LOCAL GOVERNMENT CYBERSECURITY PROGRAMME

SAM FOR COMPLIANCE

The SAM (Self Assessment and Monitoring) System was developed to allow organisations to self-assess their conformance to specific Standards. Although the system was created with information security in mind, it is not limited to this and we can embed any Standard relating to any subject or topic into the system providing that we can define the controls from the Standard. We currently have 26 standards and frameworks available applicable to New Zealand, Australia, USA and the UK.

SAM came about due to our frustration that a snap-shot-in-time audit did not provide the ongoing visibility organisations needed to manage and improve their cybersecurity performance. We believed that a dynamic tool which reflected improvement or deterioration of performance over time would be more relevant than a document that was glanced at and then confined to the back shelf.

We were also of the opinion that many of the internationally recognised cybersecurity standards were not a good fit for New Zealand. The size and scope of many of our organisations, including some Government Agencies and Local Government, were not of sufficient scale, nor did they have available the resources required to implement compliance to these extensive Standards.

While there are other compliance and risk management systems available, many of these are complex and very expensive to implement. We believe that compliance management should not just be available to the large multi-national corporations, but also to small and medium sized organisations that may not have the knowledge or resources necessary to use these big systems. Simplicity and removing cost as a barrier to entry was the key to success.

ALGIM AWARDS

AWARD WINNERS 2020

- 1st Hauraki District Council
- 2nd Christchurch City Council
- 3rd Waimakariri District Council
- 4th Timaru District Council
- 5th Stratford District Council

AWARD WINNERS 2019

- 1st Waimakariri District Council
- 2nd Central Otago District Council
- 3rd Hauraki District Council
- 4th Whakatane District Council
- 5th Ashburton District Council

www.algim.org.nz

LOCAL GOVERNMENT

Councils hold a lot of important information on a diverse range of activities and some of their systems are critical – e.g. Scada systems for managing water and sewage. Other enterprise systems hold personally identifiable information – e.g. rating databases.

Having worked within local government for many years we were concerned that not much was happening to improve cybersecurity performance and that it was time to do something about it.

We decided that a much more pragmatic approach was needed if we were to get Councils onboard. The first consideration was that we should develop a framework that was applicable to Local Government and the content of this would be achievable and measurable, irrespective of the size of the organisation.

Another important factor was that the controls should be specific and not open to interpretation as to what was actually required. To this end we chose the CIS Controls as the foundation for the framework. These are a pragmatic set of technical controls which are internationally recognised to improve baseline cybersecurity and require no additional explanation or interpretation.

We needed a structure to embed these controls into and we also felt that certain areas, important to the local government environment were not included within the CIS Controls and should be added. For example: Governance and Information management. We decided to embed the CIS Controls into the NIST CSF (Cybersecurity Framework) using the functions, categories and sub-categories, and to achieve this we added approximately 100 additional controls, creating a framework consisting of 281 controls, all of which were relevant, applicable, achievable and measurable.

We also graded the controls using levels 1 to 3 based on how difficult they were to implement. This meant that Councils could work on the level 1 controls first and then move up to level 2 and level 3 when they had the resources and the ability to meet these requirements.

ENTER ALGIM

We approached ALGIM (Association of Local Government Information Management), with whom we have a long-standing relationship, to ascertain whether they would be interested in partnering with us to deliver the programme. The area of cybersecurity and its relationship to information systems is an important part of their mission and objectives. We jointly agreed that Local

ALGIM 2021 AWARDS

The 2021 Award Winners will be announced at the ALGIM Annual Conference

21- 24 November 2021, TSB Arena/Shed 6, Wellington

ALGIM is holding one all-encompassing face-to-face conference in 2021. Predicted to be the biggest conference ALGIM has held to date with three streams of presentations running. The programme, spanning three days, will cater for all disciplines: ICT, IRM, GIS, Web & Digital and CX.

For more information about the 2021 ALGIM Conference click on the Image below.

Government needed to do better, and to this end, it made sense for ALGIM to own the framework and for SAM for Compliance Ltd to provide the platform and management services.

We then considered what would actually inspire Councils to come on board.

We proposed that ALGIM roll out a cybersecurity programme which Councils could subscribe to for a small annual subscription that was based around the framework and the SAM for Compliance tool.
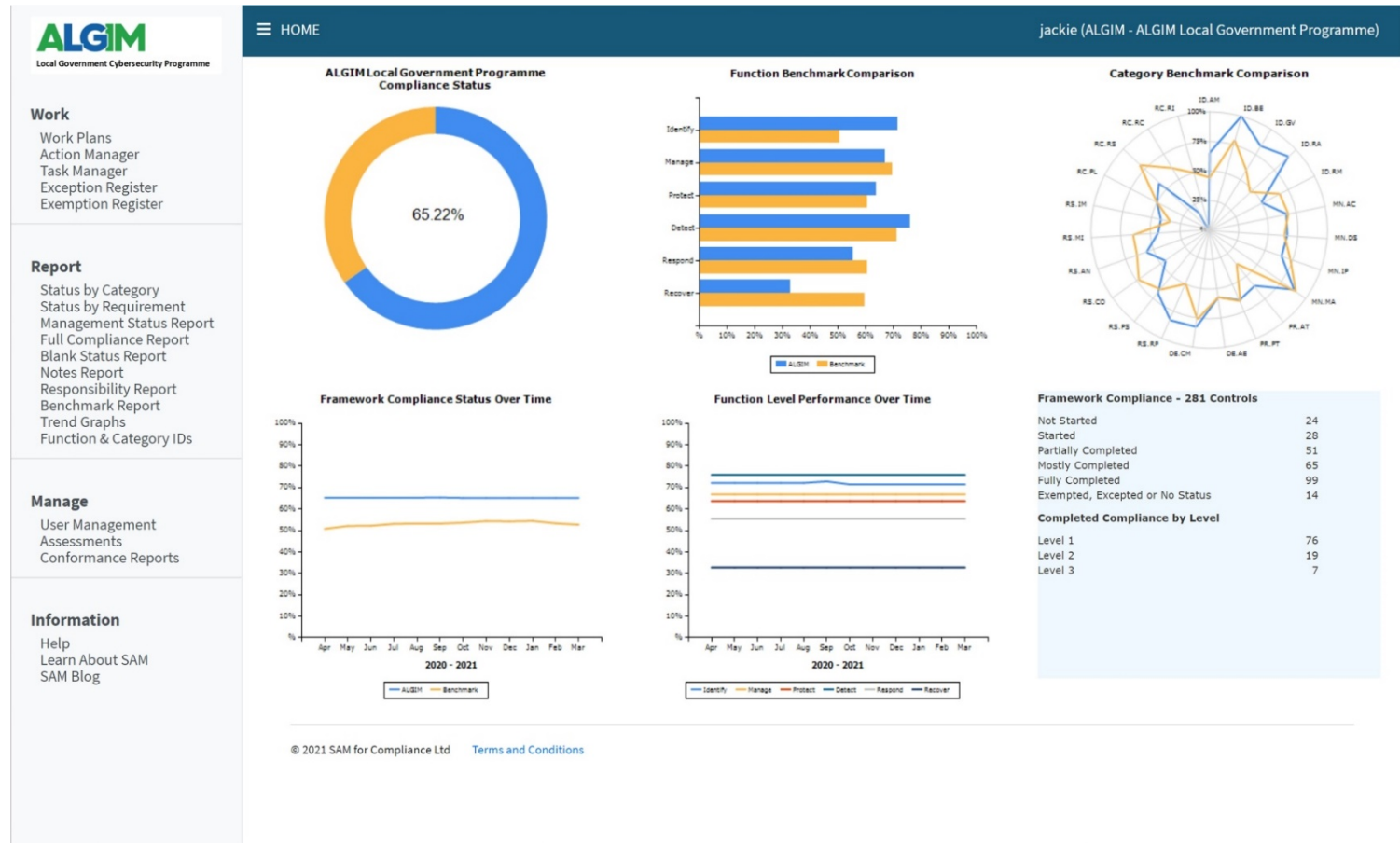
The ALGIM Local Government Cybersecurity Programme was launched with the following goals:
- Raising the bar on Local Government cybersecurity
- Promoting excellence and cybersecurity best practice within Local Government
- Rewarding achievement and improvement in Local Government cybersecurity through the ALGIM Annual Conference Awards
- Benchmarking Local Government cybersecurity
- Identifying opportunities for training and awareness to improve cybersecurity knowledge within Local Government

www.algim.org.nz

ALGIM's goal is to have all Councils and as many CCOs (Council Controlled Organisations) as possible participating in the programme. Participation in the programme as at April 2021 has grown to 40% of Councils since its inception in August 2018 and continues to grow. You can register your interest to join the programme through the [ALGIM Sam for Compliance registration of interest form](#).

In addition to the information each Council receives through their dashboard, ALGIM receive monthly consolidated reports that show the performance of the Group for the month and over time. From this information they are able to determine where Councils are performing well as a Group, and where they need additional help to improve. This enables ALGIM to deliver training and awareness programmes with a focus on specific areas of under-achievement.

Councils also group themselves into Regions and regional cybersecurity sub-groups have also been formed to help Councils share intelligence and knowledge on how to improve. ALGIM has also set up a group for sharing cybersecurity knowledge as part of the programme.

The income SAM for Compliance has received from administering and managing the programme has been used to add additional features to the system including:

- A Conformance Report (similar to a SOC 2 or SOC 3 report) that is a self-attestation to the current conformance to the ALGIM Local Government Cybersecurity framework and suitable for presentation to Councillors, Audit New Zealand and other Regulators and Insurers.
- A Risk Assessment Module which takes their current compliance posture and determines what this means to the Council in terms of risk. It also enables the Council to establish their risk tolerances and manage their risk in accordance with this.

www.algim.org.nz
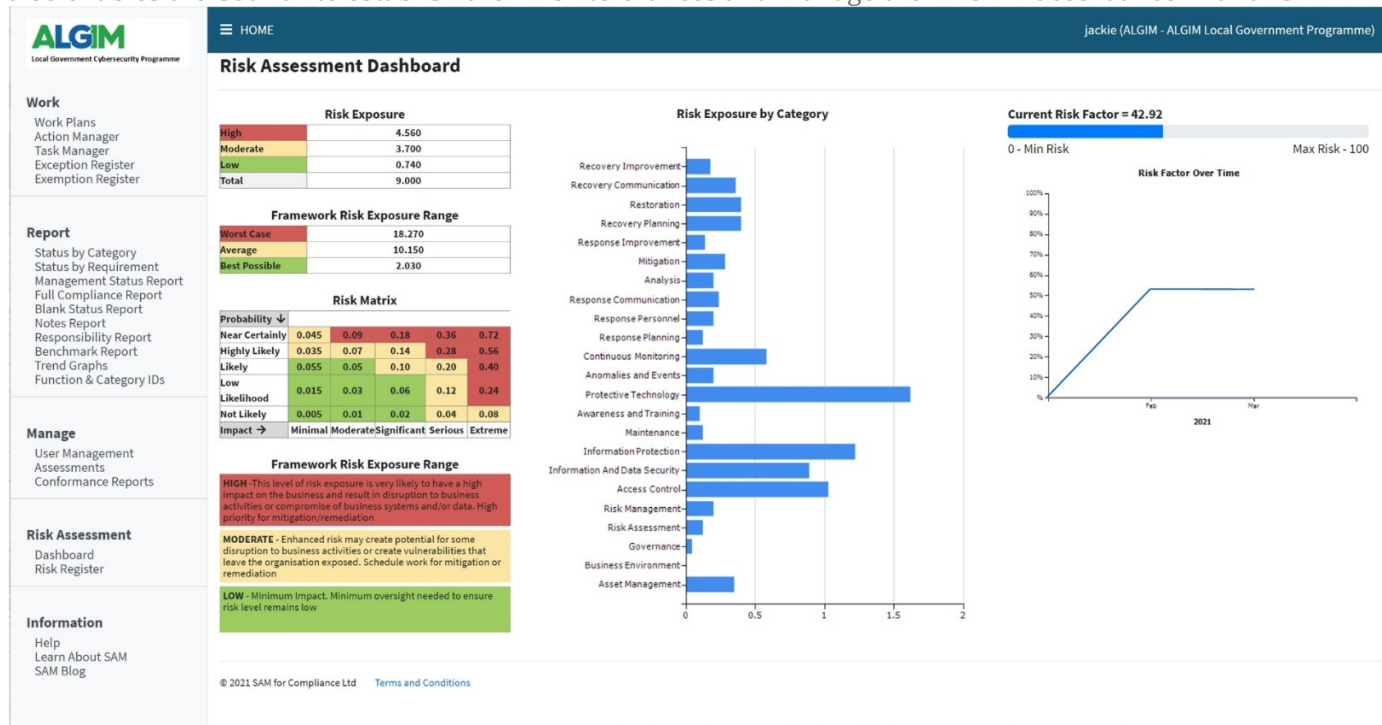
As we are continually looking for ways to improve the system and the reporting capabilities, the next system development will enable Councils to compare their performance with that of their regional group in addition to the ALGIM national group benchmark.

MAKING A DIFFERENCE

We believe that the programme has made a difference and has changed the way that Councils view cybersecurity. It is no longer considered something that has to be done in addition to system administration and management, but as part of these activities.

Mike Manson, ALGIM Chief Executive Office says *"ALGIM has a vision for all Councils to adopt the ALGIM Cybersecurity Framework as a consistent and measurable tool to ensure the sector is moving together on the journey of conformance to these defined controls. The benefits are enormous both in reducing risk for Councils, following best practice, benchmarking and recognising improvements or gains made, as this is a journey not a destination".*

The programme is effective because it is applied at the grass roots level of the IT system management. Complicated, convoluted strategies and management plans may look good and certainly have their place, but they have little impact on actual performance as they are unable to be distilled down to the actual actions being delivered through normal, business-as-usual, processes and procedures.

In summary, the key elements of success are:

- The programme belongs to ALGIM and every Council in New Zealand is a member of ALGIM
- It is promoted as a national cybersecurity improvement programme
- It rewards excellence and improvement
- There are no barriers to entry
- Benchmarking has become a driver for improvement and investment within Councils

Published April 2021

www.algim.org.nz