has been completed, all the scores for each risk area are visualized in a spider graph.

— Each risk area has obtained an overall score, ranging from level 1 to level 5, depicted in the graph on the right. The scores are elaborated in the details slides.



# Thank you


Bryan Beesley
***Senior Manager, Advisory***
***Digital Advisory Lead***
KPMG in the Isle of Man
***T:*** +44 (0) 1624 681042
***E:*** bbeesley@kpmg.co.im


**kpmg.co.im/socialmedia**