
QUOD
ORBIS
The importance of Cyber Security Controls
in Digital Risk Managment

Why Good Controls Deliver Good Security

According to Gartner the newly labelled Digital Risk Management space is a new and exciting addition to the Information Risk Management landscape. With constant breaches, threats and evolving technologies CISO's and CIO's must prepare, says Gartner, amidst an unprecedented rise in sophisticated cyber attacks.

Failure to act is having significant impact on organisations and business leaders need to take action for the future, by creating long term digital risk strategies.

In recent years protecting and defending organisations has become more complex due to the changing technological landscape and the emergence of sophisticated attacks. With the volume of security breaches and the levels of risk rising at unprecedented rates, cybersecurity strategies need to adapt.

Organisations are spending a phenomenal amount of energy and cost on controls to meet their obligations for compliance and their security concerns, yet most don't have confidence they are performing adequately, or their risks are materially reduced. The news of regular breaches and fines worldwide compounds this, as does ever changing regulatory complexity.

What do we mean by controls?

Used as safeguards or countermeasures in cyber security to prevent, detect and minimise the risk of a security breach to property, information or assets, controls can be positioned to activate at any stage of an attack.

Due to the increasing number of cyber security breaches, governments have implemented legislation (such as GDPR) which stipulates the base line controls a company must implement in order to protect data and reduce the number of successful incidents.

There are many dimensions involved to improve an organisation's security, some are more important than others, but without the right security controls businesses are not only open to fines for non-compliance, they are also more susceptible to an effective attack.

Controls are measures which are put in place to mitigate a known risk or meet a compliance requirement. Controls can be placed in three main categories:

- **Management Controls** – Focus on the management of risk and information system security through the planning and assessment of methods to reduce or manage risk. Some common management controls are; Risk Assessments, Vulnerability Assessments and Penetration Tests
- **Operational Controls** – Usually implemented to ensure the day to day operations of an organisation assist an overall security plan. These are processes which are implemented and executed manually such as Media Protection, Security Cameras, Locks and Password Security Training
- **Technical Controls** – Using technology to reduce risk and vulnerability, they are primarily implemented through hardware, software or firmware and can come in the form of encryption, antivirus software, firewalls and intrusion detection systems.

Due to the broad spectrum of their nature, controls come in all shapes and sizes, for example:

- A CIS critical control such as separate privileged administrator accounts from standard access, or can be as simple as something on the risk register such as; "for high risk environment LEGACY, do not permit direct connections and ensure the environment is isolated" or to meet a compliance requirement such as PCI, SOX, GDPR; "rotate database encryption keys annually."
- A process such as the implementation of a vulnerability management programme or recording visitors into a Datacentre.

Risk is all about controls. Compliance is all about controls. Good security is about good controls.

An example of how compliance controls bear little application to a business can be demonstrated in Formula 1 Racing. Aside from the key GDPR compliance controls, there are not many others which apply. Instead, additional controls are needed to reduce their exposure to attackers who want to steal their IP. Not only do they need to protect their intellectual property, they need to prove to their sponsors and clients that it is in safe hands.

Compliance vs Security

For many organisations the controls required for compliance also help to mitigate a lot of security risks. It would therefore be understandable for an organisation to fall into the trap of believing that compliance controls are all that would be required to secure their business, however the reality is not the case.

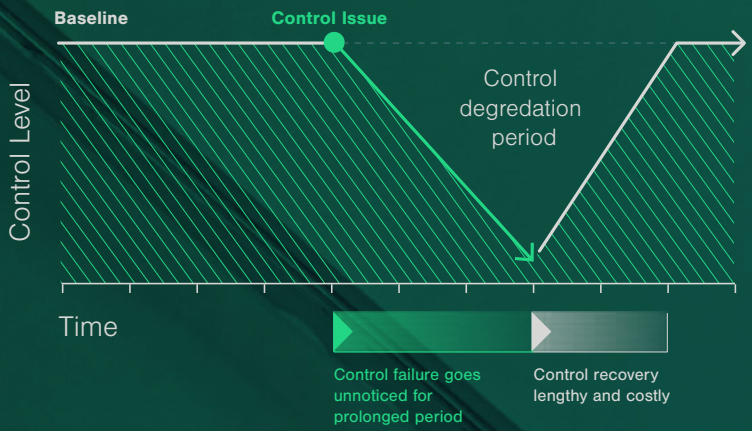
Compliance controls are the baseline in cyber security. It is certain that standards such as ISO 27001 with its 133 controls can significantly reduce risk of a security breach and is seen as an established standard of excellence, however, risk profiles differ from business to business.

A concerning number of organisations automatically put controls in place to meet compliance requirements rather than assessing and identifying their greatest security risks and analysing how they can mitigate their exposure. Compliance controls are quite prescriptive and are well documented, but risk is a little more vague.

Historically, analysing security risk was founded upon a “finger in the air” approach to determine whether each area held a high, medium or low potential of occurring. Today there is a more modern approach to assessing risk and identifying specific control requirements, which is more quantitative and science based.

Whilst technology plays its part to make its own assessments, there is a need to pair this information with expertise and knowledge. The potential downfall of internally assessing a company’s own security is that opinion and knowledge may be skewed towards an individual’s own view of how likely it is for each risk to occur. This results in the automatic elimination of controls which should ideally be implemented, so it is always prudent to seek external consultation to check nothing has been missed and lend a more global perspective to the options available.

Monitoring Controls – The Challenge



Control monitoring can not be 100% automated and human error has to be factored in.

Until recently, monitoring controls was time intensive and difficult. Typically a team of 5 people could only cover the bare minimum in terms of monitoring them, so it comes as no surprise that many manually monitored controls were audited once a year and then left to their own devices.

In addition to the time intensive management of controls, many are put in place and forgotten about. With the volume and intensity of attacks faced by cyber security teams increasing, it is easy to understand why the process of identifying, monitoring and automating controls is sinking further and further to the bottom of the “to do” list. More often than not, planning and processes to protect an organisation are taking a back seat whilst security teams are fire fighting against daily attacks.

In today’s business environment, there is increasing importance placed on the need for continually monitoring controls. Not only do they degrade over time, but they fail often and can go unnoticed for prolonged periods until a major incident or an audit occurs. Closing this potential weak point for attackers can only be undertaken through perpetual analysis.

The problem stems from a lack of centralised, real-time visibility of controls and their status.

Most GRC programmes input the data for risk and the corresponding control status manually, which is followed up by a GRC team. Due to the current cyber security skills crisis, GRC teams tend to be understaffed and cannot capture all control statuses with cadence, if at all.

Automating Control Monitoring

To determine how far it is possible to automate the monitoring of controls, the standards for compliance must be analysed to ensure the integrity of the control is not compromised through automation.

The evolution of technology has enabled the automation of control monitoring in many cases, ensuring controls are constantly checked and optimised. This introduction could not have been more timely – automating processes where possible provides a welcome relief to the pressure security teams are facing.

The supply of software providers to help automate controls is growing, but there is an increasing gap in expertise and knowledge which is required not only to identify the controls needed, but also to analyse the information generated through continuous monitoring. Relaying results to senior teams along with advice and practical solutions to improve overall security processes is a key element of control management.

The Quod Orbis Solution

Security Just Got Easier

Quod Orbis deploys real-time monitoring and automation of controls, through a simple but effective blend of software and consultancy. Rather than wait every 6months for a control audit, we monitor them on a continuous basis to ensure they provide the optimum protection for our clients.

The Quod Orbis bespoke platform monitors and automates controls for known cyber risks and compliance, along with security metrics and reporting. Our consultants follow this with an assessment of manual controls, advice on the security metrics generated and recommendations to drive positive change through the business.

We truly believe the key to good security is good controls and our blended consultancy and software approach is key to providing that. Extracting useful information from various supporting tools is somewhat the easy bit, making sense of and fully utilising the data is key.

Our team believe that technology is nothing without the people and expertise around it, our cyber security experts develop customer-focused, bespoke solutions every day. We have a unique set of skills and years of experience delivering enterprise-grade consulting across financial services and large corporations to Governments and household brands ensuring PCI and GDPR compliance.

With years of experience, skill and knowledge, Quod Orbis has proven to deliver impactful results. Through clearly and simply defining the issues and reporting against specific goals, we deliver transformative results which cut through the hype to help secure businesses around the world, giving each one complete peace of mind.

If you need more guidance and advice on the controls applicable to your business, or would like to learn more about the Quod Orbis solution, contact the team on contact@quodorbis.com

Contact us

If you need more guidance and advice on the controls applicable to your business, or would like to learn more about the Quod Orbis solution, do not hesitate to get in touch.

A: Quod Orbis, 33rd Floor, 286 Euston Road, (Euston Tower), London, NW1 3DP

T: +44 (0) 203 962 2206 E: contact@quodorbis.com

quodorbis.com