resill!on

Quality: Engineered. Tested. Assured.

Datasheet

Cyber Health Check

Cyber threats to businesses are increasing daily, leaving many without the resources to effectively manage the risks or even unclear on what they need to do. This is especially true for businesses that don't possess either the knowledge or experience to tackle the problems today's technology can bring.

A common solution is security frameworks, addressing information security in a holistic fashion. Looking at areas such as physical security, legal requirements and even your supply chain. There are a multitude of frameworks available, so how do you know which one is right for you?

Recognising this is a frustrating issue for many organisations, Resillion has developed its own Security Framework to address the problem. We've taken four nationally and internationally recognised standards, including ISO/IEC 27001 and Cyber Essentials, and extracted the most important and appropriate controls which have a direct bearing on your cyber defences across your entire organisation.

The Process

We will interview your key players, review the evidence of your cyber security journey, and provide you with a written assessment of your maturity level across multiple domains, aligned to the Cyber Security Body of Knowledge (CyBOK) knowledge areas:

- Human, Organisational & Regulatory Aspects
- Systems Security
- Software and Platform Security
- Infrastructure Security
- Attacks & Defences

Our detailed report will quickly and clearly demonstrate where your accomplishments lie and where action is needed. The results will help you become more secure and achieve a comprehensive level of protection. From the outcome you will know where to apply your resources for the best return.

Key Features & Benefits

- Hybrid approach encompassing accredited cyber directives
- Practical, straightforward assessment
- 119 requirements spanning 19 key zones
- All 19 zones aligned to the CyBOK Knowledge Areas
- Maturity measures derived from COBIT 2019
- Highlight and action specific areas of concern

Areas of Assessment

- Planning and risk management
- User education and awareness
- Employee screening & responsibilities
- Supplier security management
- Contingency planning
- Legal and other external requirements
- Removable media use
- Logical access control
- Secure configuration
- Remote working and mobile devices
- Management of assets
- Patching, change, & life-cycle management
- Physical and environmental security
- Malware protection
- Monitoring
- Incident management
- Network & cloud security
- Software development