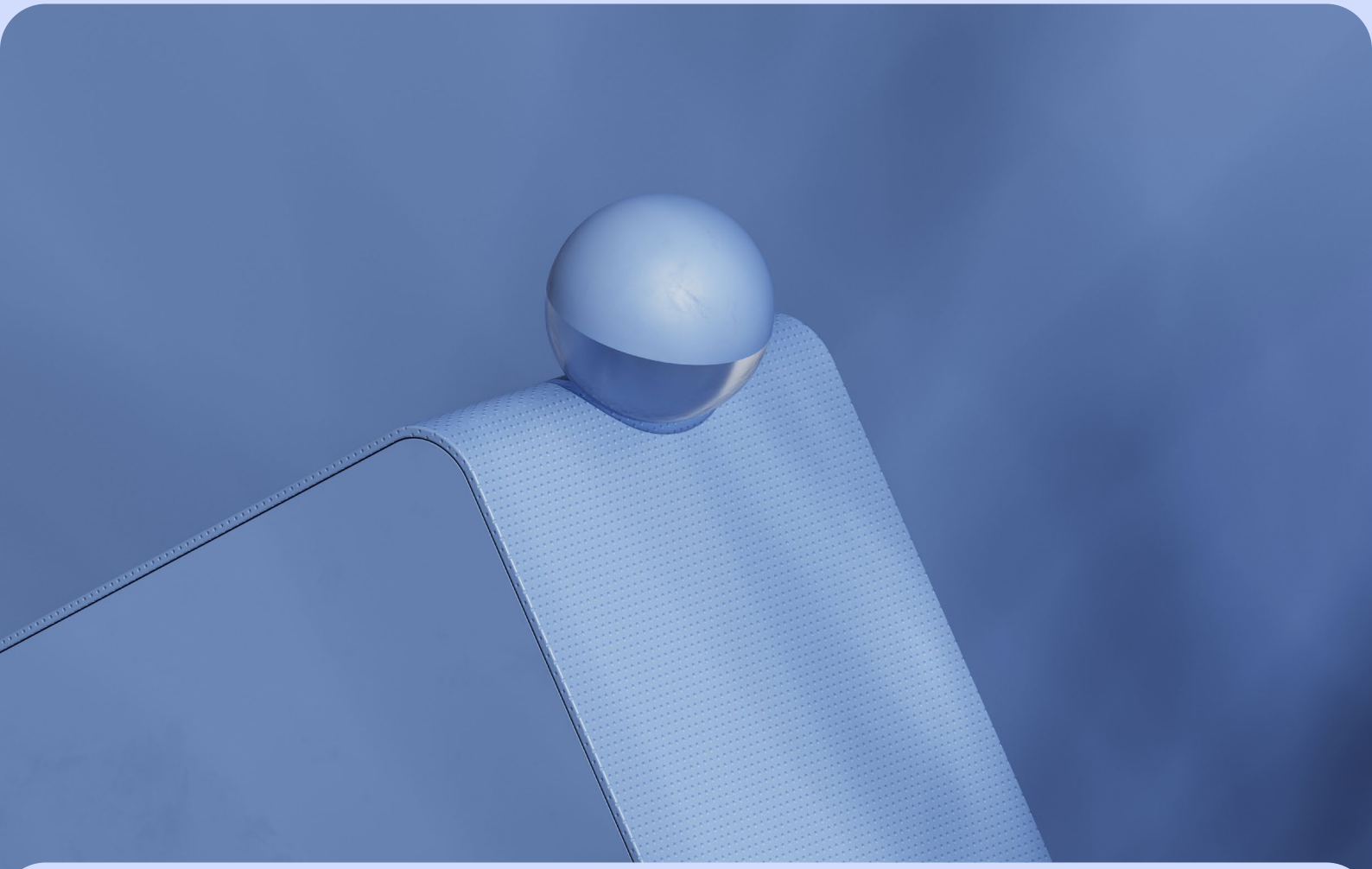
PROTECHT



E-BOOK

Compliance and compliance risk management.

Understand the difference between compliance and compliance risk management and manage your compliance obligations.

PROTECHT

Contents

01

Introduction.

We live in a world of rules. "Compliance" is the process of conforming to those rules. The rules of an organisation are referred to as "Compliance Obligations" and consist of two main types:

- Rules that an organisation has to comply with being:
  - External Regulatory, covering laws and regulations
  - External Contractual, covering rules written into contracts we have with other parties

We refer to these as "Compliance Requirements".

- Rules that an organisation chooses to comply with, which consist of:
  - External standards
  - Internal policies, codes of conduct, internal service level agreements and the like

We refer to these as "Compliance Commitments".

The management of an organisation's compliance with its compliance obligations is a formidable task, especially in relation to external regulatory compliance due to sheer volume of regulation that seems to keep expanding exponentially.

An organisation's risk appetite statement (RAS) should address the organisation's appetite for not complying with its compliance obligations. For most organisations, we would expect that risk appetite for non-compliance be zero or close to zero, that is, they will aim to comply with all of the rules to which they are subject.

Compliance management therefore involves:

- Knowing what rules apply to the organisation
- Ensuring that the organisation meets those rules

This sounds easy, but the enormous volume of rules make it quite the opposite. This eBook discusses the processes of managing compliance which we refer to as "Compliance Management" and managing compliance risk which we refer to as "Compliance Risk Management".

Further reading on risk appetite statement (RAS): A Practical Guide to Risk Appetite (eBook PDF)

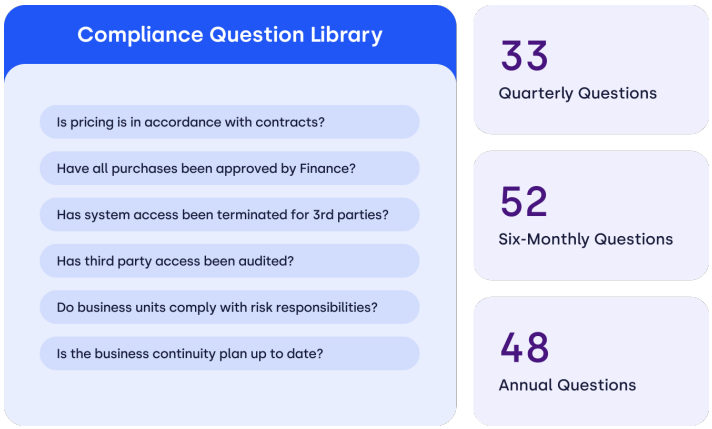
02

Definitions.

We will use the definitions contained in the ISO19600 Compliance Risk Management Systems Standard being:

- **Compliance Commitment:** Requirement that an organisation chooses to comply with
- **Compliance Requirement:** Requirement that an organisation has to comply with
- **Compliance Obligation**[1]**:** Compliance Requirement or Compliance Commitment
- **Compliance:** Meeting all of the organisations Compliance Commitments and Requirements
- **Non-compliance:** Non-fulfilment of a Compliance Commitment or Requirement
- **Compliance Risk:** Effect of uncertainty on compliance objectives

For the purposes of this eBook, we will focus on external regulatory Compliance Requirements. The process for external contractual requirements and internal compliance commitments will be similar.



Compliance risk is an operational risk and should be managed accordingly.

1 We find it useful to define compliance obligations as the plain English interpretation of the compliance requirement and compliance commitment which is the meaning we have given it throughout this eBook.

03

Compliance and compliance risk management.

Although “Compliance Management” logically covers compliance risk management as well, it is useful to differentiate the two in order to better explain each.

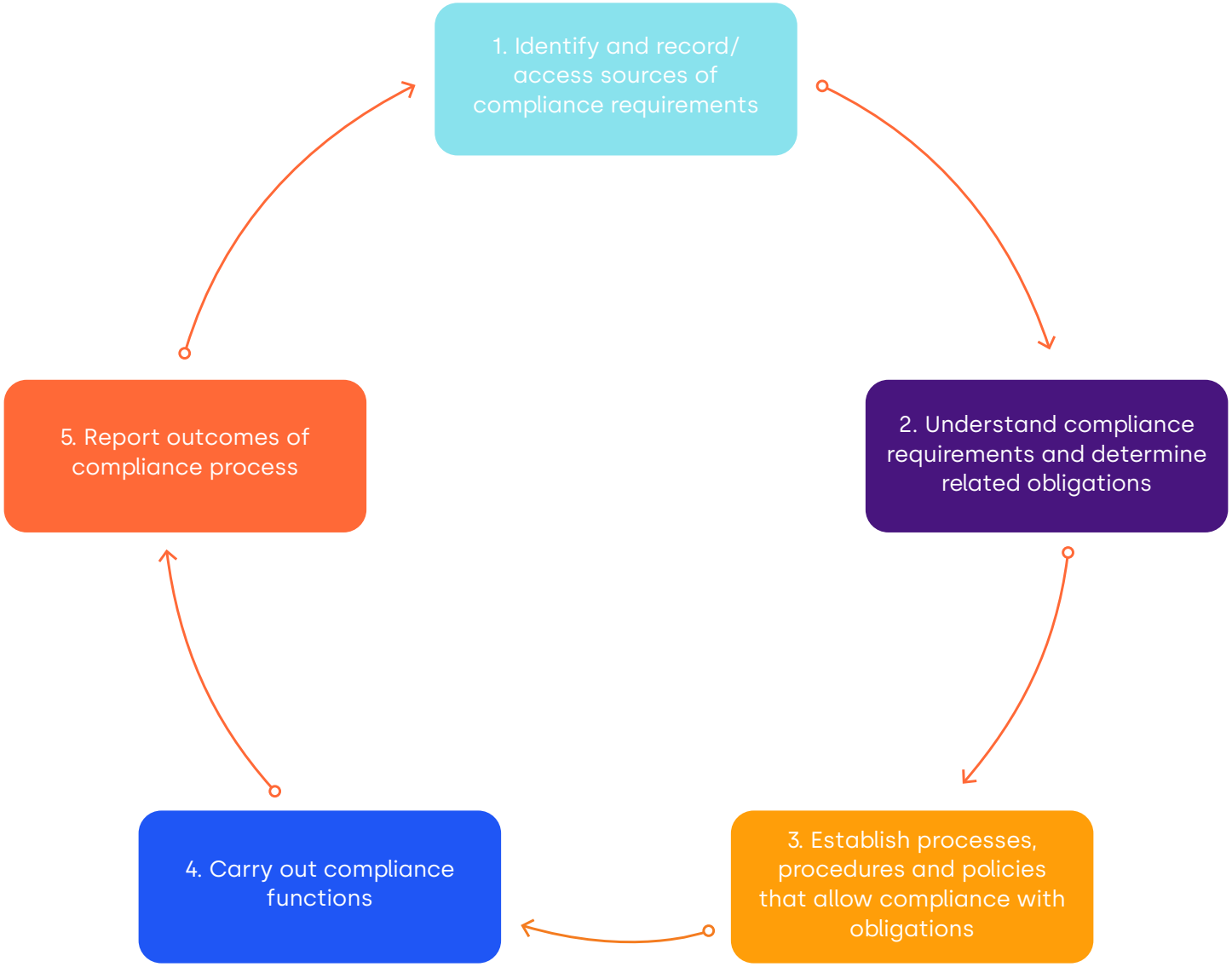
We will define “Compliance Management” as:

“Managing the organisation’s ability to comply and managing the organisation’s actual ongoing compliance” and “Compliance Risk Management” as “Managing the risks that could lead to non-compliance”.

04

Compliance management.

Compliance Management consists of the following 5 processes:

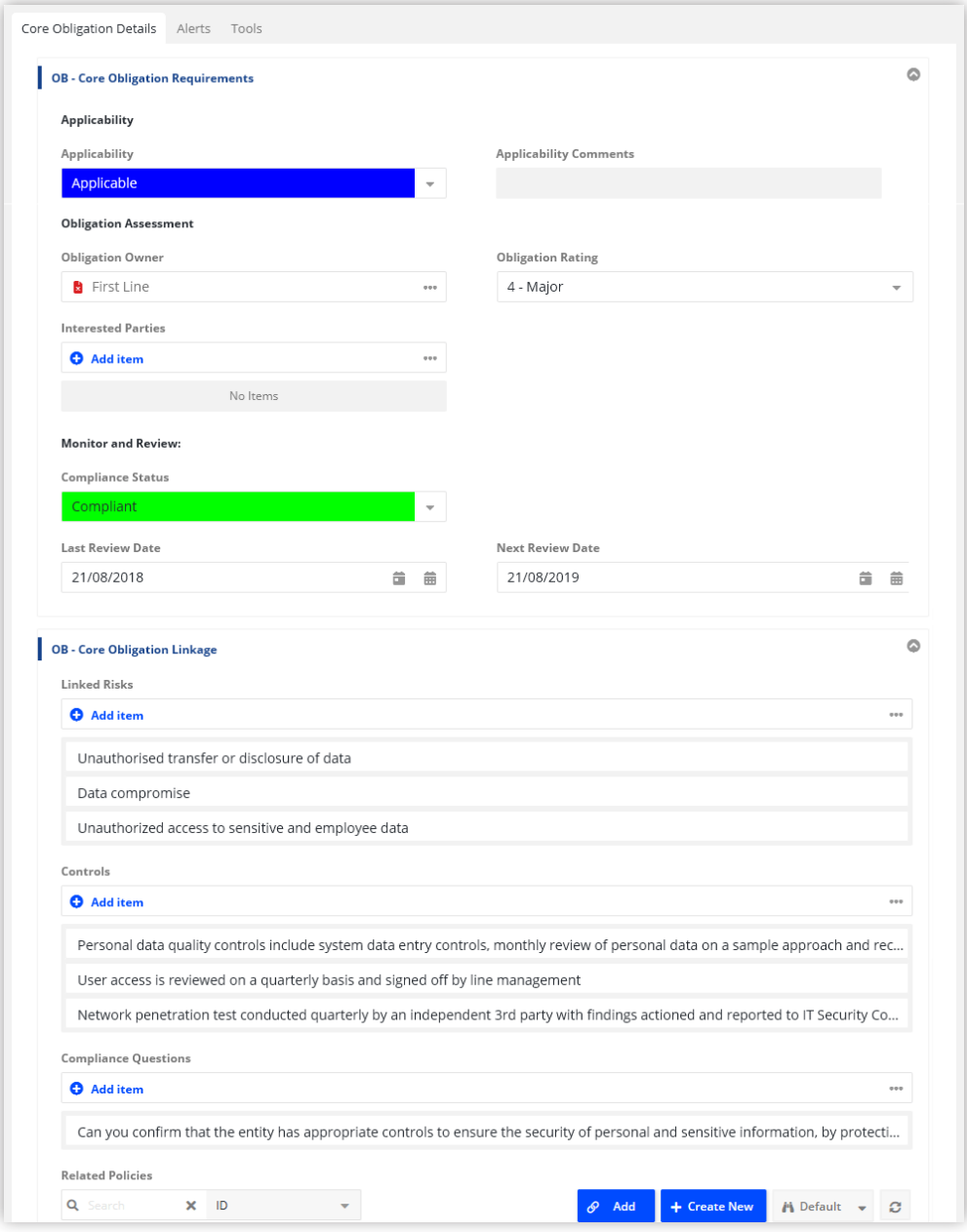


4.1 Identify and record / assess the sources of compliance requirements.

This can be a formidable task for external regulatory compliance due to the volume of laws and regulations most organisations are subject to. The sources of requirements need to be identified, recorded and understood. This gives rise to the necessity for a compliance requirements / compliance commitments or 'obligations' register.

This register should ideally include:

- The Law or Regulation name
- The sections and sub-sections of the regulations
- The parts of the organisation to which the requirements apply
- Penalties for non-compliance
- A link to policies and processes that support compliance
- A link to the risks and related controls, that could lead to non-compliance



A sample Obligations Register from the Protecht.ERM system, showing the requirement and linkages to risk, controls, compliance questions and related policies.

There must also be a process for keeping the requirements up to date with alerts sent out to the relevant parts of the business when requirements change.

The creation and maintenance of this register can either be achieved internally if you have the appropriate resources or externally using external legal experts to develop and maintain these registers.

4.2 Understand compliance requirements and determine related obligations.

4.2.1 Creating and rating obligations.

Most legislation and regulations are written in complex legal language which are difficult to understand by the business. It is therefore essential that these requirements are translated into plain English. We will refer to these plain English translations as "compliance obligations" and will create the obligations register. The keys to success in creating obligations from requirements are:

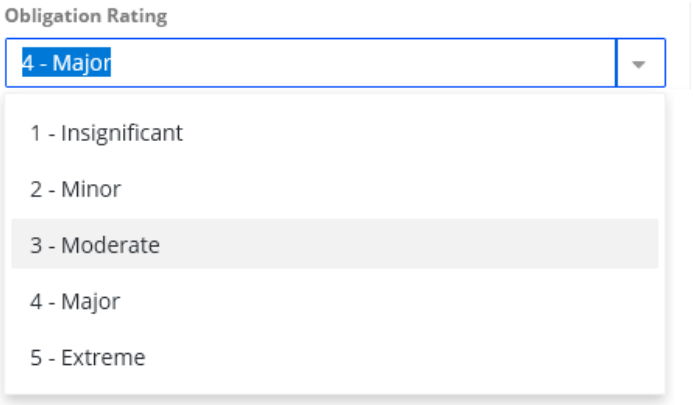
- The obligations need to be in simple, easy to understand language.
- There needs to be as few obligations as possible. This requires, where possible, obligations generated from multiple sources being combined into a single obligation.

This process is best performed by someone who has a legal background and yet also understands the nature and needs of the business. Again, it can be performed internally if you have the resources or use an external expert.

A risk-based approach should be applied to compliance so that most effort is applied to the highest risk obligations and less effort towards the lower risk obligations. This requires the obligations to be risk assessed.

We believe the best approach to this is to rate the obligations according to the size of impact if it were to be breached. This may include the impact from:

- Loss of licenses
- Fines
- Enforceable undertakings
- Reputation damage

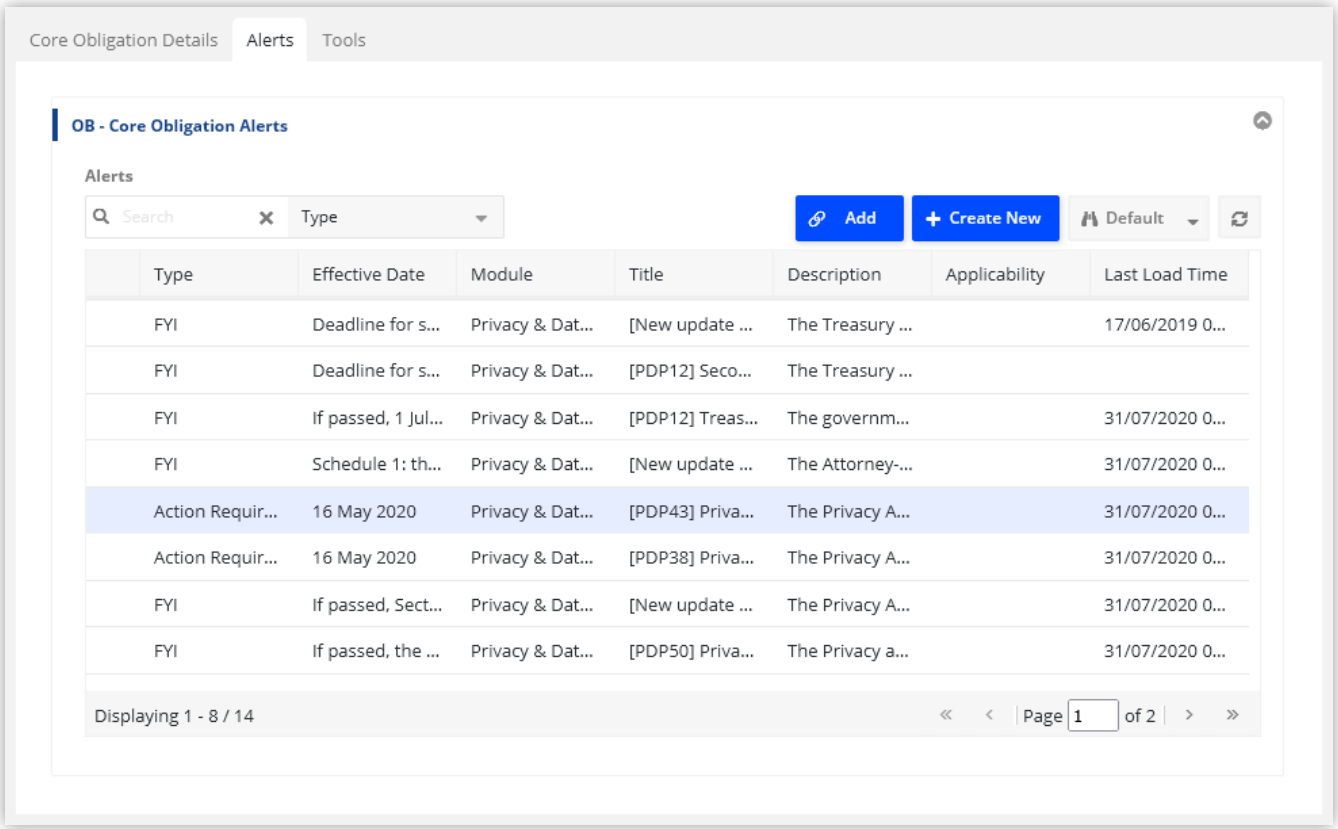


An Obligation Register can include a rating field based on the size of impact if the obligation were to be breached.

4.2.2 Other information and links to the Obligation.

It is also useful to attach other information to the obligation including

- Who is the primary owner and any interested parties?
- An assessment as to whether we are compliant with the obligation
- Date of last review – the frequency of review can be linked to the risk rating
- What attestations are being asked about the obligation
- What is the key risk linked to this obligation
- What are our key controls demonstrating compliance with the obligation



GRC systems can facilitate the circulation of legal and regulatory alerts to those who need to action it.

4.2.3 Keeping the obligation register up to date.

A critical and often difficult component of obligation registers is keeping them up to date given the ever-changing legal landscape. Organisations can subscribe to relevant industry bodies that supply legal or regulatory alerts via email and then update their obligation registers manually. The process of dealing with these emails and ensuring transparency on the importance of the alerts is often difficult and time consuming to manage.

The legislation and obligation changes then need to be circulated to those that need to action and understand the changed knowledge. GRC systems such as Protecht.ERM can be used to provide alerts and manage the process to action these changes.

4.3 Establish processes, procedures and policies that allow compliance.

The next step which can be commonly overlooked, is to ensure that business processes enable continuous ongoing compliance with obligations. This requires:

- Policies, processes and procedures to be put in place and maintained that enable the organisation to comply. These procedures should be linked to the relevant obligations in the obligations register to demonstrate how the processes meet the compliance obligations.
- Tools, such as checklists and attestations to ensure staff understand and follow the process.
- Training, to ensure relevant staff have the appropriate knowledge and skills to follow the processes correctly.

4.4 Carry out compliance functions.

On an ongoing basis, the processes and functions put in place to comply, must be followed and checks carried out that they have been followed. This will include such things as:

- Compliance attestations where responsible staff attest to their compliance with the relevant obligations.
- Independent reviews and checking including such things as call monitoring and file reviews.
- Mystery "shopping" to check whether staff follow the correct process.
- Maintenance and review of compliance training registers
- Consistent capturing of breaches and ensuring they are linked back to the relevant obligations.
- Where necessary treatment plans should be created to improve processes to prevent future breaches and systemic issues.

4.5 Reporting.

Relevant and timely reporting needs to occur on each of the above processes. This should allow all levels of the organisation, from Board to line management, to gain appropriate knowledge and assurance that these processes are performing. Reporting in relation to the obligation register should look to consider the following areas:

- Aggregation of obligations by risk rating
- Obligations deemed not compliant in the current state
- Alerts where a review is required
- Overdue treatment plans

The sample dashboard below displays a number of these concepts.

This Obligation Dashboard from Protecht.ERM provides an overview of the Obligations Register.

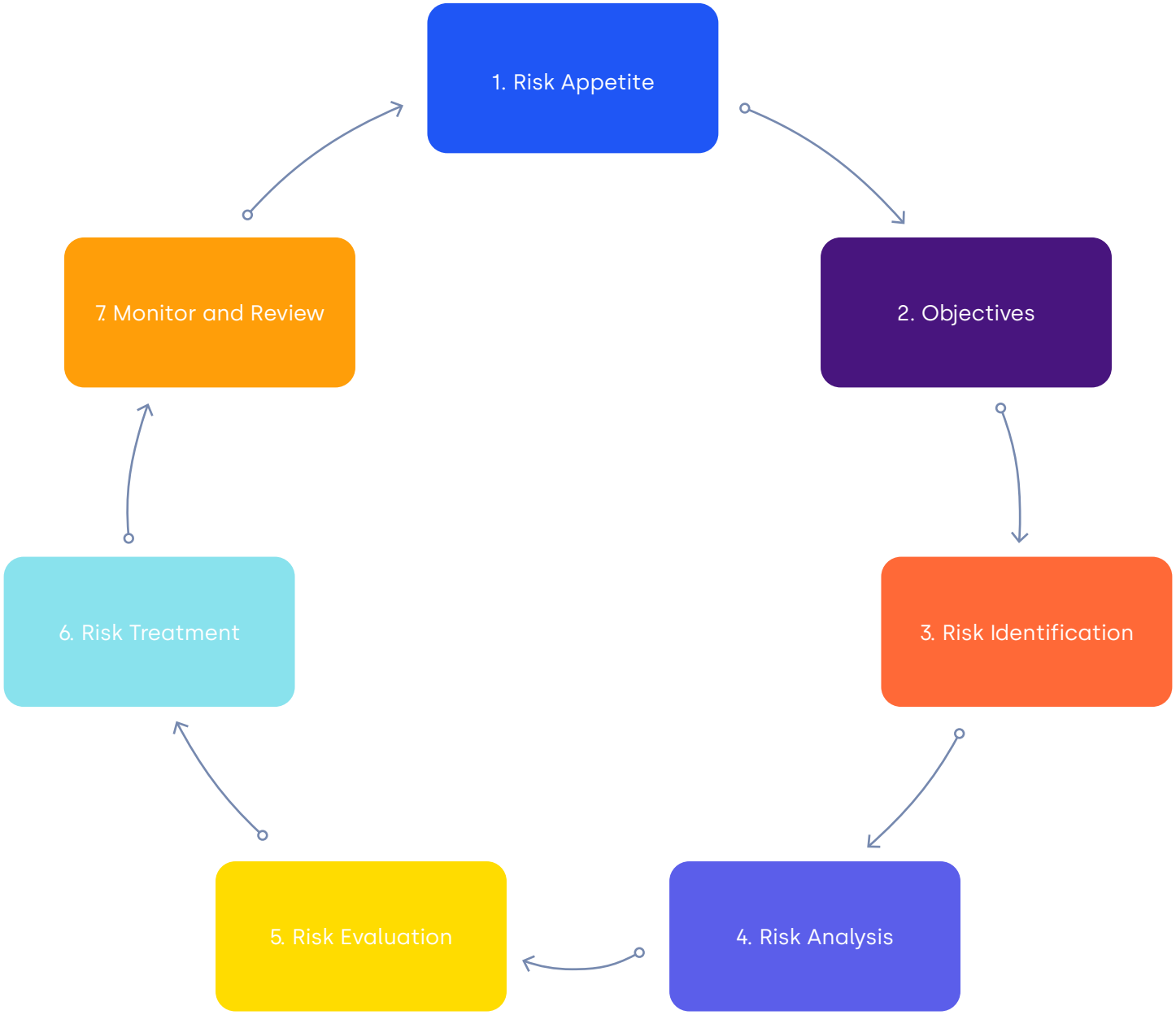
05

Compliance risk management.

Compliance risk management involves managing the risks within the organisation that could lead to non-compliance.

Compliance risk management consists of the following:

Those readers that are familiar with operational risk management recognize that this is the same process. This is because compliance risk is an operational risk and should be managed accordingly. The ISO 31000 Risk Management: Principles and Guidelines standard sets out the following 7 steps:



1. **Communication and Consultation.** This requires consulting with stakeholders to understand risk appetite. **Risk appetite for compliance risk** has been mentioned earlier.
2. **Understanding the Context.** This requires identifying the **objectives** of compliance which are commonly considered to be:

   "To comply in order to protect the organization from:
   - Financial loss including fines and management effort
   - Reputation damage
   - Regulatory action"
3. **Risk identification** involves identifying the key risks that could lead to non-compliance with the relevant obligation. Related controls over the key risks should also be identified.
4. **Risk Analysis** involves assessing the size of the risk. This is usually achieved by assessing the likelihood and impact of the risk.
5. **Risk evaluation** involves the comparison of the risk against risk appetite.
6. **Risk Treatment,** if required, involves changing the risk through internal controls, process re-engineering or avoidance.
7. **Monitoring and Review** involves the ongoing monitoring of the risks.

The above steps can be achieved using the standard operational risk management processes of:

- Risk and Controls Self-Assessment
- Controls Assurance
- Key Risk Indicators
- Compliance Breach Management
- Issues and actions management.

As we are taking a risk-based approach to compliance, we should only follow this process for the high risk obligations e.g. Level 4 and 5 ratings as per sections 4.2.1 above.

06

Compliance monitoring plans.

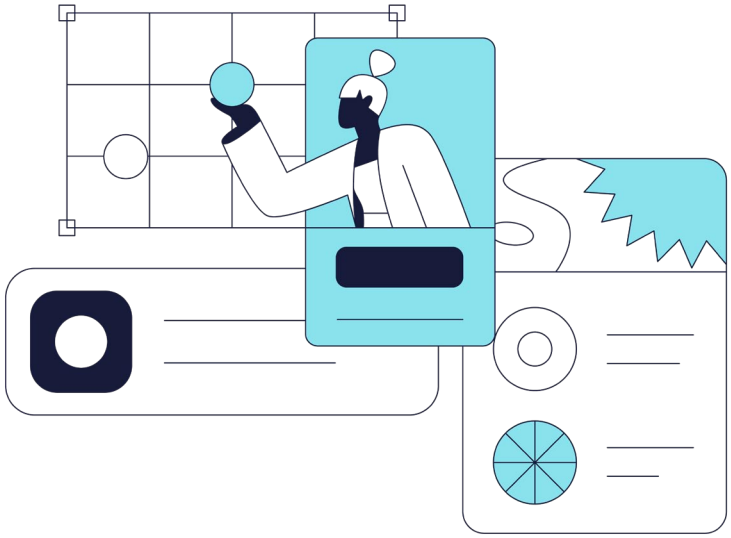
The above approach will lead to the development of your compliance monitoring plans which should be developed for each business within your organisation and should set out how compliance and compliance risk management will be carried out. This should be risk-based by applying the most effort to the highest risk rated obligations and the least effort to the lowest risk rated obligations. An example of this would be:

OBLIGATION RATING / TOOLS	1 - INSIGNIFICANT	2 - MINOR	3 - MODERATE	4 - MAJOR	5 - EXTREME
RCSA				Yes	Yes
Controls Assurance				Yes limited	Yes
KRIs				Yes limited	Yes
Compliance breach agreement	Yes	Yes	Yes	Yes	Yes
Attestations			Yes half-yearly	Yes quarterly	Yes monthly
Independent review	Yes bi-annually	Yes annually			
Mystery shopping			Yes annually	Yes quarterly	Yes monthly
Other...					

07

Conclusions.

Compliance is not easy and there is a need to ensure the correct balance between effectiveness and efficiency. If the compliance process is too onerous and cumbersome it will mean the business resists and it will be poorly executed. A risk-based approach that is supported by an efficient and effective compliance risk management system will give your organisation the best chance of being effective in managing its compliance.



Explore the main capabilities.

Protecht.ERM is an efficient, effective and agile risk management software packed with the following features:

- Compliance GRC Solution
- Compliance
- Key Risk Indicators
- Controls Testing
- Workplace Health and Safety
- Third Party Vendor Management
- Mobile Enabled
- Risk Assessment
- Obligations Content
- Business Intelligence and Analytics
- Audit
- Incidents
- Dynamic Form Builder
- Integration Capabilities

Visit www.protechtgroup.com/risk-management-software to find out how Protecht.ERM can help your organisation or email us at info@protechtgroup.com to arrange a system demo.

ABOUT THE WRITER

David Tattam

Chief Research and Content Officer

David Tattam is the Chief Research and Content Officer and co-founder of the Protecht Group. David's vision is to redefine the way the world thinks about risk and to pioneer the development of risk management to its rightful place as a key driver of value creation in each of Protecht's clients. David is the driving force behind Protecht's risk thinking, pushing risk management to the frontiers of what is possible. He is also focused on driving the uplift of people risk capability through training and content.

David is passionate about risk and risk management and in reaping the value that risk and good risk management can create for any organization willing to embrace it. He is particularly passionate about risk management research and is prolific in creating a wide range of content delivered in blogs, eBooks, webinars and training courses. He has developed Protecht's comprehensive suite of risk management training courses and has, and continues, to train many thousands of risk practitioners across the globe. David also manages Protecht's consulting business offering a range of risk consulting capabilities from Risk Management Framework to Risk Appetite Statement development.

He is also the author of "A Short Guide to Operational Risk".

Prior to co-founding Protecht, David was the Chief Risk Officer and Head of Operations for the Australian operations of two global banks. He started his career as a Chartered Accountant and Auditor with Grant Thornton and PwC. David is an Associate of the Institute of Chartered Accountants in Australia and New Zealand and a Senior Fellow of the Financial Services Institute of Australia.

ABOUT PROTECHT

Redefining the way the world thinks about risk.

For over 20 years, Protecht has redefined the way people think about risk management. We help companies increase performance and achieve strategic objectives through better understanding, monitoring and management of risk.

We provide a complete solution comprised of world class risk management, compliance, training and advisory services to businesses, regulators and governments across the world.

With our flagship SaaS platform you can dynamically manage all your risks in a single place: risks, compliance, incidents, KRIs, vendor risk, IT and cyber risk, internal audit, operational resilience, BCP, health and safety, and more.

We're with you for your full risk journey. Let's transform the way you understand and manage your risk to create exciting opportunities for growth.

AUSTRALIA & ASIA PACIFIC

+61 2 8005 1265
Level 8
299 Elizabeth St.
Sydney NSW 2000
Australia

EUROPE, THE MIDDLE EAST & AFRICA

+44 (0) 203 978 1360
77 New Cavendish Street
The Harley Building
London W1W 6XB
United Kingdom

NORTH AMERICA

+1 (833) 328 5471
4470 W Sunset Blvd
Suite 107
PMB 95227
Los Angeles California 90027

Visit our website:
protechtgroup.com

Email us:
info@protechtgroup.com