BALANCING THE SCORECARD:

Identifying, quantifying & prioritising information security risks.

Under the mandate of Victorian Privacy Legislation, Alpine Shire Council is required to submit its **Protective Data Security Plan** demonstrating their level of maturity and benchmarking against the state's data security standards.

Read how RTG worked with the Council to facilitate this process.

Data is an incredibly important asset, with the collection, storage and sharing of data being an integral operation in today's digital economy and everyday lifestyle. The exponential growth in amounts of information being collected about users, consumers and customers has made data privacy issues more salient. Many organisations and businesses today are often at risk of unintentionally violating data privacy regulations because their security measures are not mature enough nor can they keep up with the ever-evolving cyber risk landscape.

In 2014, the Victorian Privacy and Data Protection Act ("PDP Act") was passed, making it Australian's first broad-based legislated information security requirement. Part 4 of the PDP Act gives the Victorian Information Commissioner ("OVIC") power to issue standards for the security, confidentiality and integrity of public sector data. With this, OVIC scoped the **Victorian Protective Data Security Standards** (the "Standards") to **establish 12 high level mandatory requirements to protect public sector data across all security areas including governance, information, personnel, Information Communications Technology (ICT) and physical security**.

Under the mandate of OVIC, every two years Alpine Shire Council is required to submit a Protective Data Security Plan ("PDSP") demonstrating their level of maturity and benchmarking against each of the 12 Standards. To complete this submission, **the Council had to undertake a gap analysis of current approaches, structures and processes relating to information security.** "We had ad hoc structures and processes in place," said the Council's Manager of Customer and Digital Projects, relying on the Council "completing the forms and attestations to the best of our ability a few days before they were due".

Needs

- Complete a gap analysis of the Council's information security controls to ascertain its ability to identify, detect, contain & resolve data privacy incidents, plus respond proactively on potential vulnerabilities within the Council's IT infrastructure and digital risk posture.
- Use insights from the gap analysis towards the completion of the Protective Data Security Plan and Attestation ("PDSP") submitted to OVIC on 31st August 2020.
- Scope a two-year IT Data Protection and Governance roadmap for the Council that includes Key Performance Indicators, operational schedules and workflows.

Challenges

- Reliance on an ad hoc, reactive approach towards information security controls and data assets management.
- Time required to oversee and manage the risk assessment process expected from OVIC.
- Council was resource-constrained in the ICT space, with only one person managing all ICT tasks for the entire Council.
- An immature ICT governance framework that gave limited insight into the Council's compliance against OVIC regulation and standards.

The Council recognised their biggest challenge was the time commitment needed to not only complete a thorough risk assessment of its information security structures and controls, but also the scope of a two-year security plan based on identified needs and gaps. "The immaturity of our ICT governance framework was formally escalated to us via an interim audit that was conducted by our VAGO (Victorian Auditor-General's Office) appointed auditors", said the Council's Manager of Customer and Digital Projects. Findings from this initial audit gave the Council an imperative that was endorsed by their audit committee, and saw the need "to activate a project to build an appropriate ICT governance framework".

> *" Highly skilled and experienced consultants in this space who sought the relevant information up front and then got on with the job.*
> *Minimal impact on the time and energy required from our very stretched ICT Coordinator. "*

With only one person handling all ICT tasks, the Council acknowledged they were resource constrained, and through its Request for Quotation process, selected RTG as the consultants of choice to implement the Council's **IT Data Protection and Governance project**. This project followed a process-orientated model that supported Alpine Shire Council through **a risk assessment that identified, quantified and prioritised information security risks against OVIC Standards.** The key outcome of this project resulted in the scoping of an IT data protection and governance structure that not only allowed the Council to submit its PDSP, but also **identify a set of information security initiatives to strengthen the Council's reduction of risk to data assets in a timely, proactive and measured response**.

To finalise the project, a Statement of Applicability (SoA) tool was customised for the Council based on project findings. This SoA application is the main link between risk assessment and risk treatment, and forms a fundamental part of the organisation's information security management system. **The SoA application was created directly into the Council's SharePoint site, and will be used collaboratively to update, modify and report on the implementation of security controls and measures against all 12 OVIC Standards**. "A plug and play tool, built directly into our SharePoint environment that we can use to track all future work in this space" will bring great value to the Council, as said by the Manager of Customer and Digital Projects. A tool that will "simplify our attestation process in the future."

Outcomes

Findings from RTG's IT Data Protection and Governance project has provided Alpine Shire Council with deep insights on its internal and external digital environment, encompassing matters as diverse as stakeholder knowledge and adherence, policies, procedures, systems, information asset management, incident response management, business continuity, vendor management and security (physical and IT).

Alpine Shire Council has used findings from RTG's IT Data Protection and Governance project to:

- submit the Council's Protective Data Security Plan as per OVIC regulation.
- identify benchmarks in the existence of, and adherence to, information security-related best practice and OVIC data privacy regulations.
- ascertain the Council's preparedness to respond to a digital incident, including the design of customised treatment plans against identified cyber risks. These treatment plans formed the scope and digitisation of the Council's Risk Register.
- design a Statement of Applicability Tool created especially for the Council to ensure the implementation and effectiveness of its IT governance framework remains ongoing and sustainable.

Contact RTG's Risk Consultancy Team to learn how we can work with your organisation to mitigate and manage information security and data privacy projects.