Subscription Based Security & Compliance to ISM

PROTECTED

Compliance Cloud Subscription Proposal
Department of Communities & Justice
(NSW)

Nov 8, 2022

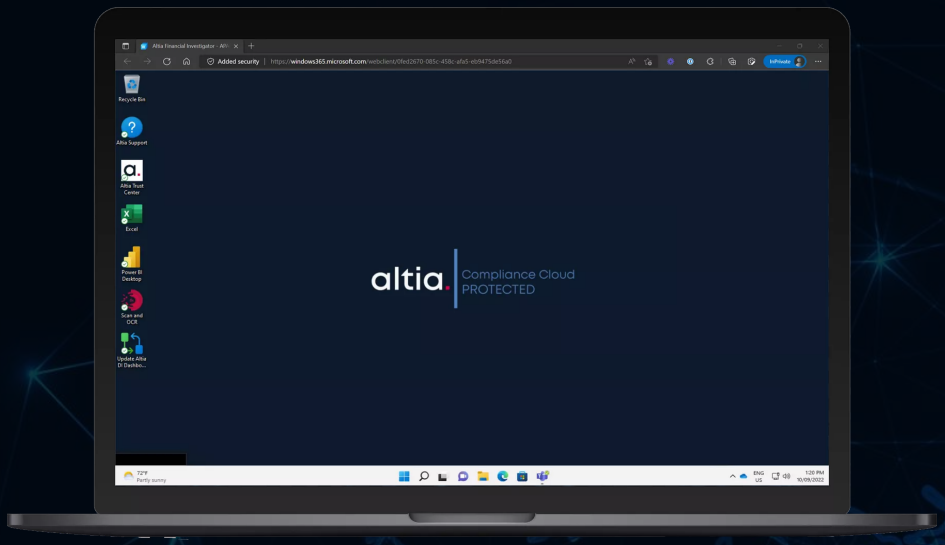
Altia Consulting Services | Altia (Global) | Information Office
12/440 Collins Street, Melbourne | Trust@altiaintel.com | 1800 573 367 | www.altiaintel.com

A cybercrime was reported every 7 minutes on average.

"Over the 2021-22 financial year, the cyber threats to Australia continued to mature as the virtualisation of Australian life has accelerated. Remote working arrangements have increased cyber security risks as employees switch regularly between personal and corporate devices. This has made the information held by individuals more valuable to malicious actors and digital technologies have made traditional crimes like extortion, identity theft and fraud far easier to replicate at a greater scale."

Australian Signals Directorate
Australian Cyber Security Centre
Annual Cyber Threat Report June 2022.

SUBSCRIBE TO REDUCE ORGANISATIONAL RISK.
SUBSCRIBE TO IRAP.



Altia Compliance Cloud is Altia's most advanced cloud service yet. Compliance Cloud is a dedicated workspace for high-risk, regulated, intelligence or investigative most mission-critical and sensitive workloads. An isolated space where operations & PROTECTED material can reside in a completely secure environment, removing the legacy operating & capital expenses in securing services and data.

Compliance Cloud is a subscription-based service, not unlike your favourite entertainment streaming platform. Surrounded by assurance, Compliance Cloud enforces 726 Security Controls independently assessed at a PROTECTED level as 100% effective, measured against the **Australian Government Information Security Manual (ISM)** during **InfoSec Registered Assessors Program (IRAP)** assessment.

Organisations can not only adopt the highest security benchmarks but embrace the mobility of remote work with confidence high-risk functions can be performed off-site, removing the shackles from organisations that have been surpassed by industries that have adapted and benefited from hybrid work. With Compliance Cloud, your security posture in the workspace is the same at home or in a remote office, as it would be at your headquarters. Through any device, everywhere - Compliance Cloud follows. And as Compliance Cloud is a managed and isolated package, an organisation's IT resources no longer carry the specialist burden to maintain, monitor and support such critical operating environments - saving money, resources, and internal pressures.

Compliance Cloud delivers this unmatched security while providing **PROTECTED** access to all Microsoft Services including Outlook, OneDrive, SharePoint, Teams, and others, allowing user-friendly collaboration, sharing, communication and messaging normally restricted to consumers who aren't handling at-risk information - as agencies struggle to meet these 726 Security Controls.

Information Security Management System ISO 27001 Certified

CYBER ESSENTIALS PLUS

2021

irap®

SECURITY MEET AND PRODUCTIVITY, COST EFFICIENCY, AND COMPLIANCE

Secure by Design.

Altia's Compliance Cloud is built against global general security frameworks by Altia's specialist Cloud Security Architecture Team. In collaboration with Microsoft's FastTrack for Azure Engineers, every component was rigorously assessed, configured, and tested against the most common, and unlikely threats.

Independently Assured.

The 726 controls safeguarding your workspace have been independently and rigorously assessed against the Australian Cyber Security Centre's Information Security Registered Assessors Program (IRAP) Assessment to ensure assurance and compliance with Australian Government Frameworks.

Unexpected Utility.

In addition to the peace of mind in complying with national benchmarks, leverage the utility of PROTECTED collaboration, sharing, archiving, secure messaging, and file transfer with specially configured Microsoft 365 Business Applications. With Compliance Cloud, efficiency isn't punished by security and control.

Unmatched Mobility.

Compliance Cloud brings today's hybrid-working world and security together, with the PROTECTED workspace's security framework following wherever mission-critical work is required. Access your highly valuable information by workstation, laptop, tablet, or phone. Headquarters, or home - always secure.

Compliance in Hours, Not Years.

Meet your information & cybersecurity, human rights, privacy, and archiving obligations within hours, not years. We've done the work, so you don't have to. Compliance Cloud is 'off the shelf', and deployment-ready regardless of internal IT dependency.

Cost Certainty and No Surprise.

Investing in best practices is the beginning. Maintaining it is the debt. Compliance Cloud ensures ongoing cost-certain compliance, with a subscription model not unlike consumer streaming services. No capital expense. No surprises.

Change Management, Managed.

Designed in collaboration with Microsoft, Compliance Cloud ensures end users can transition smoothly into a secure space without learning novel technology or tools. While end users will benefit from the modern interface of Windows 11, their daily process remains unchanged while interacting with the apps they love.

THE FRESH START YOU WANT. THE HISTORY YOU NEED.

Meeting the information & cybersecurity standards required to combat today's modern threats to comply with regulatory frameworks is daunting. Organisations often crave a fresh start. Compliance Cloud is above all, a fresh start. A zero-day and zero-trust baseline for your organisation to build a resilient future - without losing the past.

ALTIA CONSULTING SERVICES | ALTIA (GLOBAL) | INFORMATION OFFICE

12/440 COLLINS STREET, MELBOURNE | TRUST@ALTIAINTEL.COM | 1800 573 367 | WWW.ALTIAINTEL.COM

altia

TRUST. IT MAKES ALL THE DIFFERENCE.

Altia is committed to full and frank disclosure. We have developed the Altia Trust Center which is a collation of legal, compliance, disclosure and trust documentation made available both publicly, and openly after registering your details. Altia's Trust Center can be accessed here. You will find articles such as the Altia Master Services Agreement, Information and Cybersecurity Schedule, General Privacy Policy, Data Processing Agreement, and other documents relating to Altia's commitment to global information and cybersecurity. Altia complies with and holds assessment outcomes asserting effective controls of the Australian Government Information Security Manual & Australian Government Protective Security Policy Framework to PROTECTED; United States FEDRamp Assurance Program; United Kingdom's Cyber Essentials Plus and ISO:IEC 27001.

Transparent Pricing. Overnight Compliance.

LICENCE TIER	COST PER USER (PER YEAR)
5 to 10 Licences	$3,900
10 to 30 Licences	$3,300
30 to 100 Licences	$3,000
100 to 250 Licences	$2,600
250 to 500 Licences	$2,200
500 to 1,000 Licences	$1,800
1000 + Licences	$1,400

THE ABOVE PRICES ARE EXCLUSIVE OF GST AND REFERENCED IN AUD.

26 YEARS OF PROTECTING THOSE WHO PROTECT US

Altia is the global leader in intelligence, investigation, case, and evidence management software, security & compliance platforms, and highly specialised consulting services.

Established in 1996, Altia has grown to service over 370 Public Safety & Justice government and non-governmental bodies across organisations in the United Kingdom, Canada, New Zealand, the United States, and Australia. Altia has offices in all locations it serves, with over 100 staff supporting our growing list of loyal customers.

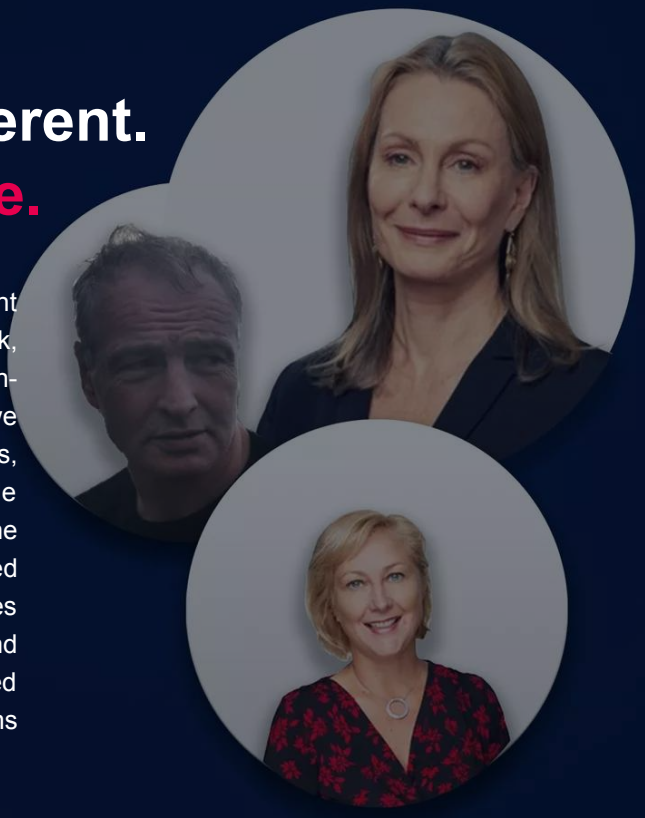
Altia's workforce represents the customers it serves. A majority of Altia employees have a Public Safety & Justice, or investigative background – including members of Altia's Board of Management. This includes Altia Chief Information Officer, Brice Neilson, who spent 16 years in Australian government positions and now leads Altia's Information, Cybersecurity and Innovation Division, and Altia's Consulting Services (ACS) - its premium support and delivery team. As an experienced Microsoft Certified Cloud Solution Architect and recognised expert in strategic policy, risk, and governance in the field of information management - Brice leads ACS's cross-functional team of subject matter experts to deliver our most mission-critical solutions.

Privately owned by sophisticated and ethical investors, Altia is a well-established, funded, and resourced provider, protecting its customers' most critical capabilities, streamlining their workloads, and safeguarding them from individual and repetitional harm, through the ever-changing, dynamic, and often challenging threat landscape confronting technology tomorrow.

When consuming our products or engaging ACS services, you become part of the Altia family, along with many other organisations across the world, and, right here in Australia.

Microsoft
Cloud Solution Provider

Altia's approach makes it different. *Altia's people make it* effective.



Altia's 70 technology specialists operate in a unique environment supporting digital solutions that are entrenched in areas of extreme risk, and regulatory constraints that only exist to support high-stakes, mission-critical and volatile practices. The technology used by industries we specialise in almost always has a material link to areas of human rights, privacy, rules of evidence or complex laws which must operate alongside the systems and not against them. With this material link between the technology, we work with and other areas of speciality, Altia entrenched that subject matter expertise into our teams and projects. Altia operates cross-functional teams of technology specialists, strategic visionaries, and globally recognised experts in niche areas of risk, law, and policy - involved in every project to ensure our digital answers to significant problems operate WITH, not AGAINST the environments of risk they reside.

Dr Allison Stanfield PhD, LLM has 30 years of experience as a lawyer and in business, with expertise in cybersecurity compliance, privacy, and commercial impacts of technology. Having obtained a PhD in electronic & digital evidence, Dr Stanfield works closely with solution design and risk analysis teams to identify and mitigate risks born from digital operations that are often overlooked. The most basic example is security controls being implemented to purge, delete, or alter information that is perceived as a security risk. By implementing the control to reduce cyber risks; one threat is mitigated - but is another risk born when that purged information is deemed evidence and the control is in fact committing criminal acts in the destruction of evidence? Dr Stanfield works with our architects and risk teams to ensure compliance with all facets of information management and archiving to reduce the likelihood of exposure to these instances, but important document an understanding that can be relied on if required if challenged. Dr Stanfield is also authorised to represent Altia and its customers, if required, in legal proceedings.

Helaine Leggat LLB, CISSP, CISM, CIPP, CIPT is a specialist lawyer admitted to the Supreme Court of Victoria, Australia. Helaine is an expert in cyberlaw, hybrid warfare, and data security while internationally experienced in cyber security, personal data protection and governance. Helaine contributes to the greater information and cybersecurity community, often called upon by the Australian Information Security Association, Expert Network for the Australian Government Department of Industry Innovation and Science, Law Institute of Victoria Technology and Law Committee, and the Australian Institute of Company Directors. CISSP, CISM, CIPP, CIPT and author of Women in the Security Profession: A Practical Guide to Career Development. (2016 – Elsevier Science Publishing. Spring 2016. Ed. Sandi J. Davies). Helaine is critical in Altia's project delivery as she horizon scans throughout the discovery, design, and delivery processes, continually assessing for exposure risks not only in the present - but the future, to ensure the technical architecture is not dependent on legally or politically volatile technologies. Like Dr Stanfield, Helaine is an expert witness and authorised to represent Altia and its customers, if required, in legal proceedings.

Dr John Buckley PhD is an internationally recognised expert in risks stemming from high-risk processes. Dr Buckley specialises in assessing risks presented by activities, processes, policies, or the general nature of work being undertaken. Dr Buckley's focus is to look at an organisation's risks holistically and profile those risks, so an organisation knows where to focus particular risk treatment programs, training, or refine robust policy frameworks. Dr Buckley empowers organisations to accept tolerable risks, before working on mitigation strategies for the residual. More importantly, Dr Buckley provides documented justification of WHY it is necessary to undertake and accept risks, and the rationale behind the framework of policies, governance practices and procedures to ensure the framework is holistically and readily defendable. Dr Buckley informs design teams and architects of ways to better align risk with operational and administrative priorities. Like Dr Stanfield and Ms Leggat Dr Buckley is accepted as an expert witness in this field and authorised to represent Altia and its customers, if required, in legal proceedings

726 SECURITY CONTROLS, IMPLEMENTED FOR ONE.

The world has changed, and it continues to change each day as technology becomes more entrenched in the lives of every Australian. It powers our critical infrastructure, supports our economy, and enriches our healthcare system. It makes our lives easier, and more enjoyable. It brings digital efficiency, quite literally, to everything we do. Technology provides our military capabilities with a digital advantage over those looking to do us harm. The digital world is now one of our most valuable assets and fundamentally important to every facet of our lives. Technology empowers everyone, everywhere. Such an inordinately valuable asset would, if it existed in physical form, be locked away, surrounded by cameras, sensors, and armed guards. However, this asset, a $5.2 trillion technology industry, is left vulnerable as the phone in your pocket, or the smart watch on your wrist.

9,000 & $9,000,000.00

Today, rather than criminals confronting victims in a violent robbery, the new age cybercriminal would rather steal from a safe difference. Sitting comfortably at an unknown location, protected from view, and with endless time to take a part of that $5.2 trillion asset and leave long before the robbery is detected. In Australia (2021-2022), robberies decreased by 3% from the previous year, down to **9,140** incidents, with property crime still costing the economy an astonishing **$9 million** per year. **$173,076** per week taken away from our vulnerable community members who require it to survive, as the country faces economic uncertainty and fiscal stress. **9,000 robberies. $9 million impact.**

67,500 & $33,000,000,000.00

In that same period, 67,500 Australians were subject to a cyber security attack at an economic cost of **$33 BILLION** per year, **$634 MILLON** every week, or **$90 MILLION** every day as a cyber-attack occurs on average, every seven minutes just in Australia. 726 Security Controls seemed like a substantial number, but not compared against **33,000,000,000.00.** Now that's a substantial number. These big numbers are daunting. They put a dollar value on the costs of cybercrime in Australia so we can contextualise the importance of 726 Security Controls. **But the number that matters the most is ONE.**

JUST ONE OF THESE ATTACKS OCCURING EVERY SEVEN MINUTES

Cyber-attack is Australia's fourth most likely crime, only outdone by minor drug possession, traffic offences, and shop stealing. With a cyber-attack occurring every seven minutes, exploring just ONE hypothetical attack scenario truly contextualises this threat.

A uniformed police officer observed a vehicle pulling into a driveway on a normal suburban street. The officer stopped their patrol car and went to speak with the driver. He introduced himself to her. Her name was Melissa. She was 28 years of age, and her baby son was in the rear of the vehicle. The officer politely told Melissa the reason he was speaking to her was due to a problem with the lights on her vehicle. The officer asked to see her licence. Melissa was reluctant and nervous but gave the license to the officer. The licenced address was from another state but otherwise in order. Everything checked out. After giving words of advice about the vehicle's lights the officer returned to his car. Melissa walked into the house with her child. The officer completed an incident report containing the details of the traffic stop into the police records management system and both parties went on with their day. Months later, the police service was the victim of a cyber-attack, and many records were stolen, soon appearing on the Dark Net, sold by cybercriminals to others to exploit. *Melissa's details were **ONE**.*

*When told of the breach, Melissa took comfort she had not updated her interstate address - very intentionally. Melissa fled her interstate address from a domestic violence relationship where she genuinly feared for her own safety, and that of her child. According to Melissa, there was no record of her new address. No risk to her from the breach. But, there was **ONE**. Meticulous in his record keeping, the police officer in completing his traffic report from a few months prior, included the precise location of the stop. That was all that was needed for her motivated ex-partner to find her.*

If the billions of dollars previously mentioned doesn't highlight the critical importance of strict information and cybersecurity practices - perhaps Melissa's (albiet hypthetical) story might. Sitting in her house, seemingly safe by very intentionally protecting her address, and herself from databases. Melissa is perhaps the only ONE factor in considering the impact cyber-attacks have on our community. 726 Security Controls implimented to stop ONE.

altia.