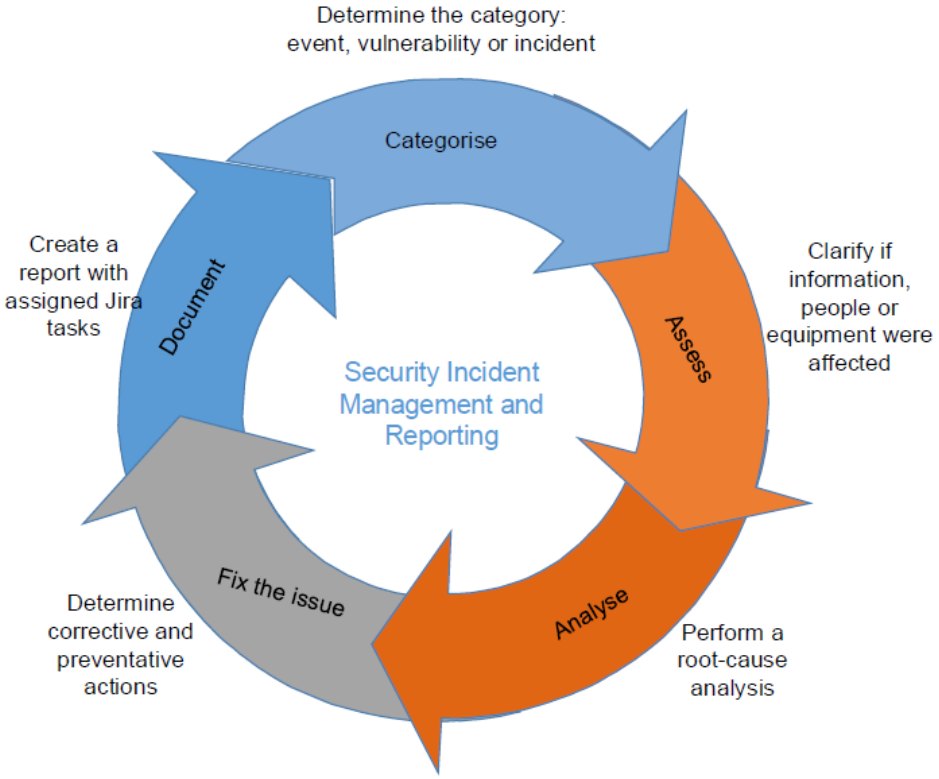
Compliance

1	Do you have any relevant certifications in relation to Information Security Standards that are held by your organisation (such as ISO 27001, PCI DSS, etc.)?	Yes. Maytech's Information Security Management Systems are ISO 27001 certified. Our certificate number is 10009780 and the certificate is available on request. Maytech's products are PCI-DSS compliant and our annual PCI-DSS SAQ (level D) and Attestation of Compliance are available on request. Maytech's services are also GDPR and HIPAA compliant.
2	Have your information security controls been assessed by an external auditor or certification body?	Yes. Maytech are audited twice a year by Lloyd's Register Quality Assurance — one of the leading business assurance providers in the world.

3	Can you fully disclose the scope under which Information Security was achieved?	Scope of Applicability: Information Security relating to the design, development, support and provisioning of Maytech's SaaS hosted services. Statement of applicability can be provided upon Customer's request.
4	Do you have the independently conducted third-party security control assessment, such as SOC 2 /SOC 1 reports?	Yes, for data centres. Maytech do not have a SOC 2 report. Our information security management systems are instead ISO 27001 certified, and audited twice a year by Lloyd's Register Quality Assurance, one of the leading global business assurance providers. The criteria / controls required by the two standards were developed to mitigate similar risks and there is considerable overlap in the criteria defined in the Trust Service Principles of SOC 2 and the controls defined in Annex A of ISO 27001. Both standards provide independent assurance that the necessary controls are in place and whereas ISO 27001 is an international standard with its origin in a British standard, SOC 2 is created and governed by the American Institute of Certified Public Accountants, AICPA.
5	Is your service suitable for Government data?	Maytech's government service and associated infrastructure is dedicated to public sector customers and is accessible from the internet. It is suitable for UK public sector customers with data sensitivity levels up to OFFICIAL and including OFFICIAL SENSITIVE. These categories represent up to 85% of data created or processed by the UK public sector. Maytech is a registered G-CLoud supplier (Service ID no: 110486484775596) and further information can be found on UK government Digital Marketplace.
6	When were written security policies last updated?	Policies are reviewed during monthly ISMS mgmt meetings and updated regularly, as necessitated or identified within review / training, as part of Maytech's Continual Improvement program.

7	Do you have a documented information security policy or program? If YES, what is covered by written information security policies?	Yes ISMS 01. This document provides a policy and framework of the main requirements of ISO 27001 that Maytech adheres to, in order to ensure that the company remains compliant. Our ISMS documentation includes regulatory obligations, all potential risk factors, policy & procedures, internal checking methods, recording, analysis and review which determines a proposed action.

8	Do you have any incident response programs in place?	All reports of information security weaknesses/incidents or events relating to any of Maytech's information assets are within the scope of:  If the incident results in unauthorised access to customer data we will inform the Customer within one hour on what actions have been taken and what controls are put into place to prevent any repeat incidents. Users are not allowed to continue working after identifying a possible weakness/incident or information security event which affects their activities.

9	Are your information security controls regularly assessed by an internal audit team? If so, please describe and provide their findings.	Yes, we conduct thorough internal audits which cover core aspects of the ISMS throughout the year. Results available on request.