

Crimson Service Definition

Product Overview

Crimson is an investigation and case management system designed to support investigators working in the public and private sector. It delivers an intelligent secure database for any type of organisation that has a need to investigate incidents, allegations, or any type of criminal activity.

From complex investigations to straightforward lower-level crime management Crimson will support every stage of the investigative process.

Crimson has been developed in close liaison with investigators across a number of law enforcement agencies including the Police and Trading Standards. In developing the system, the recurring theme was to provide end users with a modern, flexible, scalable, and easy to use software solution that can be used for any type of investigation.

Crimson provides a number of modules that can be used together or individually. This allows organisations to choose which module(s) best fit their requirements.

The investigations module provides a central hub for all investigations across an organisation. These can be recorded using Agency, Region and Department providing organisations working across a wider geographical area with a greater management reporting facility. Access to investigations can be restricted on a 'need to know basis'; Crimson is configured to allow a user to see all the investigations to which they are attached. Top-level users, such as supervisors, can be configured to view all investigations by default.

A central intelligence hub is provided to allow the recording of intelligence held outside of an investigation. Intelligence reports are added using the National Intelligence Model structure providing provenance, handling codes, risk assessments and records of dissemination. Access to intelligence is provided using "level permissions". The central intelligence hub also has the facility to add intelligence log entries, attach documentation and link to other intelligence reports or Crimson records (People, Addresses, Organisations, Telephones and Categories).

The incident module provides an area to record complaints or allegations that an organisation may want to record and review to decide whether an investigation should take place. Incidents can be classified and graded as per the organisation's need through customisable code tables. Details of the person reporting, victim and suspects are also recorded along with a description, date, time and location. An incident log is also provided allowing users to record any work or decisions taken on the incident. At the conclusion of the incident an "outcome" is recorded providing the organisation with a comprehensive reporting tool.

At the conclusion of an investigation, users can conduct a disclosure assessment from within the investigation. Crimson allows disclosure assessments under CPIA and Disclosure for Scotland, and prompts users where disclosure assessment is required. At the end of the disclosure process a full list of disclosure items is produced in an electronic format. Witness lists and exhibits lists are also produced from within Crimson. This saves the exhibits officer time and effort ensuring a smooth transition of witnesses and exhibits during any court appearance. The system also includes a court bundling feature which allows statement and exhibit lists to be bundled for court use.

Crimson also incorporates its own Document Management System. This provides a user with the facility to attach various types of electronic files and efficiently manage the many documents, images and other media associated with investigation work, creating a virtual filing cabinet. This

storage facility will provide the ability to store and view documents of all types, from text documents to images to audio/video media.

Crimson CIA

The Crimson Crime in Action module is designed to assist organisations in the management of time critical and fast-paced incidents. It can either integrate with our full investigation management solution, Crimson, or work as a separate "Crime in Action" module.

The solution delivers an efficient and secure database which, coupled with the complete Crimson solution, manages the entire incident and post investigation process, all the way through to preparation for court.

Crimson CIA focuses on improving the management, communication and delegation of the "Crime in Action" team, by streamlining the management of such fast-paced incidents. It manages all incidents and documents in one centralised database, ensuring all team members are up to date with the most recent and important information at all times.

Crimson Features

- Investigation, Incident, and Intelligence modules
- Records management and information recording
- Dissemination to other agencies
- Restricting access to sensitive intelligence
- Risk Assessment of data as required
- Investigation Logs
- Witness Statements
- Actions Management
- Exhibits Module
- Document management (including the attachment of electronic file types)
- Surveillance Logs
- Disclosure
- Creation of court documentation
- Case progression and final outcome
- Configurable integration with email for the electronic allocation of tasks/actions
- User defined Forms feature using customer templates
- Management Information Statistics – reporting module
- Statement and Exhibit court bundling
- Events timeline
- Visual link chart
- Separate Crime in Action module

Crimson Technical Overview

WPC Crimson is a web-based application making use of the latest web development methodologies and technologies. This section is a high-level technical overview of the solution.

Cloud Software and Information Assurance

WPC Products delivered as a cloud service is delivered by WPC Software through our cloud-hosting partner Microsoft Azure.

WPC has a fully implemented Information Security Management System, which outlines the governance and clear responsibilities relating to information security including the cloud service provided. The ISMS is accredited to ISO27001. WPC Software also holds ISO9001 and Cyber Essentials Plus accreditation.

Microsoft Azure undertake formal accreditation activities and accreditations include NPIRMT – PASF, Cyber Essentials Plus, CIS Benchmarks, CSA STAR Certification, ISO 20000, ISO 22301, ISO 27001, ISO 27018, ISO 27701, ISO 9001, and SOC 1/2/3.

All data centres used by WPC are highly resilient, UK-based and separated by >100 miles for geographical diversity.

Relevant WPC staff are vetted to NPPV3 level and are Security Cleared.

WPC Cloud Products standard package

WPC Products can be delivered as cloud software through Microsoft Azure. The standard service includes:

- Provision of a multi-tenanted environment within Microsoft Azure. Separation between customers is ensured with completely individual databases dedicated to the customer along with dedicated credentials.
- Delivery of Premium Disk/High Memory Trusted Launch Web Servers through Azure IaaS Compute which are scalable to meet customer needs.
- Azure SQL Server Managed Instance with provision for up to 500GB of storage per customer (individual files should not exceed 50MB).
- Both the Web and Database environments are provided with 99.95% availability.
- All data is stored in a clustered environment with three copies within geo-redundant data centres, with each data centre within the UK.
- Access via Standard Internet connectivity over common protocols - namely HTTPS, using a SHA-256 Secure Hash Algorithm and TLS 1.2/1.3 protocol.
- Backup of the Web Servers is taken as a daily VM snapshot and is stored for 7 days.
- Backup within Azure SQL Server MI includes transaction log backups every 5 to 10 minutes, which are retained for a seven-day period. All data is stored in geo-redundant storage BLOBs with replication only in UK data centres and allows for point in time restoration.
- Access to WPC cloud solution is restricted to authorised users only, with role-based access being key to system authentication. Access to the service can be restricted in a number of ways. Our Standards options include:
 - A two-step authentication process, where a user is required to log-in to access the service prior to logging into the application itself.
 - IP Address Restriction to a customer network.

In addition, WPC also offer the following authentication methods, although these would need to be discussed and confirmed with WPC Software.

- Two-factor authentication using mobile application (additional costs and configuration may apply)
- Potential integration with Azure Active Directory or ADFS (additional costs and configuration may apply).
- WPC perform regular internal penetration tests and other security checks on our software. Internally, we make use of the Burp Penetration Test suite, which automatically detects and highlights any possible vulnerability from SQL Injection to Cross Site Scripting to authentication/password protocols. Third-party penetration tests are also commissioned annually on WPC products, as well as customer-commissioned penetration testing taking place regularly. Any highlighted issues raised by internal or external testing are prioritised for immediate resolution, retesting and release.

The above outlines the standard cloud software offering. Customers will need to discuss requirements with WPC should alternative options around resiliency and configuration be required. Additional details are available in WPC's Cloud Security Principles and Information Assurance documentation, which is available upon request.

Service management details

Software support

Software support is provided by WPC Software's dedicated team of developers. The support is provided from 8:30am to 5:30pm Monday to Friday (excluding English public holidays). When purchasing support each customer is entitled to receive fixes and upgrades to the version of the application they are using.

WPC has active User Groups for each of its products, all new customers will be invited to join and become an active member of the user group community. Each group is entitled to a number of development days within the support agreement, new customers will be able to influence the direction and development of the application.

Service Levels

WPC Software's service levels and support guidance is outlined within our Support Issue Management Process guidance, which is available upon request. Our standard SLA for software support is:

Priority	Time to respond	Regularity of Updates	Time to fix
Critical	4 working hours	Every 1 working hour	4 working hours
Major	4 working hours	Every 4 working hours	8 working hours
Minor	8 working hours	Every 2 working days	2 working days
Cosmetic / Trivial	2 working days	Every 2 working days	Next release, or earlier by agreement.

As part of the basic package, WPC cloud software is delivered through Microsoft Azure and has an availability of 99.95% on a monthly basis.

Service constraints

All software upgrades and patches are applied by WPC Software and agreed in advance with the customer. Planned maintenance of the product cloud service occurs on the second Tuesday of every month between the hours of 18:00 and 23:30. Urgent security patches may be applied on an ad-hoc basis if required and any possible downtime will be notified to the customer.

Details of the level of backup/restore and disaster recovery that will be provided

Backup of the Web Servers is taken as a daily VM snapshot and is stored for 7 days.

Backup within Azure SQL Server MI includes transaction log backups every 5 to 10 minutes, which are retained for a seven-day period. All data is stored in geo-redundant storage BLOBs with replication only in UK data centres and allows for point in time restoration.

Disaster Recovery

As part of our standard service, backups are stored at a remote site. In the event of a major failure affecting the primary data centre, WPC Software will endeavour to re-provision the environment within the second data centre, subject to capacity. In a complete disaster the RPO would be “up to” 60 minutes with an RTO of 1 working day.

Training

WPC Software have a team of trainers available to train end users in the use of our systems. Prices for training can be supplied on request based upon our advertised daily rate.

Details of any trial/demo service available.

WPC Software can provide access to a demo system upon request. It should be noted that this system should only contain demo, not live data.

On-boarding and Off-boarding processes/scope etc.

On Boarding

Prior to the service commencing WPC Software will appoint a Project Manager. The Project Manager will obtain information including the following from the customer:

- The configuration details for the product
- A copy of any data to be migrated into the system
- Quantity of users requiring access and resource requirements
- List of users requiring access and privileges
- The training requirements for the users

Once this information has been gathered the Project Manager will put together a project plan to complete the On-Boarding process. This project plan will identify the actions and timeframes to complete a successful start to the contract.

Off Boarding

When a termination date has been agreed WPC Software will archive the customer data in an agreed format. This data will be sent to the customer in a secure manner. The service will be switched off at the point of data archiving and service termination. All data will be securely deleted.

The price for completing the On-boarding and Off-Boarding can be provided following consultation with WPC and dependent on customer needs.

Customer responsibilities

Any customer using the hosted service is responsible for the content of data held on the system.

The customer is responsible for obtaining connectivity to the system within their own network.

The customer is responsible to ensure all users of the system are aware of the service definition and the constraints / Service Levels provided by the system.

Technical requirements

Consumers will require appropriate network connectivity such as internet access. Where required, consumers are responsible for procuring and managing appropriate devices or software to meet the requirement for data security over the various forms of connectivity.

Customers will require access to a modern up to date browser to use WPC cloud software.

Ordering and invoicing process

Communication with WPC Software should be made to ensure the correct elements have been specified. Once concluded a purchase order should be sent to the WPC Software Account Manager. Invoicing will be sent based on agreed payment profile or as outlined within the quotation, with payment required within 30 days.

Termination terms

The contract can be terminated with 30 days' notice. On the day of termination, the customer data will be archived and sent securely to the customer. Once terminated system access will be removed and restoration of the service will not be possible.