REPLY
SYTEL

IS YOUR ORGANISATION CHALLENGED TO DEMONSTRATE SECURITY COMPLIANCE?

Any organisation, either operating within a B2C or a B2B environment, is constantly required by its clients to demonstrate compliance to industry standards, laws and regulations, with a current emphasis on security, and to provide evidence of their compliance posture. If as an organisation you are faced with the same challenge, Sytel Reply's Reve@l:Comply solution can help you tackle the problem by centralising your organisations' knowledge, allowing you to achieve compliance governance and demonstrate a proactive approach to your clients.

REVE@L:COMPLY

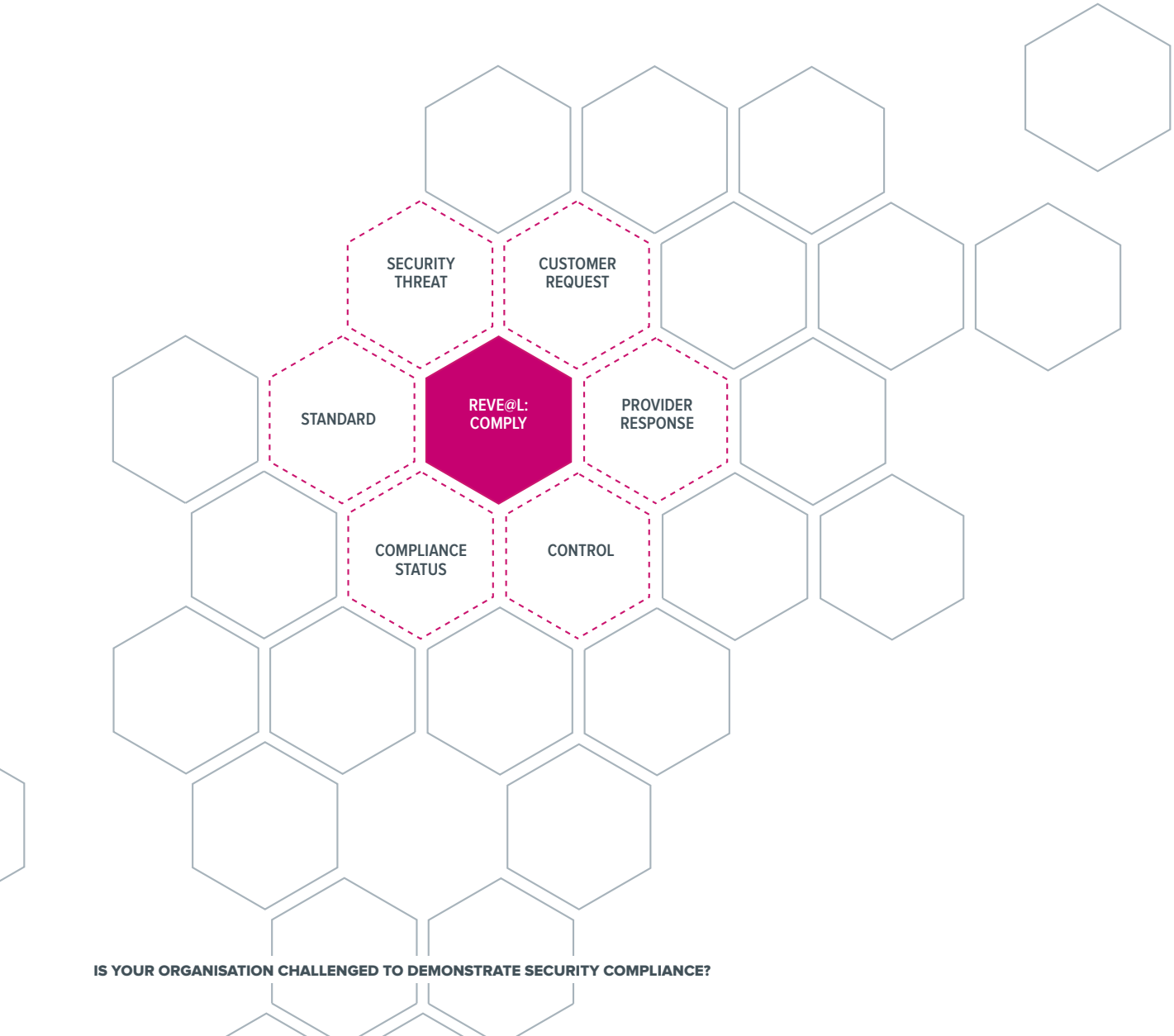
Organisations across the globe, and in particular those providing communication technology services to other enterprises, are increasingly required to provide evidence of compliance to industry standards, with a current emphasis on security. This could be required both on an ad-hoc, or recurring basis.

In most cases, requests from external parties arise in the form of Requests for Information (RFIs) or due diligence questionnaires, which consist of a series of questions regarding the organisation's (Provider) conformance to one or more industry standards, laws or regulations.

More often than not, Providers approach these requests following a manual, or semi-manual process, resulting in non-efficient resource and time allocation. Through Reve@l:Comply, Sytel Reply provides a solution to reduce the overheads required to respond to Customer RFIs or due diligence questionnaires by means of automation relying on an authoritative Knowledge Base. This provides a repository for Security Standards and associated Threats, related Provider Responses supported by Provider Evidence, as well as Customer RFI details.

The result is a significant reduction in resource and time demands, due to the boilerplate Provider Responses linked to related Policy, Process, Standards and Operational Evidence artefacts; all mapped to the Controls of the Standards for which compliance statements are requested.

When the Knowledge Base information is properly maintained, the quality of Provider responses increases incrementally and superior responses are provided to Customers.



IS YOUR ORGANISATION CHALLENGED TO DEMONSTRATE SECURITY COMPLIANCE?

SECURITY & COMPLIANCE TRENDS

Security has always been in scope of the agenda for most organisations. Within the past few years organisations have been investing in protecting themselves from security threats and have acquired the means (technological, people, processes) to monitor, detect and respond to threats. However, an exponential increase of attacks, accompanied by a number of publicly announced data breaches as a result of these attacks have increased the focus on security and compliance governance. The following list details a number of drivers, which contributed to the increase of focus in security and compliance.

Advance Persistent Threats: Until recently organisations have been investing in protecting themselves from external threats and attacks mainly targeted at loss of service, such as Distributed Denial of Service (DDoS) attacks. It was recently proven that attacks of Advanced Persistent Threats, where attackers have gained unauthorised access to organisational data and remained undetected for long periods, have been realised.

Major Data Breaches: Recent cases of data breaches, such as TalkTalk, Experian, Ashley Madison, Anthem and Premera BlueCross, have demonstrated that data breaches are a reality even for large organisations with numerous security controls in place. These attacks have contributed to a shift in mentality across the industry from “My organisation is well protected” to “My organisation can be attacked at any time, regardless of how well protected it is”.

Governmental and Industry Security Standards: Security and compliance governance, alongside of data protection and privacy, are on the top of global agendas within governments and industry bodies. The UK recently published the ‘Cyber Essentials Standard’ to which UK companies have to comply; the EU is publishing a revision to the previous Data Protection Directive requiring all businesses operating within EU countries to comply with the General Data Protection Regulation; Industry standards, such as ISO27001, are becoming a baseline requirement for companies offering services, rather than a brand differentiator.

All of the aforementioned drivers result in increased requirements for organisations to demonstrate compliance and prove their effectiveness in regard to both the design and the operational aspects of security controls that they have in place.

THE CHALLENGE

It has been demonstrated that organisations are not fully aware of where the risks are and whether the security measures they have in place are adequate. It is also apparent that organisations will need to adopt a comprehensive security and compliance governance framework, in order to compliment their ability to offer their services to their clients, as well as demonstrate compliance as part of their legal and regulatory requirements.

Today most organisations have adopted a reactive approach, especially when required to demonstrate compliance as part of their sales cycle and interaction with clients. In most cases, requests from external parties arise in the form of Requests for Information (RFIs) or due diligence questionnaires, which consist of a series of questions regarding the organisation’s (Provider) conformance to one or more industry standards, laws or regulations.

Providers have to face a number of challenges during this process, since normally they are required to provide formal responses to these requests, including some of the following:

- Significant demands on resources and time if the process of responding is manual, or semi-manual;
- Repetitive and incremental processes, consuming significant time and requiring reworking of responses until external parties are satisfied with the level of detail of the information provided;
- Due diligence questionnaires and RFIs vary in format, although they are based in the same overall information security principles, creating further delays as understanding and clarifications might be needed;
- Requirements are sometimes tailored to specific country legislation, which requires further investigation and detailed analysis to be conducted.

More often than not responses are inconsistent, the effort and time invested in such activities offers limited value and the knowledge captured as part of this process is not monetised.

THE SOLUTION

An increasing number of organisations have decided to adopt the ISO27001 standard requirements as a baseline for maintaining security within the organisation, and have also acquired the equivalent certification to be provided as a proof to their customers. For some organisations a certification may suffice as evidence to secure a sales deal and provide their services, however for most the requirement of responding to custom due diligence questionnaires and RFIs still remains. In addition those that have adopted ISO27001 are required to demonstrate their compliance to the standard and maintain an Information Security Management System to capture control status, as part of continuous improvement.

Sytel Reply has created **Reve@l:Comply, a component of a larger solution, which is aimed at informing and assisting anyone who is interested in the Security Standard Controls that mitigate a Security Threat, thereby assisting them in managing their Standards Compliance activities and demonstrating their level of compliance.**

In addition to managing their compliance requirements, **Reve@l:Comply** offers a number of benefits and capabilities to a Provider, allowing them to:

- **Capture Customer specific questionnaires and RFIs** and associate their particular questions to the Provider's standard response;
- **Map specific controls to security threats,** in order to mitigate related attacks and decrease their risk footprint;
- **Maintain an inventory of evidences and artefacts,** associated to specific controls, in order to demonstrate operational efficiency of these controls;
- **Capture location specific requirements and demonstrate compliance** against different regions, assisting them in expanding their offerings.

Sytel Reply's **Reve@l:Comply** can be paired with **Reve@l:Verify,** which is a custom tool designed to provide a picture of the security posture of a network within minutes by simply specifying the network domain of interest. The two solutions together allow an organisation to proactively identify threats and implement adequate security controls for their mitigation, whilst at the same time demonstrating compliance.

REPLY
SYTEL

Sytel Reply UK is the Reply Group Company specialising in an open and pioneering consultancy approach that helps clients successfully innovate and transform in today's ever-changing digital world. With a 'Give to Get' mentality, Sytel Reply UK enables clients to grow through the development and delivery of secure, compliant and future-proofed solutions for some of the largest telco and media enterprises worldwide. By bridging the gap between technology and business, Sytel Reply UK focuses on increasing revenue streams and efficiency, whilst reducing costs and time to market.

Founded in 2010, Sytel Reply UK is a focused, dedicated, agile group of talented and experienced technologists and consultants. Sytel Reply UK is part of Reply, a network of highly specialised companies focused on the design and implementation of solutions based on new communication channels and digital media.

www.reply.com