DYNAMIC GRC

Cyber-Security Management

The Maestro-Solution for Cyber-Security Management consists of a collection of Maestro-Templates which are designed to manage, control and evidence compliance with the regulations which apply to your business:

- **Governance –** responsibility, procedures, monitoring and reporting
- **Risk –** identifying risks, assessing criticality and mitigation approach
- **Outsourcing –** checks on Cyber-Security at vendors/service providers
- **Attacks** – identifying and reporting unauthorized activities

Fast & Flexible

Download pre-set Maestro-Templates to cover the Cyber-Security requirements of different regulators with an option to customize to meet your own specific requirements or build your own.

- **Download** – use Maestro-Templates prepared to meet best practice standards by Dynamic-GRC
- **Build** – prepare customised Maestro-Templates based on specific Cyber-Security risks
- **Copy & Edit** – use downloaded or self built Maestro-Templates and edit to specific requirements

Key Features

Powerful inbuilt security and internal controls to efficiently manage and evidence your GRC environment:

- **Targets –** apply control to regulated firms and by Cyber-Security Risks
- **Incident Identification –** rule based or manual assessment
- **Incident Assessment –** manual classification with reason of breaches and non-breaches
- **Responses –** text, dates, numbers, single select, multi select, attach, etc.

Cyber-Security Requirements

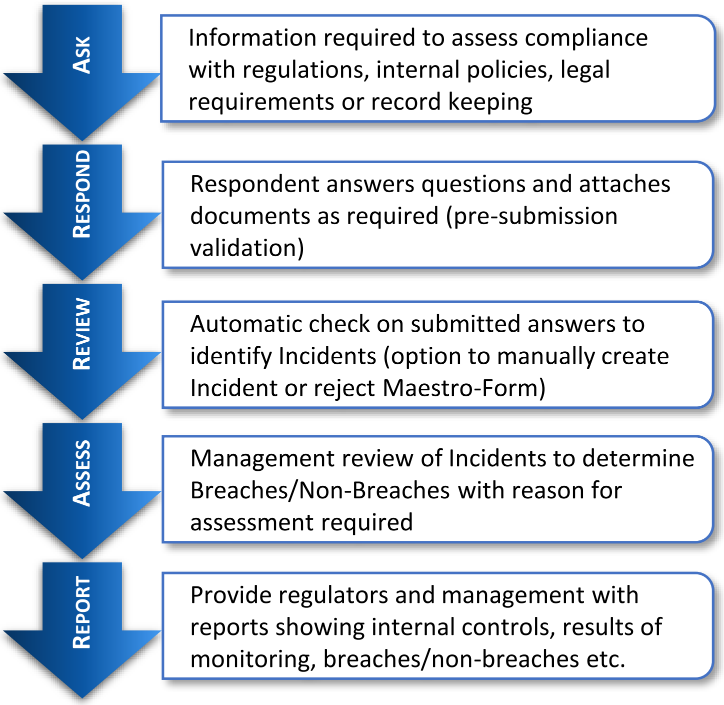
GRC-Maestro supports your Cyber-Security management requirements across your organisation.

The platform functionality is generic, specific checks and controls are built into your Maestro-Templates.

Regulatory Requirements/Best Practice

- **Governance**: Board Cyber-Security including escalation reporting of risks and attacks/actual breaches
- **Cyber-Security Officer**: including their qualifications and Cyber-Security strategy
- **Record keeping**: information required to evidence Cyber-Security management environment
- **Assessment**: how Cyber-Security risks are identified and quantified
- **Outsourcing**: ensuring that all outsourced software, services and systems have a Cyber-Security assessment and are periodically monitored
- **Monitoring**: the work performed to ensure that Cyber-Security risks are managed and actions taken to resolve risks and breaches
- **Reporting:** attacks and breaches: note that attacks can include unauthorized access by employees

Ask, Respond, Review, Assess, Report and Record



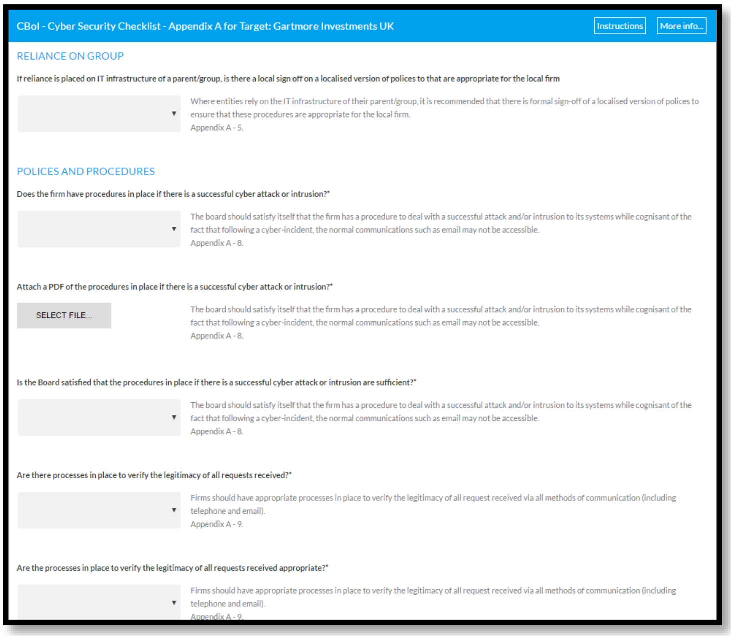
ASK — Information required to assess compliance with regulations, internal policies, legal requirements or record keeping

RESPOND — Respondent answers questions and attaches documents as required (pre-submission validation)

REVIEW — Automatic check on submitted answers to identify Incidents (option to manually create Incident or reject Maestro-Form)

ASSESS — Management review of Incidents to determine Breaches/Non-Breaches with reason for assessment required

REPORT — Provide regulators and management with reports showing internal controls, results of monitoring, breaches/non-breaches etc.



CBoI - Cyber Security Checklist - Appendix A for Target: Gartmore Investments UK

RELIANCE ON GROUP

If reliance is placed on IT infrastructure of a parent/group, is there a local sign off on a localised version of polices to that are appropriate for the local firm

Where entities rely on the IT infrastructure of their parent/group, it is recommended that there is formal sign-off of a localised version of polices to ensure that these procedures are appropriate for the local firm.
Appendix A - 5.

POLICES AND PROCEDURES

Does the firm have procedures in place if there is a successful cyber attack or intrusion?*

The board should satisfy itself that the firm has a procedure to deal with a successful attack and/or intrusion to its systems while cognisant of the fact that following a cyber-incident, the normal communications such as email may not be accessible.
Appendix A - 8.

Attach a PDF of the procedures in place if there is a successful cyber attack or intrusion?*

SELECT FILE...

The board should satisfy itself that the firm has a procedure to deal with a successful attack and/or intrusion to its systems while cognisant of the fact that following a cyber-incident, the normal communications such as email may not be accessible.
Appendix A - 8.

Is the Board satisfied that the procedures in place if there is a successful cyber attack or intrusion are sufficient?*

The board should satisfy itself that the firm has a procedure to deal with a successful attack and/or intrusion to its systems while cognisant of the fact that following a cyber-incident, the normal communications such as email may not be accessible.
Appendix A - 8.

Are there processes in place to verify the legitimacy of all requests received?*

Firms should have appropriate processes in place to verify the legitimacy of all request received via all methods of communication (including telephone and email).
Appendix A - 9.

Are the processes in place to verify the legitimacy of all requests received appropriate?*

Firms should have appropriate processes in place to verify the legitimacy of all request received via all methods of communication (including telephone and email).
Appendix A - 9.

Contacts

Australia & New Zealand: +61 2 8006 5008

Singapore: +65 9385 7455

UK & Ireland: +44 20 3286 0800

USA: +1 617 401 8009

Web site: www.dynamic-grc.com

Email: info@dynamic-grc.com

LinkedIn: https://www.linkedin.com/company/dynamic-grc