



CASE STUDY

Hollard Leads the Insurance Market and Maintains Cyber Security Flexibility with Whistic



Introduction

Few companies have the expansive reach of the Hollard Insurance Company of Australia. With over 700,000 customers, they ensure the lives, homes, income—and even the pets—of their clients. An intensely customer-focused organization, they take the obligation of keeping information protected seriously.

"It's our responsibility to ensure that all of Hollard's information assets are secure and protected from cyber threats and risks," said Grae Meyer-Gleaves, Chief Information Security Officer. "We hold sensitive information about our customers and prospects, and they expect us to protect them well."

In addition to expectations of customer privacy, the insurance industry is subject to regulatory, contractual, and legislative obligations in regard to their information systems.

Customers rely on Hollard during difficult times, so compounding problems with security issues isn't an option. "Our role is to ensure that people are covered during their time of need," said Grae. "We also have an extensive partner network. In order to grow as a business, trust is important for us, our partners, and our customers."

Grae needed the right tools to help complete their world-class infrastructure. Enter Whistic.





Our role is to ensure that people are covered during their time of need. And that includes protecting their information.

Grae Meyer-Gleaves, Chief Information Security Officer



Problem

A problem in need of simplification and automation

Like most companies, Hollard used to assess the security posture of their vendors using spreadsheets. It was a slow process, requiring long email chains and weeks or months of back-and-forth communication. On top of this was the requirement to create reports and extract meaningful information from their collected assessment spreadsheets.

Grae decided to find a system that would help him automate the security review process and make it easier for his partners and suppliers. He turned to the Cloud Security Alliance (CSA) and Vendor Security Alliance (VSA) for ideas and quickly discovered that both organizations recommended Whistic.

Hollard has 250 third-party vendors and another 50 IT vendors. It required two full-time employ-

ees to handle the security review workload with their manual process. That's an inefficiency Grae found unacceptable.

And given new industry regulations, they had a small window of time to get through 250 assessments. It was a daunting task.

Two full-time employees were needed to handle the manual security review workload.





Solution

Grae identified four primary drivers that led him to update his vendor security practice.

1. He needed to assess many suppliers quickly.
2. Security resources are expensive and in high demand.
3. Partners and internal resources were frustrated with the pace of their old system.
4. Their existing assessments weren't standardized and didn't align with needed industry frameworks.

Flexibility is an essential factor for Hollard, as they needed to ask specialized questions for compliance purposes, and they needed to add them easily. Grae's team modified existing templates already found in the Whistic platform.

"Whistic had questionnaires in template form, which enabled us to fast-track deployment," said Grae. "Also, we use the Whistic Trust Catalog® to evaluate major vendors, allowing us to evaluate suppliers with Zero-Touch Assessments."

"Someone recently suggested a new vendor. I checked and found their profile in the Trust Catalog and approved them right away," Grae said. "When we're looking for a supplier, we start with the Trust Catalog. It makes vendor selection easier and helps us establish trust between organizations quickly."

In addition, Hollard has partners that require them to complete security assessments. Hollard is creating their own Whistic profile and will publish it to the Trust Catalog as part of its journey to ISO 27001 certification.

Another important part of Grae's decision to use Whistic is that it allows his team to create inherent and residual risk ratings for each vendor, and then align the ratings to their corporate standards. "I like that we can configure that, and many systems don't allow that level of flexibility," said Grae. "Plus, our supply chain changes all the time, and we have a constant moving target of third parties that need assessment. We're continually adapting to the business, and with Whistic, our cybersecurity team isn't a bottleneck to these changes."

Grae's team now only spends a few hours a week on vendor risk as a result of their implementation of Whistic. These capabilities lead to better outcomes for Hollard's sales teams and their customers. "I don't get calls from the sales team asking when assessments will be completed any longer. That's a good day for a CISO," said Grae.

The Whistic Trust Catalog® evaluates major vendors, allowing teams to fast-track suppliers with Zero-Touch Assessments.



Results

Reduced security review workloads, fewer spreadsheets, and increased utility of third-party vendor analytics

faster security reviews

From 2 full-time employees to a few hours per week using Whistic.



no lost work

They were able to import all of the spreadsheets for assessments into Whistic so they didn't use any legacy work.

reporting benefits

They can now pull useful information from Whistic across all of their third-party vendors, exporting the raw data and analyzing it with other analytic tools.





The Future

The future is bright for Hollard. Whistic gives them the ability to remain agile and embrace change at the pace of their customers. It's also helping them as a supplier to others by creating their own Whistic profile as part of their journey to ISO 27001 certification.

Flexibility and adapting to change make for strong insurance, indeed.



www.whistic.com