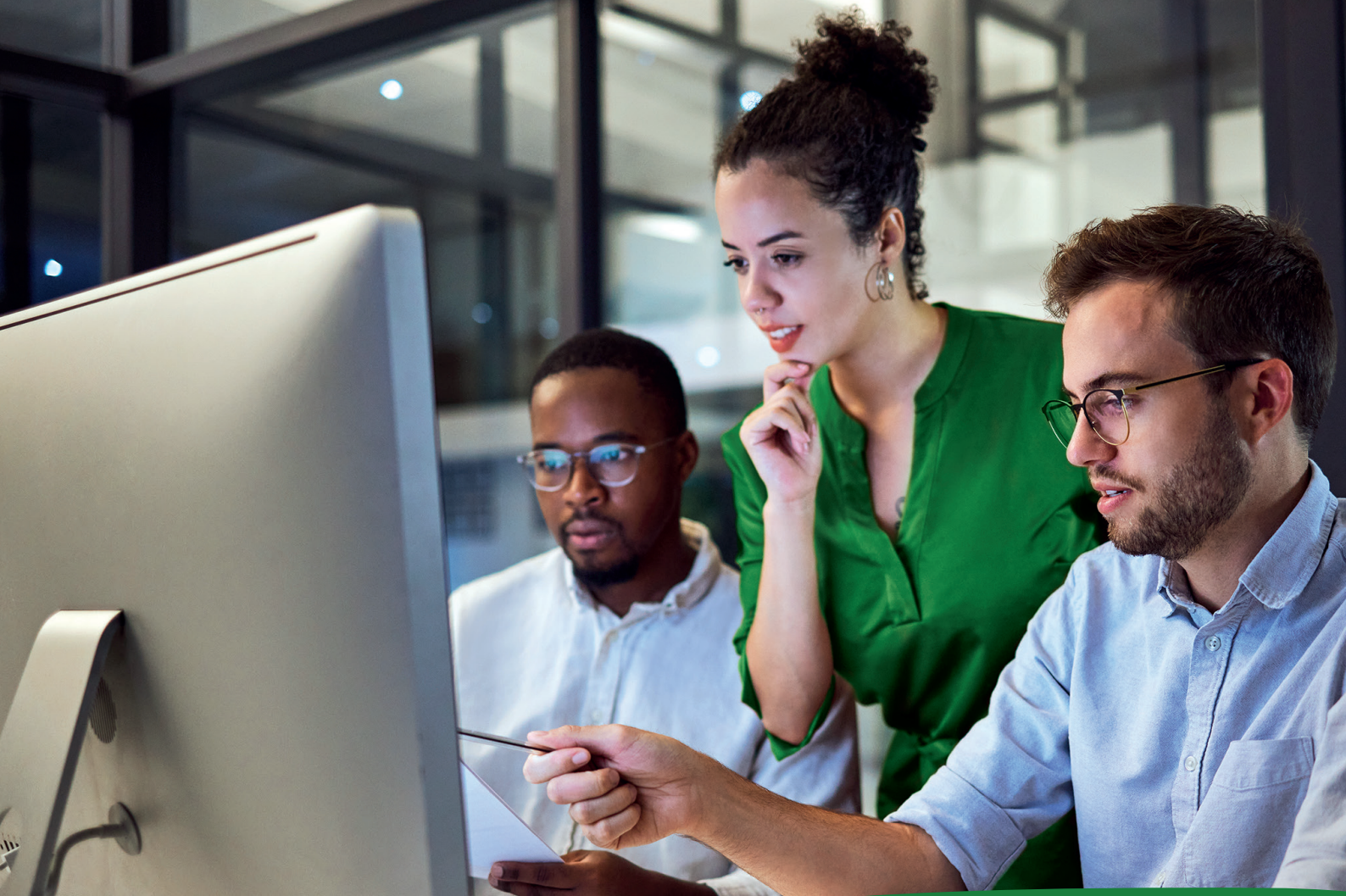


TAKE STEPS TOWARDS DATA SECURITY:

Designing your organisation's data protection framework

Aussie Broadband

THE ACTUAL AUSSIE WAY

Introduction

Data touches every element of an enterprise operation whether it's finance, marketing, HR or customer service. Losing control of it can be disastrous and not just to your bottom line. The reputational damage that comes with a data breach can be far longer lasting and continue to erode customer confidence long after your balance sheets have taken a hit.

It's no wonder data security is one of, if not the foremost, concern in the enterprise sector.

Setting a platform that fosters data protection and boosts the security posture of an enterprise requires a multifaceted approach including:

- Tech stack analysis
- Security diagnosis
- Strategy creation
- Solution and partner selection

Aussie Broadband's data protection solution is built on Veeam technology and serves as a cornerstone for delivering disaster recovery solutions to B2B customers.
Our team has to drawn on our collective experience in delivering data protection solutions to outline a range of elements to consider on your data security journey.

In this eBook, we'll give you the analysis and advice to assist you in making the important data security decisions for your business, staff and customers.

Veeam Cloud Connect

Cloud Connect provides a seamless and reliable method for enterprises to securely transfer and store their backups on immutable storage in off-site cloud repositories. The solution eliminates the need for costly and complex traditional backup infrastructure while ensuring critical data is protected and accessible in case of malicious activity such as ransomware, accidents or disasters.

About Aussie Broadband

Aussie Broadband is one of Australia's leading providers of telecommunications and technology products to residential, SME and enterprise customers across the country. The company is a Tier 1 voice provider and delivers a wide-ranging set of solutions including cloud services, connectivity, networking, internet, voice, managed IT and data security.

About Veeam

Founded in 2006, Veeam Software is a privately held information technology company focused on simplifying backups for virtual machines. Veeam's company vision is to be the most trusted provider of backup, recovery and data management solutions that deliver modern data protection and continues to charge forward to innovate the industry so customers can own, control and protect their data anywhere in the hybrid cloud.

Get Started

Step 1 – Analyse your tech stack

Gaining a clear understanding of components and capability of your tech stack is the first step to building your data protection framework. This process includes identifying the applications, data protection solutions, storage solutions, cloud infrastructure and network components that form the foundation of your technology environment.

A typical enterprise tech stack comprises apps and programs such as (CRM) systems, enterprise resource planning (ERP) software, file servers, databases and cloud infrastructure. Large organisations can include an eclectic mix of vendors e.g. Salesforce for CRM, SAP for ERP solution and Amazon Web Services (AWS) for cloud infrastructure. Each has its own requirements, vulnerabilities and specifications to consider.

Part two of the tech stack analysis is to identify and recruit key stakeholders who have the knowledge to shape your data protection solution. Consider a data protection working group consisting of:

- **Chief Technology Officer** - To provide strategic direction for the data protection framework.
- **Compliance Officer** - To ensure data protection practices comply with applicable regulations.
- **IT Manager** - To oversee the overall technology infrastructure.
- **IT Engineer or technical subject matter expert** - For expertise in implementation and management of any data protection solutions.
- **Data owners** - To assist in establishing your organisation's framework.

Their insights and expertise will help ensure that the data protection framework aligns with the organisation's security objectives.

Step 2 – Diagnosis

The next step is to rank the different components based on their cost to the business and their criticality in generating and saving revenue.

Consider a scenario where an e-commerce company relies on its website and customer database for revenue generation. The website and database would be ranked as critical components with high financial impact in case of a disruption. Conversely, an internal collaboration tool like Slack would likely have a lower financial impact on the business despite being widely used in day-to-day operations.

Performing cost analysis identifies tech stack risks and monetary implications. For example, if the customer database is breached, the organisation can face financial penalties, reputational damage and loss of customer trust. Quantifying these costs helps prioritise investments in data protection measures for critical components.

It's important to note the cost is not solely limited to monetary factors. Disruptions can also lead to productivity loss and breaching of Service Level Agreements (SLAs). This process enables informed decision-making and ensures resources are allocated appropriately in your framework.

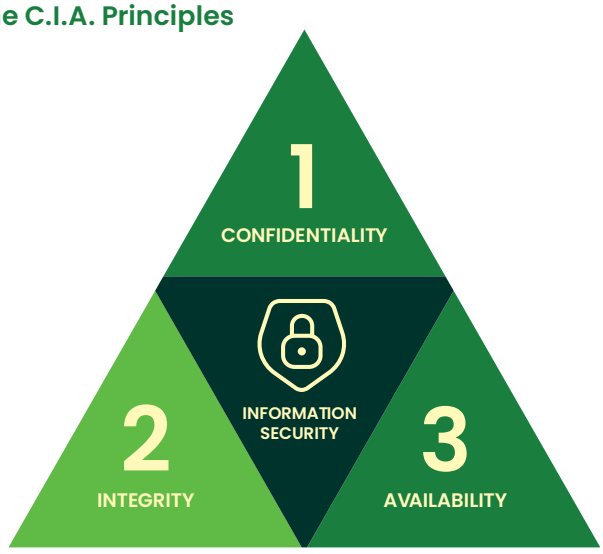
Step 3 – Construct your Risk Mitigation Strategy

With your steering committee in place and a cost analysis in hand, you can now begin to construct a Data Protection Framework.

But where to start?

A simple way to kickstart the practical side is by building out your framework using the **Confidentiality, Integrity** and **Availability** (C.I.A.) methodology.

The C.I.A. Principles



Confidentiality ensures that only authorised and authenitcated individuals within the company have access to protected data. This principle focuses on maintaining the privacy and secrecy of sensitive information and preventing unauthorised disclosure or access.

Support your Confidentiality pillar through the AAA method.

- Access controls
- Authorisation
- Secure authentication mechanisms

Integrity is about ensuring data remains intact and unaltered. It involves protecting data from unauthorised modification, deletion or corruption.

Support your Integrity pillar through:

- Robust data validation
- Checksums
- Audit trail mechanisms

Availability refers to the accessibility of data when needed. It involves having the tools and procedures in place to ensure data can be restored quickly in the event of a disaster.

Support the Availability pillar through:

- Data replication solutions
- Recovery Time Objective (RTO) specifications
- Recovery Point Objective (RPO) specifications

Start by discussing the tactics available to mitigate risks across the C.I.A. dimensions and assessing the effectiveness of:

- Security controls
- Encryption methods
- Backup strategies and procedures
- Disaster recovery plans

C.I.A. Use Case

Suppose you're constructing a data protection strategy for a financial institution. Confidentiality will be of the utmost importance due to the nature of the sensitive nature of financial information. Securing this data requires confidentiality tactics such as:

- Access controls
- Strong authentication mechanisms
- Data encryption at rest and in transit
- Security awareness training for employees

Ensuring the accuracy of transactions and customer interactions are critical for meeting the Integrity dimension of the institution's security environment. Establish audit trails and implementing change management processes to detect and prevent unauthorised modifications will be critical to supporting this pillar.

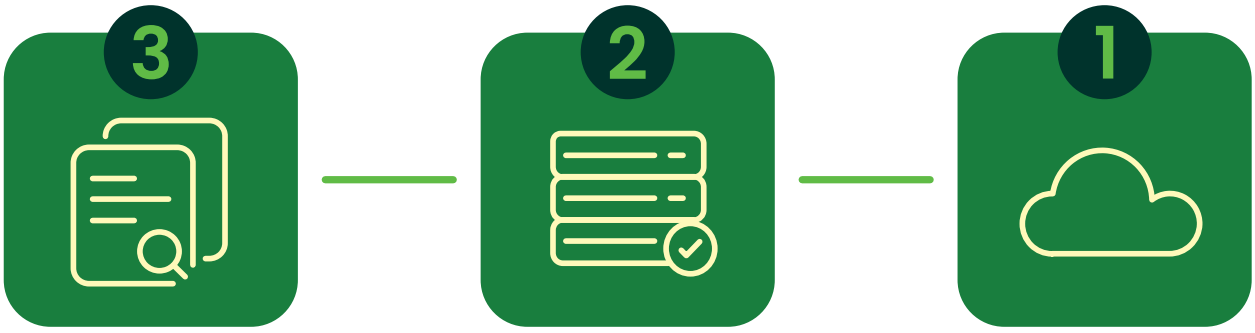
The organisation may invest in redundant systems and backup solutions to bolster the Availability dimension of its environment. This key step ensures uninterrupted access to financial data. Regular testing and updates of disaster recovery plans would also contribute to maintaining availability in the event of system failures or natural disasters.

Categorising data protection levels for each component in the tech stack is also essential. This process requires analysis of each component and identifying their specific risks. This process enables the organisation to prioritise their efforts and allocate resources efficiently.

Consider seeking guidance from internal leaders of different disciplines in this process. Their expertise can help your steering committee understand the criticality of data and apps that are used in the everyday duties of their teams. This feedback will help you better identify appropriate solutions and vendors that can assist delivering your framework.

Data Protection in 3-2-1

The 3-2-1 methodology of data protection acts as the tactical deployment or realisation of the strategic direction laid out by the C.I.A. strategy. The 3-2-1 backup strategy is centred on delivering an environment where there is no single point of failure in the event of a disaster or malicious corruption of data. The breakdown of the methodology is:



Keeping **3 copies** of all critical data

Utilising **2 different** storage types

Keeping **1 copy** of data in an offsite location

3-2-1 should be a key consideration in your **Selection Criteria (Step 4)** and in **Selecting Your Solutions Provider (Step 5).**

Step 4 – Selection criteria

Selecting the right technology and tools is crucial for designing an effective data protection framework. Compatibility and easy integration with your tech stack should be the defining criteria for selection to ensure your implementation phase is easily executable and aligned to your organisation's risk mitigation strategy.

Consider a software development company that relies on version control systems and code repositories. Various options such as GitLab, GitHub or Bitbucket could be evaluated to slot into its existing development workflow. There'd be a range of features to consider including user-friendliness and collaboration ability such as code review and issue tracking. Collaboration features and sharing of sensitive IP or data naturally brings security concerns.

Look for solutions that offer real-time monitoring, threat detection and incident response mechanisms. These features enable organisations to identify and mitigate security risks promptly and minimise breaches or data loss.

Moreover, assess whether the solutions offer self-management tools or managed service functionality. These features can simplify your security admin and improve operational efficiency. Proactive security monitoring becomes crucial for automating threat detection and ensuring the availability of the application.

You can also factor in service level agreements (SLAs) that align with specific needs and risk tolerance such as uptime, recovery point objectives (RPOs) and recovery time objectives (RTOs). Structuring an SLA in line with your tech stack audit sets the platform for maintaining consistency and effectiveness in your data protection framework.

Finally, it is essential to evaluate the costs associated with the chosen solutions. This includes initial investment and ongoing expenses such as licensing fees, maintenance costs and scalability options. Cost needs to be balanced with effectiveness and suitability to your data protection requirements.

Step 5 – Selecting your Solutions Provider

A reliable solutions provider can help cover any skills gaps in your organisation when it comes to implementing and maintaining your data protection framework.

Implementation is often the key motivator for seeking out a partner but many are equally adept at diagnosis and maintenance. Prioritise your selection on the partner's ability to work efficiently with your tech stack and the ease with which internal staff can utilise and manage them.

Assess whether the solutions provider offers self-management tools or managed services that align with the organisation's needs and preferences. These features empower organisations to have greater control and flexibility over their data protection measures.

Proactive security monitoring of any solutions should be a key feature offered by the provider. Look for one that demonstrates proven capability in security monitoring with SLAs aligned to your risk mitigation strategy and uptime guarantees.

Use case - Healthcare

In the healthcare industry, a hospital might need to select a solutions provider to implement a stronger data protection framework. Key considerations for the hospital's steering committee should be to choose a provider with a track record of implementation for data protection matching the compliance requirements of the healthcare organisation. Meeting regulatory standards for sensitive patient information will be paramount to remediation in a disaster recovery scenario and minimise the risk of data breaches.

While cost should not be the determining factor in selecting a partner, it's important to align with your budgetary constraints for implementation and consumption. Quality, functionality and reliability of the solutions provided are equally crucial.

Working with the selected solutions provider requires establishing an effective operating rhythm. Communication between the organisation's IT staff and the vendor is essential for sharing technical information, addressing concerns and resolving issues. It is advisable to designate a service delivery manager to facilitate regular governance meetings, ensuring ongoing collaboration and alignment.

It is essential to establish a cohesive view of virtual or physical workloads, storage utilisation, recovery points and long-term retention goals. Involving the internal technical team as key stakeholders from the beginning helps facilitate a shared understanding and enables smooth implementation and operation of the data protection framework.

Step 6 - Implementation and Continuous Improvement

Once the data protection framework and solutions provider are chosen, it is time to implement the necessary measures to continuously improve the system.
This involves:

- Configuring and integrating the selected technologies into the organisation's infrastructure
- Training staff on usage and adherence to data protection policies
- Conducting regular assessments and audits to identify potential vulnerabilities

Organisations often face challenges such as system compatibility issues, user resistance to change or resource constraints during the implementation phase.
Continuous improvement the process that helps overcome these challenges and is essential for maintaining the effectiveness of the data protection framework.

Key tactics to include in your continuous improvement planning include:

- Regular security updates
- Penetration testing
- Incorporating feedback from internal stakeholders and the solutions provider.
- Data recovery testing

Conclusion

Designing and executing a robust data protection framework is a critical endeavour for enterprises. Constructing the right framework requires a systematic approach that encompasses understanding the tech stack, diagnosing risks, strategy creation and collaboration with reliable solutions providers. Leveraging the CIA principles of Confidentiality, Integrity and Availability sets a reliable platform for data protection and assists in smoothing the implementation process.

By taking steps towards security, organisations can safeguard their valuable data assets, maintain customer trust and mitigate the financial and reputational damages associated with data breaches or loss.

DATA PROTECTION SOLUTIONS THAT PROTECT THE GROWTH OF YOUR BUSINESS.

Aussie Broadband's data protection solutions deliver business continuity when you really need it through duplication and reinstatement of your critical systems. Maintain peace of mind, in the event of malicious activity, unintentional deletion or natural disaster.

For more information or to book a discovery session, call us on 1300 161 625.

aussiebroadband.com/enterprise

Morwell Office
3 Electra Avenue,
Morwell, VIC 3840

Aussie Broadband

THE ACTUAL AUSSIE WAY