
avertro
The cyber-why company

SOLUTION BRIEF

avertro
The cyber-why company

OVERVIEW

Avertro is the strategic cybersecurity headquarters that helps leaders manage the business of cyber. The CyberHQ™ Software-as-a-Service (SaaS) platform helps elevate your game by:

- Explaining cybersecurity to executives
- Forecasting outcomes
- Right-sizing spend
- Validating cyber strategies

This allows organisations to optimise the use of external assistance and prove you are doing cyber right.

INTRODUCTION

One of the key challenges facing leaders is the disconnect between the cyber team and everyone else, particularly with the executive layer.

Organisations continue to struggle with aligning the tracks. The promise of Governance, Risk and Compliance (GRC) technology was to address this. The reality is that teams still need spreadsheets and consultants.

We can do better than the GRC and spreadsheet status quo. Elevating our game requires a focus on the business representation of cyber and building that permanent bridge to translate and normalise cybersecurity for everyone else.

CYBERSECURITY HEADQUARTERS

Avertro CyberHQ™ can streamline and automate up to 75% of an organisation's manual effort by taking relevant data points, calculating, normalising, and translating them into a taxonomy that makes sense to executives and board members, giving cybersecurity leaders the power to make their business case, and continuously prove they are doing cyber right.

Only by bringing business concepts to the cyber discussion can we finally illuminate the strategic value of what has traditionally been perceived as a tactical cost centre. Avertro aligns everyone with the cyber mission to ensure its success.

Most importantly, we help elevate the security team to where they deserve to be: the heroes in the story.

SOLUTION BRIEF

avertro
The cyber-why company

SEGMENTATION

A common challenge for most organisations is that different locations, business units, logical groups (e.g. IT vs OT), or subsidiaries need to be treated differently when it comes to cybersecurity. For example, the cyber resilience of head office may need to be higher than a remote outpost. Current solutions do not provide enough precision and fine-grained control to account for these differences.

Avertro CyberHQ™ supports the ability to segment an organisation into its constituent sub-components, manage each separately, while providing the power to consolidate, compare and aggregate cyber resilience management and reporting to provide distinct segmented lenses, as well as a pan-organisational view on cyber resilience.

COMMON USE CASES

- Produce board and executive narratives with a single click.
- Perform a cost benefit analysis of your cyber program and operational spend.
- Compare budgetary program options tied to outcomes.
- Continuously track current and target state cyber risks.
- Continuously track current and target state cybersecurity controls, capabilities and services.
- Continuously manage your cybersecurity transformation program and strategy.
- Manage issues (e.g. penetration test findings, audit findings, vulnerability scans) and have these influence business-level cyber risks at all times.
- Manage third party and project cyber risk assessments.
- Auto-translate between cybersecurity standards (e.g. translate between NIST CSF and ISO27001).
- Continuously assess the effectiveness of controls.

OUTCOMES

- No more spreadsheets.
- Manage and model the business of cyber and right-size spend by aligning costs with outcomes that make sense to all stakeholders.
- Forecast and predict strategic outcomes and timelines.
- Streamline the way continuous cyber risk management and assessments are done.
- Solve your Governance, Risk and Compliance challenges in a fit-for-purpose manner.
- Repeatable, standardised executive and board reporting for cybersecurity.
- Prove you are doing cyber right.

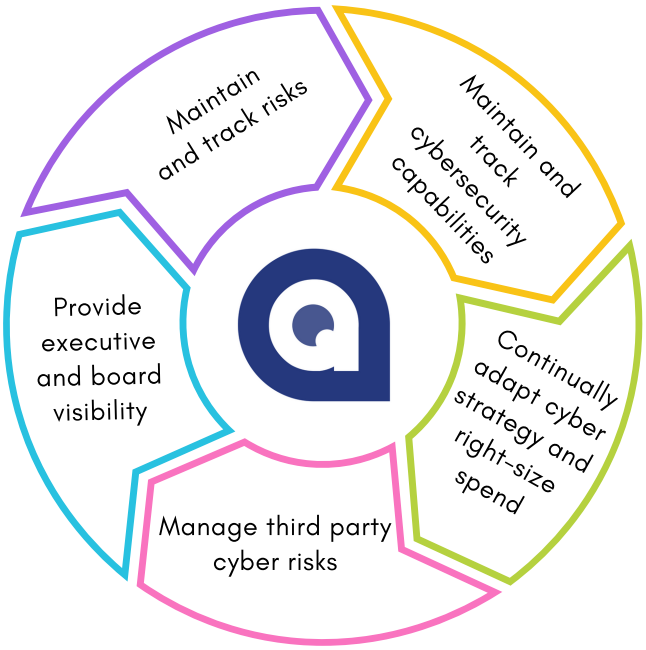
SOLUTION BRIEF

avertro
The cyber-why company

SOLUTION

Avertro is designed to provide organisations with the ability to manage and translate cybersecurity in a normalised way and facilitate a cycle of continuous improvement for cyber resilience and maturity.

The illustration below outlines the iterative process which allows an organisation to measure, track, plan, visualise and improve their cybersecurity posture. Each component of the Avertro platform addresses a section of the illustration and provides an intuitive way to bridge the gap between cybersecurity and executive teams.



The platform empowers cybersecurity leaders to take control of their strategic cybersecurity function which traditionally would have required external consultants, spreadsheets, and GRC tools.

The ability for the platform to ingest and model security data enhances the picture further, thus providing a holistic, consolidated view of an organisation's cyber resilience posture. Operationalising, streamlining and automating the processes involved and the ingestion of data provides an up-to-date representation of the cyber risk that is present within an organisation, and enables the true agility required to adapt to the risks at hand.

SOLUTION BRIEF

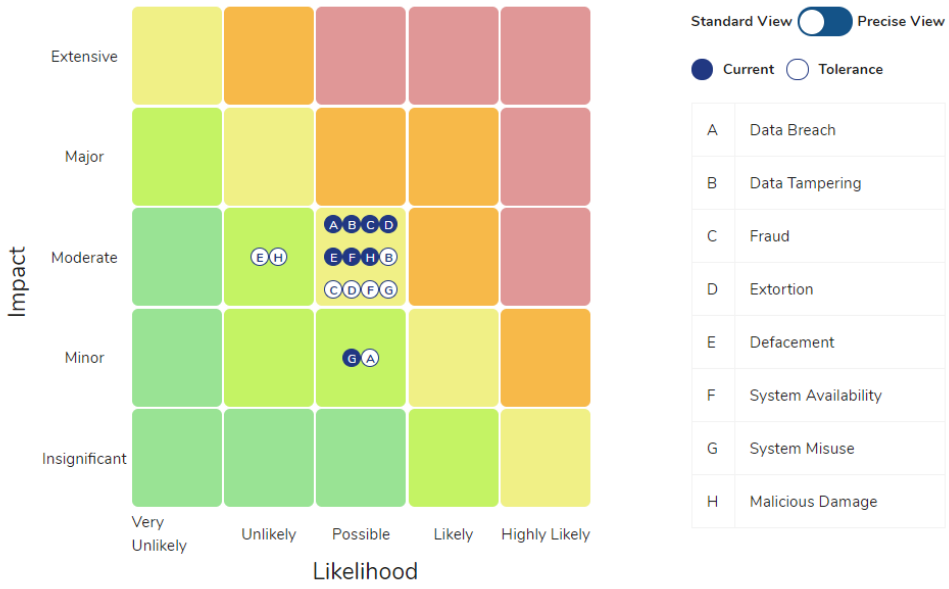
avertro
The cyber-why company

CYBER RISK

Cybersecurity is ultimately about managing risk. The Avertro platform fast-tracks an organisation's ability to identify, track and manage its cyber risks for executives at the business level, as well as cybersecurity teams at the technical level.

Business Risks

Avertro provides a set of pre-configured, industry-curated business-level cyber risks and key risk indicators. In addition, the solution can be adapted to fit existing cyber risks being managed as well as align with an organisation's enterprise risk framework.



The combination of fast-tracked onboarding and adaptability to existing taxonomies is a powerful ally in supporting the diverse challenges that organisations face across the various aspects of their business.

Most importantly, the risk-driven approach serves as a powerful representation of cybersecurity within an organisation that helps contextualise the strategic conversations required between cyber leaders, other executives, and board members.

The cyber risk posture of an organisation shifts over time and this is reflected within the platform. In addition, the cyber risk position of the organisation at any point in time is always available for historical reporting and trending. As a bonus, the platform is able to forecast cyber risk posture for an organisation when all aspects of the platform are properly utilised.

SOLUTION BRIEF

avertro
The cyber-why company

Issues

Cybersecurity issues are a constant in the digital world today. Zero-day vulnerabilities are a source of panic for most organisations since news of a breach can do massive damage to not only the organisation's finances but also its reputation.

The platform allows an organisation to manage and track issues that can impact its cyber resilience position. Issues that arise can and should increase the business-level cyber risks that are being managed.

Issues being managed within Avertro CyberHQ™ can come from various sources, including penetration testing findings, security audits, or vulnerability scans. The issues management module can function as a technical risk register and allows a cybersecurity team to take complete control of day-to-day operational issues.

While they remain open, issues can increase business-level cyber risks, and will have remediation steps that need to be completed before they can be resolved. Each issue can be closed as having been resolved or accepted; when resolved, an issue no longer affects the business-level risks it was tied to.

CAPABILITIES

Cybersecurity capabilities are managed using various lenses. The most commonly used lens involves the tracking of controls maturity over time against a framework of choice such as the NIST CSF. An alternate and complementary lens is the use of a logical security services catalogue, which allows teams to track capabilities in the form of operational services being provided to the organisation.

SOLUTION BRIEF

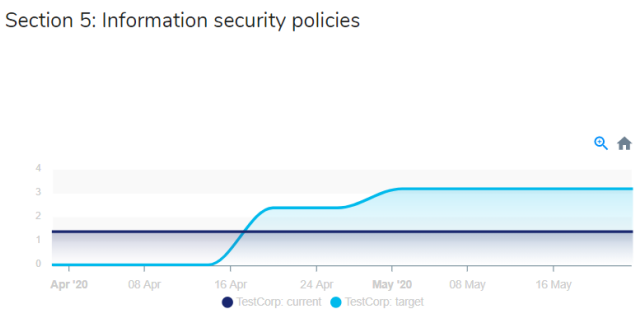
avertro
The cyber-why company

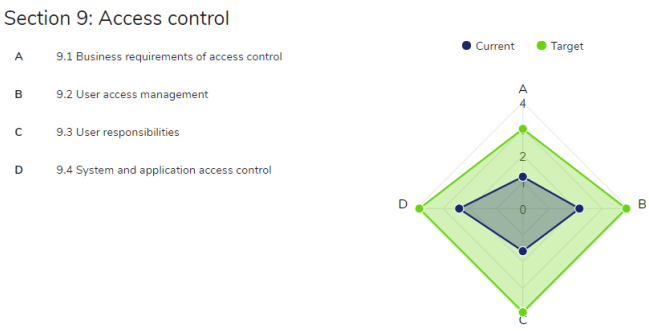
Controls Maturity

Maintaining and tracking cybersecurity control maturity levels is typically the first step in any cybersecurity uplift initiative. Avertro CyberHQ™ provides an intuitive yet functionally rich controls maturity module to continuously assess, score, validate, and periodically attest to the effectiveness and maturity of each control and identify gaps.

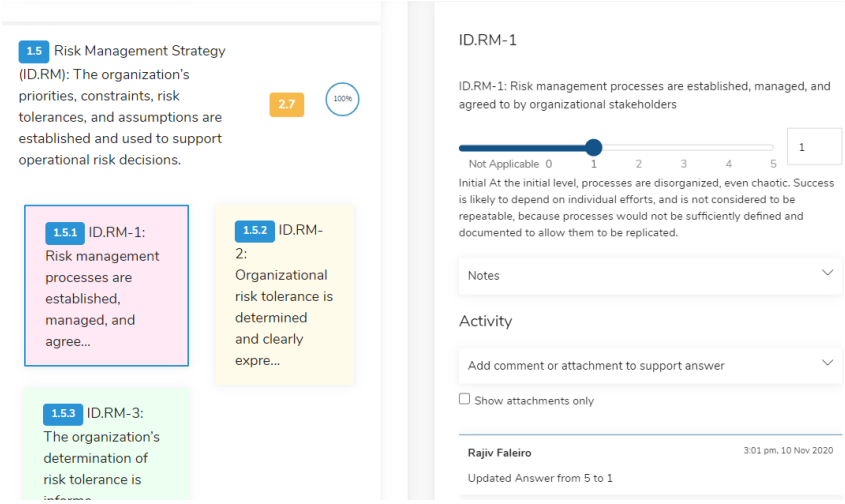
This can be based on standard frameworks such as NIST CSF or ISO27001. The platform supports a few common frameworks out-of-the-box, and allows the configuration of custom frameworks.

Organisations can also choose to use the Avertro Framework, which is based on the NIST 800-53 standard. This path removes the ambiguity and subjectivity that is sometimes present in controls assessments, and allows the organisation to use more of the rich, expert capabilities available in the platform.





A full audit trail is maintained to ensure audit requirements can be easily and painlessly met. On completion of your assessment of choice, reporting and visualisation of how an organisation scores against a framework is provided so that executive level reporting can be achieved to highlight any gaps within an organisation's cybersecurity maturity.



Security Services Catalogue

The ongoing maintenance of the services that the security team provides to an organisation is something that most cybersecurity leaders find challenging to manage. The platform makes this easy as we have pre-configured building blocks to support the creation and maintenance of an operational logical security services catalogue.

As is the case with other modules, we provide the flexibility to create and edit our service catalogue in a way that fits any organisation. In essence, the platform fast-tracks the onboarding of an organisation, but allows enough customisation to ensure it is fit-for-purpose.

The platform also continues to maintain the relationship of each security service with all related aspects across the platform, including the assets and technologies being used to support each service, as well as the relevant controls.

STRATEGY AND THE BUSINESS OF CYBER

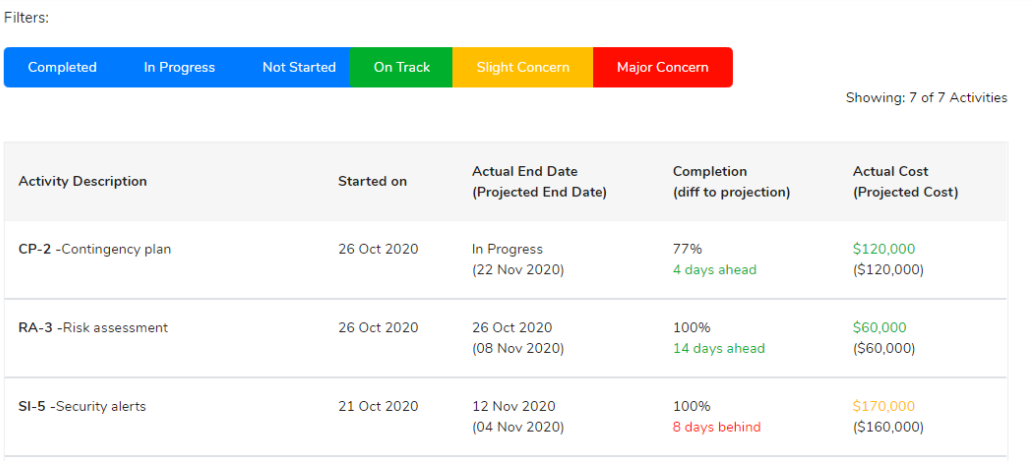
Cybersecurity program management can cover a spectrum of teams and a multitude of different conditions can affect its completion. In most cases, the cybersecurity transformation program becomes known as the cyber strategy. It is, in effect, the strategic plan to improve cyber resilience over time.

The key components from an executive and board standpoint are:

- Duration
- Cost
- Outcomes (in terms of risk mitigation)

Most organisations struggle to right-size their strategy in terms of finding the optimal spend for the desired outcome. Add the fact that cyber risk is a moving target, and it is an extremely difficult challenge to ensure one's cyber strategy is optimised at all times. The continuous visibility and business-lens required to manage this in an agile manner is something that very few have.

The platform provides these capabilities in the form of a program management foundation, pre-loaded with our library of activities, but still maintaining the required level of flexibility to support existing cyber strategies.



All cyber program activities managed in Avertro CyberHQ™ are tied to capabilities, which allows us to model outcomes in terms of cyber risks being mitigated, controls maturity improvements, and overall cyber resilience posture. The module provides foundational project management and reporting capabilities, as well as hooks into cyber resilience metrics that allow us to forecast and project outcomes in the future.

We are able to calculate cost-benefit metrics across the activities, projects and the program as a whole. This power can be used to compare different options and budgets to determine the cyber resilience outcomes that will be achieved for different spends, providing an extremely useful context that allows cybersecurity leaders to have business conversations with executives and board members about the benefits that the cybersecurity function can and will be delivering to the organisation.

More importantly, it allows for a powerful, yet simple way to articulate how spend affects outcomes, which is critical in facilitating a constructive discussion to determine the right cybersecurity budget required for an organisation.

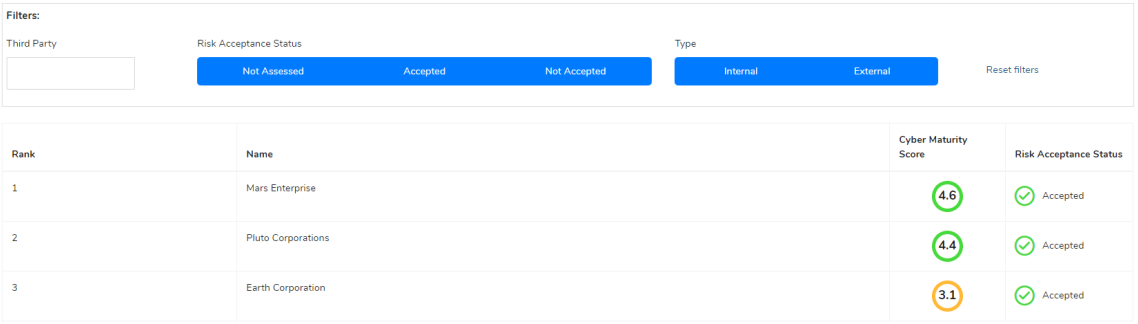
THIRD PARTY CYBER RISK MANAGEMENT

Organisations work with vendors in their supply chain that introduce additional cyber risks. To manage this risk properly, most organisations ensure a third-party cyber risk assessment is conducted before agreeing to do business with external vendors. This is commonly done via spreadsheets and emails, which is highly inefficient and time-consuming.

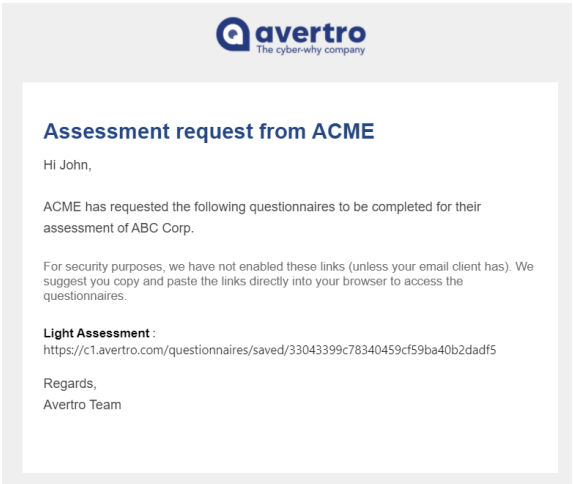
SOLUTION BRIEF

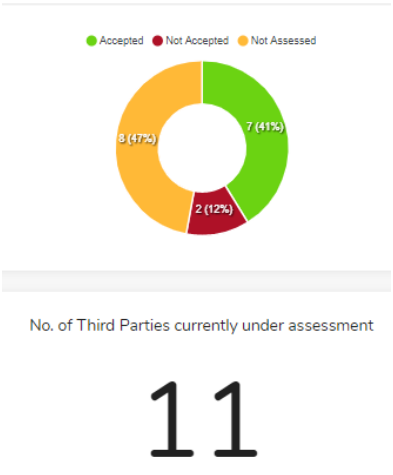
avertro
The cyber-why company

Avertro CyberHQ™ removes the need for spreadsheets and streamlines the whole third-party
assessment process. The platform provides a full audit trail of the back-and-forth process required during each assessment, and includes the reporting required to manage third-party cyber risk over time, normalised to a score that allows for easy comparison across all third-parties.



Given that the platform supports multiple cybersecurity frameworks, organisations can report on third parties against their framework of choice. Default third party questionnaires are provided with the Avertro platform for the purposes of fast-onboarding of an organisation. In addition, organisations can continue to use their existing assessments if required; we simply load existing assessment questionnaires into the platform to provide a “like for like” replacement while completely removing the inefficiencies inherent in the prior process.





The platform serves as a communication hub and audit mechanism for correspondence during the assessment, and system of record for evidence and commentary required as part of the assessment process.

SOLUTION BRIEF

avertro
The cyber-why company

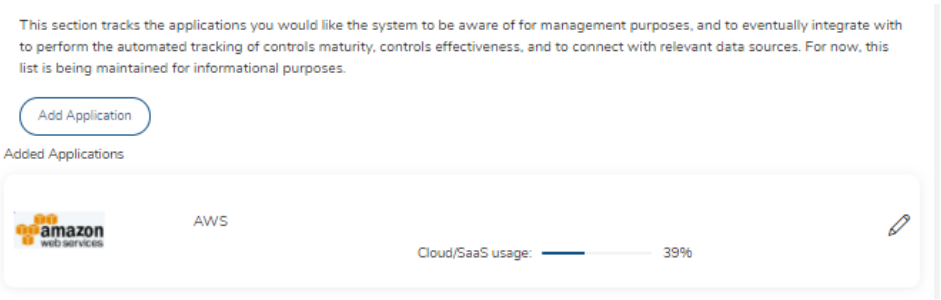
DATA SOURCES AND RELATIONSHIPS

Avertro CyberHQ™ stores all the data required to manage the ongoing cyber resilience posture of organisations. Capabilities within the system help to streamline the ongoing collection of data required on an ongoing basis. As such, much of the manual work required is reduced. In addition, there are aspects of data collection that can be automated via connectors.

Cloud Platform Integrations

The platform is able to automatically connect with cloud platforms such as AWS to extract security-related configuration settings and relevant data points, and maps these to control settings being managed within the system.

In this instance, Avertro CyberHQ™ normalises the technical data and subsequently uses the information to inform other metrics being stored and calculated to inform an organisation's overall cyber resilience.



For example, when the platform scans AWS, the information is mapped to a standard controls framework, allowing us to determine the maturity level of the AWS environment in question. The relationship of the AWS environment in question to the overall organisation is then used to determine how much the posture of said AWS environment should affect the cyber risks being managed, and ultimately, the cyber resilience of the organisation.

Security Technology Integrations

Various security technologies can inform certain aspects of the Avertro CyberHQ™ platform. In general, integrations in this context can affect the following:

- Cyber risk posture
- Controls effectiveness

Cyber Risk Posture

Integrations with threat intelligence feeds or security monitoring platforms can increase cyber risks. For example, certain threat actor campaigns may increase the likelihood of a data breach. At the same time, if the security monitoring platform has determined that a specific attack may be taking place, the related business-level cyber risks should also be elevated.

Feeds from vulnerability scanning tools however, can indicate that a set of issues exist that need to be remediated. In this case, such a feed would influence the business-level risk via one or more issues being created as a result of the automated feed.

Controls Effectiveness

In the case of technologies that have been implemented to support controls, the automated integration points can serve as a way to determine if the relevant controls are effective. For example, integration with endpoint protection platforms allow us to automatically update controls effectiveness settings of the related mapped controls, which will in turn increase or decrease the maturity of those controls and related capabilities.

STRATEGIC CYBERSECURITY HEADQUARTERS

Avertro is unique in how we help organisations manage the business of cyber. The platform has been built by industry experts and advisors with real experience in doing things right. Our iterative product development process is based on a design thinking approach, which involves our customers as well as industry luminaries, ensuring we are always evolving for the better.

We can supercharge your journey towards cyber resilience and help you create a constant cycle of continuous improvement. For further information, a demonstration, or a conversation about how Avertro CyberHQ™ can help you, email us at info@avertro.com and get started on proving you are doing cyber right.