



FAQs





TECHNICAL SPECIFICATIONS

WHAT IS THE COMTRAC PLATFORM BUILT ON?

- The Comtrac platform is built on the modern Cloud SaaS platform, Microsoft Azure, implementing best-of-breed technologies including Microsoft.net, Cloud-native services, and front-end Single-Page-Applications for responsive user interfaces. The tech stack includes:
- Middleware and backend services developed in .Net 6+/C#
- Azure Cloud Native services including SQL Server, Service Bus, CosmosDB, Storage, Active Directory and more.
- Front end technologies including Single Page Applications using Angular 12+, Vue.js 3.0, and Flutter/Dart 2+.

HOW WELL IS THE COMTRAC PLATFORM EQUIPPED TO SCALE WITH YOUR BUSINESS?

Comtrac uses Microsoft's recommended architecture patterns and practices for building applications that scale in the Cloud.

Using Microsoft Azure's Cloud infrastructure, Comtrac can scale with your business by leveraging Azure's services and resources to scale. Comtrac can support 1000s of users and store terabytes of data.

HOW DOES COMTRAC INTEGRATE WITH THIRD PARTY APPLICATIONS?

Comtrac is a platform-based product with APIs. It can integrate into a range of systems. Existing integrations we have built:

- SafetyCulture (iAuditor),
- Axon Evidence,
- Salesforce,
- Docusign™
- Google services (Map & address data),
- Australian Business Register (ABR),
- A range of bespoke customer record management systems.

Our integration team has extensive experience in documenting, developing and testing system integrations and data migrations. Integration with 3rd party applications is achieved through several mechanisms:

- APIs (REST) for system-to-system communication. Comtrac provides an integration API document and system-integration-environments (SIT) for agency IT integrators.
- Webhooks (through a proprietary PlugIn architecture) that enables integrations that don't work with out of the box integrations via the API.
- Custom fields to extend the data storage capabilities of Comtrac when system integrations require the display of data in Comtrac sourced from external systems.



DOES COMTRAC SUPPORT SINGLE SIGN ON?

Comtrac supports Single-Sign-On via SAML 2.0. The process is straightforward, Comtrac requires access to the agency IT staff to configure the Single-Sign-On capability.

- Comtrac provides the agency with a service provider metadata file to assist the agency with Identity Provider (IDP) setup.
- The agency provides Comtrac with their IDP metadata file once the IDP setup is complete.
- The SSO integration is verified in the agency's UAT environment before deployment to Production.

HOW DOES COMTRAC APPROACH DATA MIGRATION FROM LEGACY SYSTEMS?

Data from agency systems can be migrated into the Comtrac application. The technical approach varies due to the diversity of agency systems and data. Our analysts typically initiate a discovery project and provide a detailed transition-in plan for the migration project. We provide a variety of solutions, including:

- Using standard SQL Server ETL tools for ingestion of data via csv files, xml or json files.
- API to API ingestion where historical datasets are not large.
- Custom ETL tool development for sophisticated rules and data requirements.

We use a standard process where data is loaded into staging environment(s), verified, and loaded into production with rollback/recovery at each environment.

HOW DOES COMTRAC DEPLOY UPDATES?

Your Comtrac licence includes support, maintenance, and upgrades from our continuous R&D programs. Updates are deployed according to Comtrac's internal feature-release cadence, with minimal downtime to customers.

We use a fully automated Continuous Integration/Continuous Delivery deployment pipeline.

For agencies with customisations and integrations, updates concerning these are first deployed to a UAT environment for agency testing and approval before deployment to Production occurs.

All updates can be 'rolled back' if required.

THIRD PARTY PENETRATION TESTING

Comtrac has a policy to engage a third party to perform penetration testing on every new Comtrac feature when it is ready for testing, or every three months, whichever comes first.

This ensures the integrity of the system is continually tested, and that the system is not open to exploitation or vulnerabilities.

The scope of the penetration testing is white box testing, ensuring complete coverage of the software from end to end, including testing authenticated user access and endpoints.

Any issues identified are remediated and the system is penetration tested again prior to release to client environments.



CYBER SECURITY & INTEGRITY

ISO 27001: 2013 CERTIFIED – INFORMATION SECURITY MANAGEMENT SYSTEMS

Your agency's data and information are valuable assets and deserve to be protected from potential risks or threats.

To secure your intellectual property and business data, Comtrac implements and maintains an Information Security Management System (ISMS) which is certified and audited annually.

Our Certification to ISO/IEC 27001 helps us comply with numerous regulatory and legal requirements that relate to the security of information.

PROTECTED HOSTING

To align with the Australian Government Information Security Manual (AGISM) with respect to data classified as PROTECTED, we have partnered with Protected Cloud Providers assessed and compliant with the policies and controls that make up the PROTECTED standard.

As Cyber threats become more prevalent, it is paramount that the Comtrac solution can be hosted within an environment that meets and exceeds the needs of the Australian Government as outlined in the AGISM.

SECURE VPN GATEWAY

Each client version of Comtrac has the option for additional security using a virtual private gateway as a tool for establishing a safe tunnel to connect and transport encrypted data between devices, the cloud, and enterprise servers across the internet.

The virtual private gateway is used to create a VPN connection that is both secure and reliable.

APRA REQUIREMENTS

Comtrac has been assessed and complies with the regulations as outlined by APRA with regards to hosting APRA regulated organisations data in a secure environment.

This assessment reviewed our policies and controls related to Disaster Recovery and Business Continuity, as well as an in-depth review of our Azure environment and the security controls that have been implemented to secure our customer data.

**For more information, request a copy of the
Comtrac Cloud Security Statement 2022 (220801).**



AUSTRALIA: 1300 292 939

sales@comtrac.com.au

www.comtrac.com.au