Cardinus Limited Cardinus LLC	Collectively Cardinus

Technical Overview – NG applications

Cardinus Risk Management 4th Floor 3 East Grinstead House Wood Street East Grinstead RH19 1UZ
Cardinus LLC, 8335, Sunset Blvd, West Hollywood, CA 90069
Tel UK: +44 (0) 20 7469 0200 Tel US: 323 337-9016info@cardinus.com www.cardinus.com

Contents

1.0 Introduction

1.1 Purpose of document

The objective of this document is to provide a technical overview for the following Cardinus products:

- PACE - A reporting, administration and risk management control engine designed to be used with Cardinus programs.
- Risk management program (e.g. Heathy Working Program) – containing e-learning content with built in self-risk assessment designed to reduce the risk of accident or injury to course users.
- Authoring tools and programme engine - to allow the rapid build and configuration of e-learning and risk assessment content.
- File manager – access to the Cardinus content library together with the ability to upload and store customer content applicable to courses and services purchased.

It should be noted that:

- This document defines the architecture of Cardinus standard products.
- Implementation and architecture can be varied subject to a customer's exact needs (if required).

1.2 Intended audience

This document has been developed to help technical staff understand the architecture of the Cardinus solution.

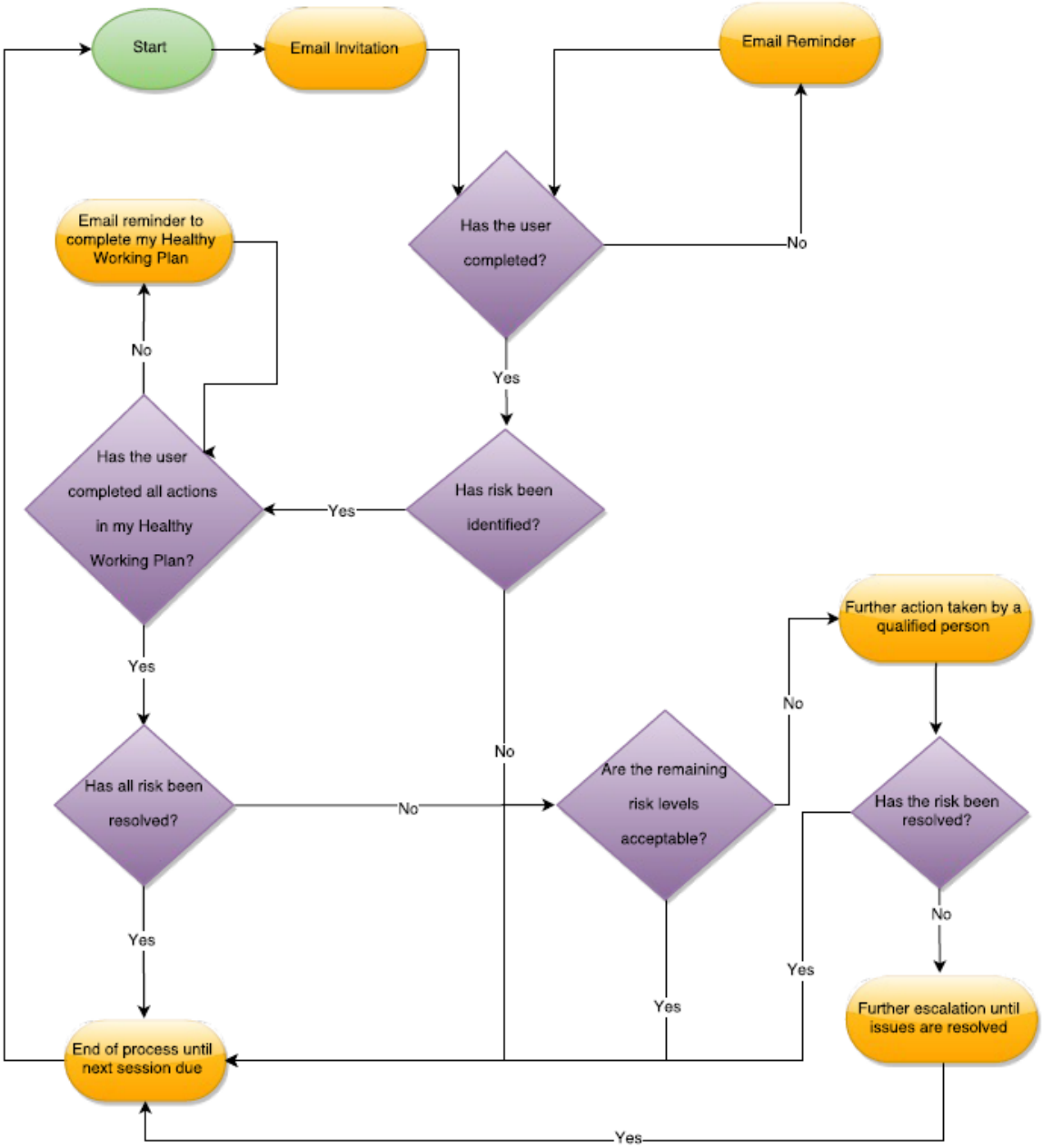
Assumptions

The following assumptions have been made:

- Access to Cardinus e-learning courses will be achieved by validating the user's login credentials against a set of values pre-populated into the PACE database.
- Whilst this document refers to the 'Healthy Working' program to describe the processes available within the Cardinus products, it should be noted that the majority of the processes are applicable across the range of our courses.

2.0 System architecture

2.1 Healthy Working business process



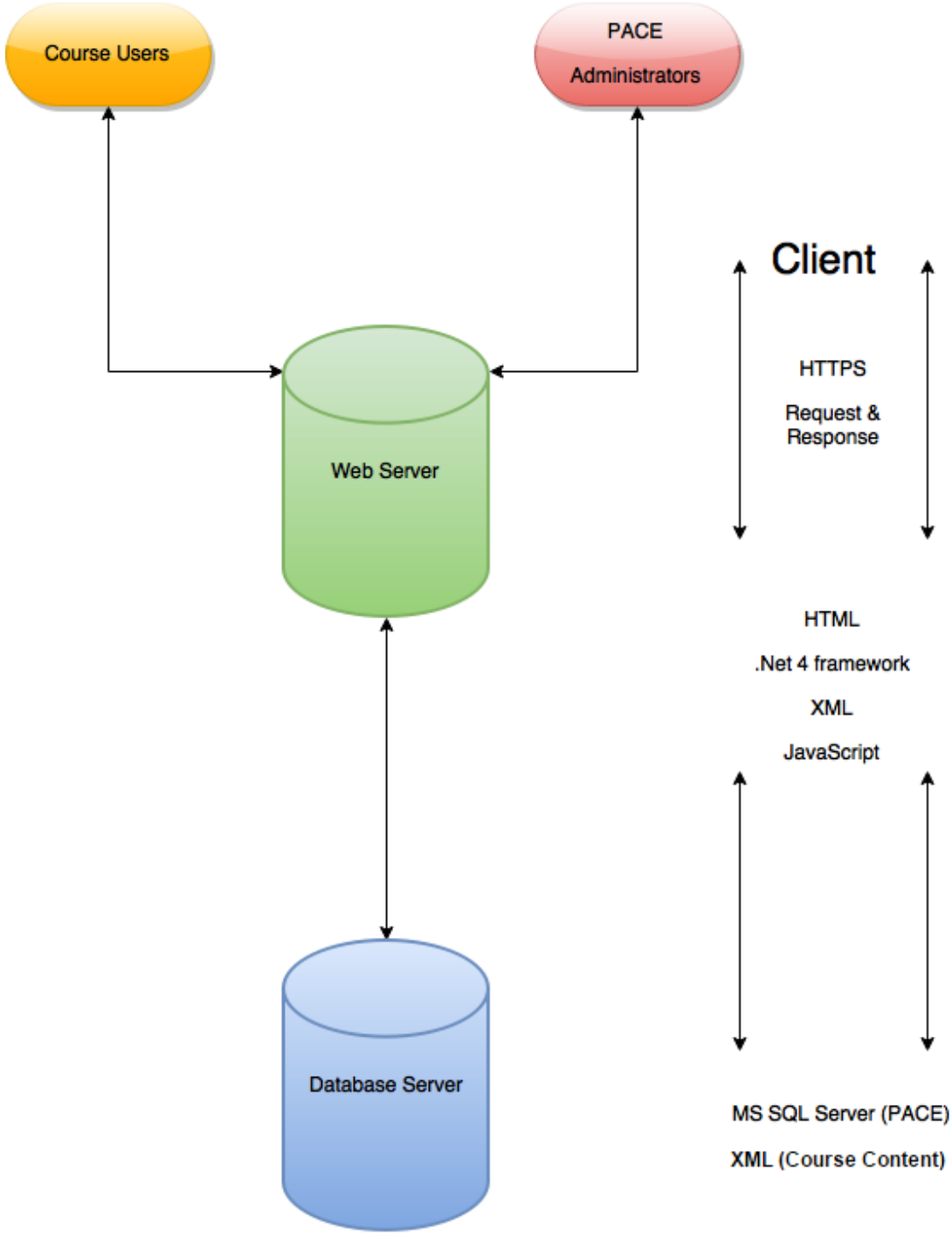
The diagram above shows a standard process for the Healthy Working program.

The workflow is controlled by scheduled emails which trigger user actions. Scheduled emails are made up of the following components:

- email templates
- email rules
- email schedules

2.2 Logical architecture

The Cardinus software is a web-based application, requiring a Web, Database and Email (SMTP) Server. All access to the software is via a standard web browser, requiring no additional client-side components or plug-ins.



2.3 Information flows

Standard system inputs

- Employee data from import files (or manually entered) including unique ID, first name, last name, email address, organization / department the employee resides within, plus user defined fields
- Self-risk assessment and training information gathered from the end-user
- 'Database update' where the user updates their own risk assessment records by checking items on the 'My Healthy Working Plan'
- Follow-up tasks entered into PACE by administrators to track inspections, reviews, maintenance, procurement etc., in fact any operation that is considered material to the issue raised by the user
- Comments/notes, configuration and scheduling entered by administrators

Extended system inputs

Additional automatic touch points can be integrated into PACE (please contact us to discuss your requirements) for example:

- Single Sign On (SAML 2.0 IDP & SP initiated)
- Driver Licence Information (through an API when hosted by Cardinus)

System outputs

- Training content, test questions and risk assessment questions
- 'My Healthy Working Plan' – viewed/printed by the user after self-risk assessment
- Optional - Ergonomic Desk Assessment
- Automated (scheduled) email alerts – set up inside PACE and processed by the (Cardinus Communication Dispatcher) CCD mail system
- Ad-hoc emails sent from within PACE
- PACE screen displays / Dashboards
- PACE printed reports (and PDF Reports)

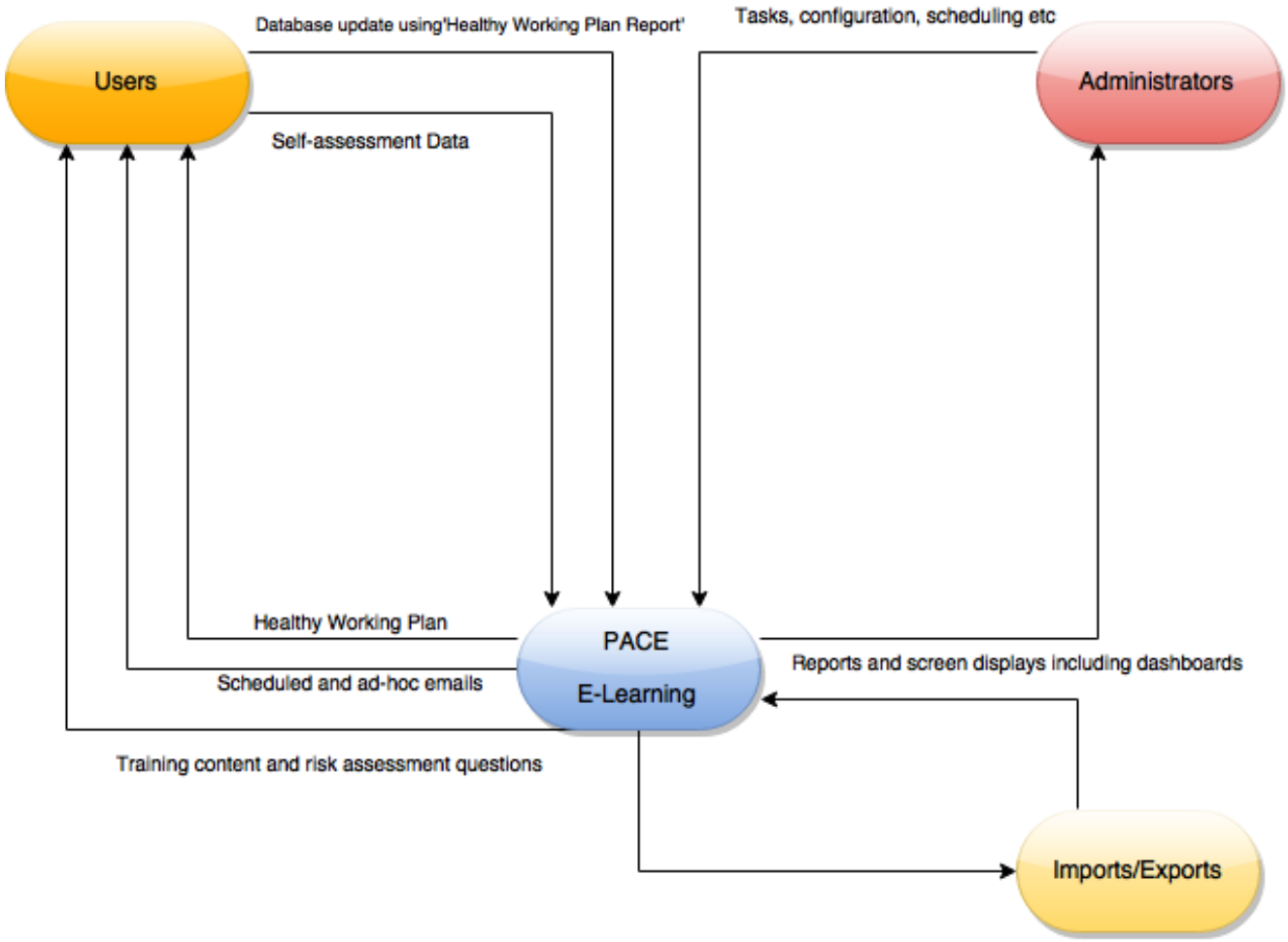
Extended system outputs

Additional automated feeds can be integrated into PACE.
Please contact Cardinus to discuss your requirements.

Example feeds are:

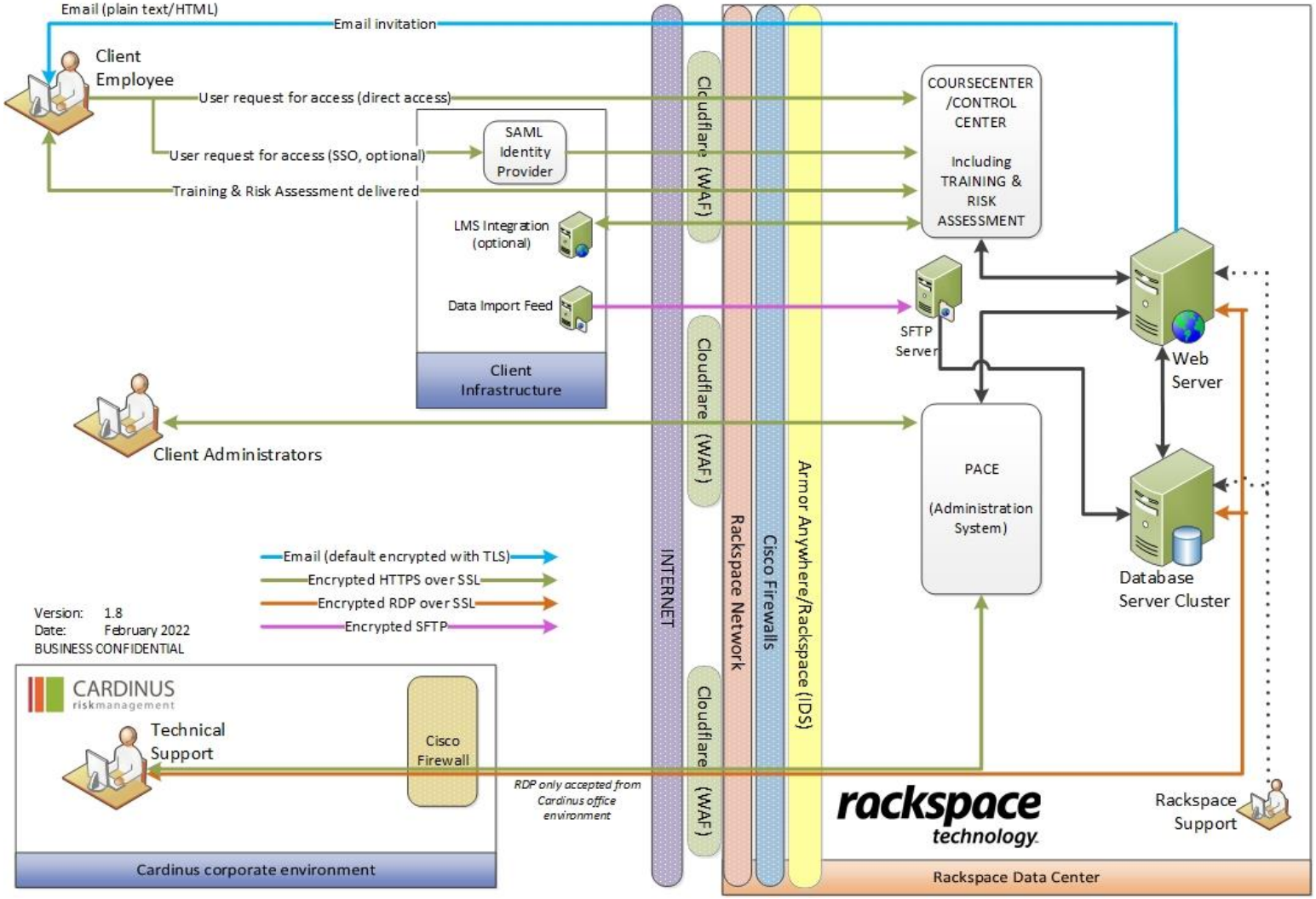
- LMS (AICC) exports
- Driver's license, MOT and insurance checking services
- API (data extracts & updates)

The diagram below shows the inputs and outputs from the system as a whole:

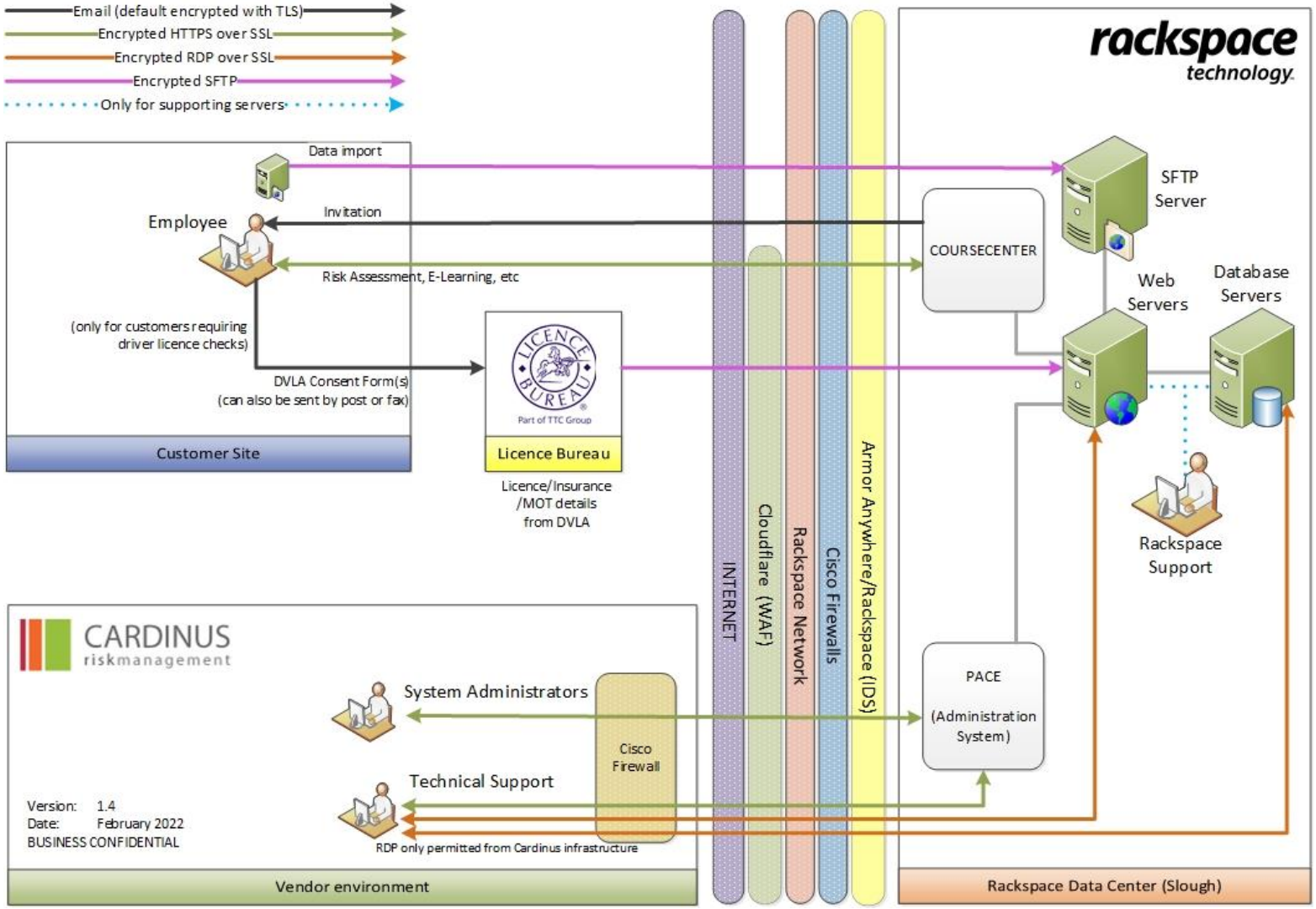


2.4 Data flows

Standard flow for Healthy Working customers



Standard flow for Fleet customers



3.0 System design

3.1 Overview

The Cardinus software is a web-based environment with courseware written in .Net MVC and including JavaScript and JQuery.

The administration tool, PACE, is also a web based product written using .Net MVC, JavaScript and JQuery. All access to the software is via a standard web browser.

3.2 Data sources

The Cardinus software uses different formats for storing data, these are as follows:

- XML – this is used for course content and application settings
- MS SQL database which acts as the central 'read-write' repository, referred to as the PACE Database. This database is where all infrastructure data (organizational hierarchy, course users etc.) resides. This includes all training, risk assessment and user profile records. The PACE management tool is used to generate reports from this database and to generate follow-up actions as a result of issues identified by users
- RDL files - these are used for report templates.
- Json – User for system configuration files.

3.3 Software components

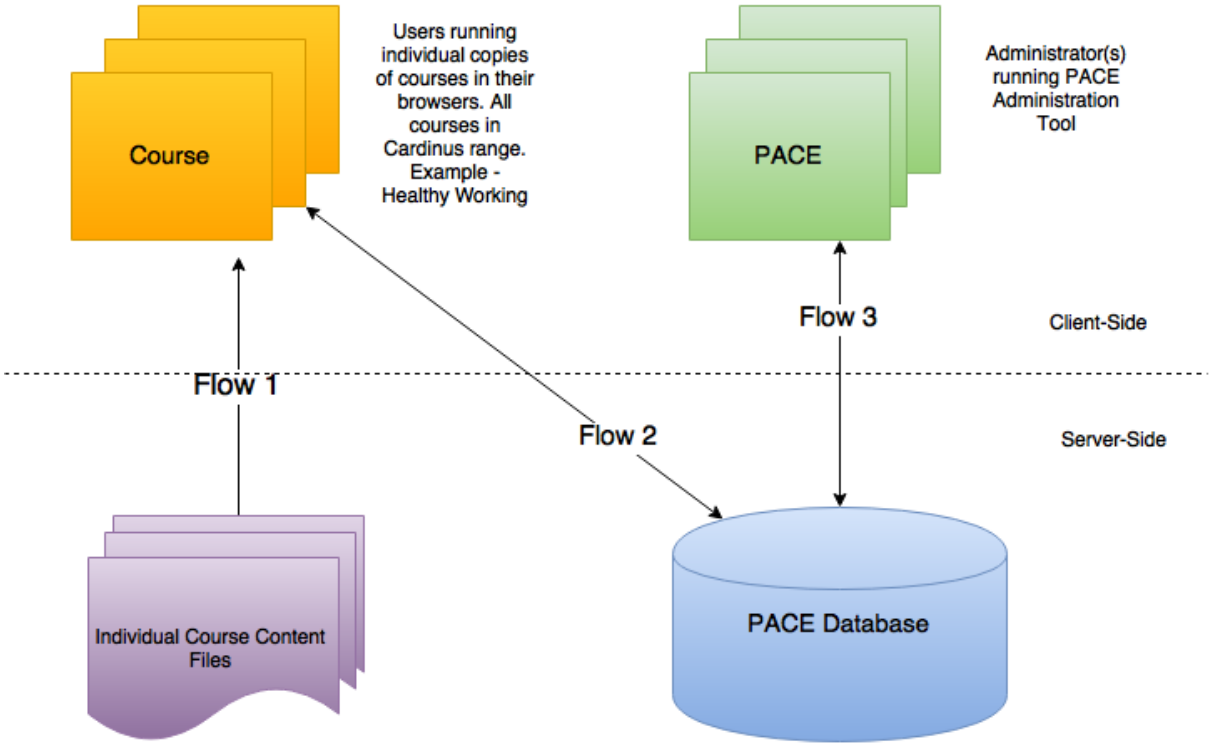
The system comprises of these main software components:

- The course(s), comprising of XML page definition. Each page definition references graphics and JQuery widgets
- The Course Hub. This too is based on .Net MVC and forms the framework in which the course is to run
- PACE administration system – developed in .Net MVC. The data is stored in a SQL server database
- Cardinus Communication Dispatcher (CCD). CCD runs as a service and communicates with the PACE database to determine which email schedules should be run or processed
- Authoring tools and programme engine to allow the rapid build and configuration of e-learning and risk assessment modules
  These tools are currently available to Cardinus staff to assist each organisation with their customization requirements whether text or image based.
  Please note that the standard service does not extend to the manipulation or creation of any images for the customer. Cardinus will quote for this type of work on request and provision of related information
- File manager – access to the Cardinus content library together with the ability to upload and store customer content applicable to courses and services purchased

3.4 Software and database interaction

The diagram below illustrates the way in which the courses interact with both the course content files (XML) and the PACE database. The individual course content files hold course-specific information, for example course test questions and pages and the PACE database holds both user information (name, department, location etc.).

Information Flows and Course/Pace Setup



Key:

Flow 1: Course-specific information and Risk Assessment questions from course content files, formatted for display in the user's browser.

Flow 2: At start of course: Creation of validation of User Login details, together with their place in the course if revisiting an uncompleted course. At end of course: Saving of course progress and/or saving of answers to Risk Assessment questions.

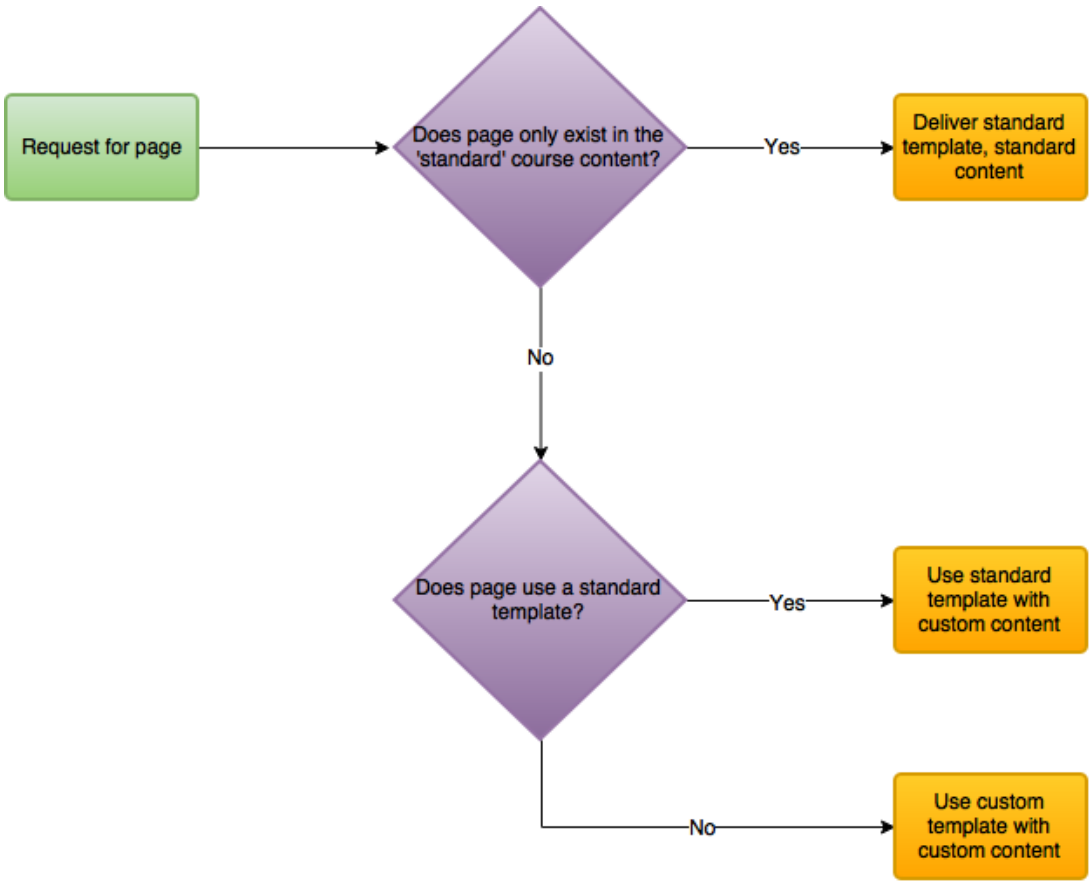
Flow 3: All administration activities, creation of users, locations and departments, generation of reports etc.

3.5 Dynamic customized content

Cardinus courses are CML template driven, bringing content together from both the 'standard' course content and the customers 'customized' course content. This methodology makes it easy to update the generic courses content without affecting the customer's custom content

The customized course content is an exact replica of the structure of the standard course content. However the customized course content only holds content that has been altered or changed. All other content required for the course, is pulled from the standard course content.

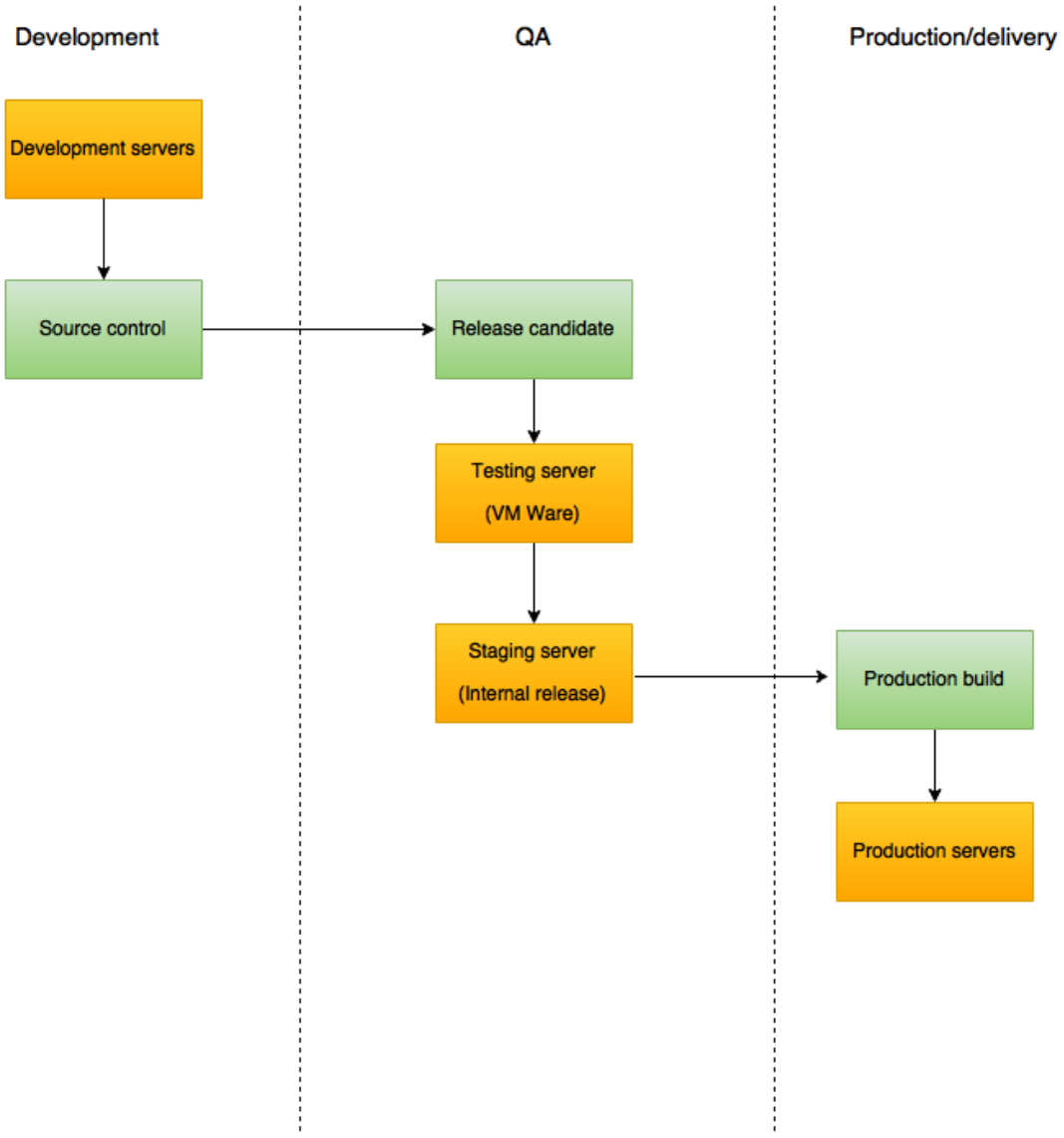
The process below can be used to describe how course content is displayed to a user.



3.6 Development process and testing

Development and testing are integrated into a single development methodology, starting with the development of test scripts covering the required functionality. These scripts are used both during development and functionality testing. For future development the same scripts are used for regression testing. After the development/testing process is completed, the application is stress tested and Beta tested.

Development environment



4.0 External interfaces and integration

4.1 Importing/updating user data

The following describes the standard procedure for importing data.

- The standard import process will populate, update and archive course users. If required, Cardinus can develop custom import processes to update extra user information. Please contact Cardinus for more information.
- The file layout for the import/update feed is specified in supporting documentation. Advanced Requirements Form (ARF).
- It is important that a complete import file is provided each time (not an incremental feed of new staff). This enables the script to automatically archive records (see below).

When the import runs, one unified SQL Server script performs the following:

- Where it finds a matching unique ID on the database:
  i) It will update data. **NOTE:** Before it updates a column (field), the script will scan the input file to see if ANY data is being provided for that column (in any record). If there is then it will update that column with the import data for all records. This will include removing data which is in the PACE database but not provided in the import file. If no data is provided for a column, then that column will be ignored and any data in the database will be unchanged.
  ii) It will perform a check on the archive flag. If it finds that the user is archived then the archive flag will be removed, bringing a user back from archive.
- Where it does not find a matching unique ID already on the database it will add the user's record.
- Where a database record exists but there is no matching unique ID in the import file, the database record will be archived.
- Whenever a record is being added, updated or archived, the organisational structure will be checked and added to the relevant database tables if missing. NOTE: If there are various versions of the same hierarchy name they will all get added. It is therefore vital that data is clean and consistent.

4.2 LMS integration

Refer to the Cardinus Advanced Requirements Form for detailed information.
It should be noted that the non-linear pathway offered by the latest generation of Cardinus elearning courses does not currently replicate into the SCORM v1.2 standard. Our courses offer a unique course experience based on selections made within the Profile.
Any queries around the support of SCORM should be directed to the Support desk in the first instance.

5.0 Data security and resilience

5.1 Introduction

Cardinus systems are designed to capture, hold and manipulate information, which could be of a confidential nature. Therefore, Cardinus systems are monitored constantly to ensure:

- Protection against unauthorized access to data
- Protection against hacking / viruses
- Protection against accidental loss through hardware or software failure

Customer hosting servers are located within Rackspace data centres in:

- (UK) Slough, Berkshire
- (US) Richardson, Texas

The devices within the network infrastructure are protected and monitored using a combination of security products:

- Armor Anywhere/Rackspace IDS (Managed Service)
- Armor Anywhere/Rackspace SIEM (Managed Service)
- Cloudflare DDoS Mitigation
- Cloudflare Web Application Firewall
- Opswat MetaDefender (file upload scanning)

In addition, all devices are vulnerability scanned daily (internal & external) by Armor Anywhere/Rackspace, and applications are penetration/web application tested at least quarterly by Appcheck, designed and built by CREST and CHECK accredited penetration testers.

5.2 Application security

User types

There are two types of application user:

- Course Users, who undertake the training and risk assessments
- PACE Administrators, who manage risk assessment data, organize user access, manage issues arising from risk assessments, generate follow-up actions, etc.

PACE administrators can be sub-divided into:

- Master Administrators with full access to all features
- Sub Administrators with limited access to user data and functionality

Further granularity for administrator rights can be specified by using rights and roles.

Note: As permissions for administrators can be configured to suit the customer's preferences, it the customer's responsibility to audit and maintain these permissions.

Course access

Course users can be validated using different methods of authentication. For example, the user's unique ID (typically a personnel number, username, email address, etc.) and a password which is set upon first login.

The PACE database is pre-populated with user data via:

- A spreadsheet of user data supplied by email to the Cardinus Support department
- A comma separated value (CSV) file sent directly to the production server for automatic processing
- An administrator adding the information manually into PACE

Note: It is feasible that the methods of authentication for PACE and the Course Hub are different. For example, PACE might ask for a Username and Password while Course Hub requires Username and Email.

All data exchanged between a client/browser and Cardinus production servers is encrypted in transit (HTTPS, TLS1.2+, SHA256) and at rest (AES-256) using DELL EMC Data at Rest Encryption (D@RE)..

5.3 Hosted service security, availability and resilience

Physical security and resilience

All hosting servers are located within Rackspace data centres. UK-based servers are located in Slough, Berkshire, and US-based servers are in Richardson, Texas.

Rackspace and Cardinus are ISO27001 accredited, and Rackspace are annually audited to SSAE16-ISAE 3402 SOC1 Type II (formerly SAS70), SOC2 & SOC3.

All data centres are manned 24x7x365 by Rackspace Operations personnel and Data Centre engineers, and security guards are also on site 24x7x365. Site access is controlled through two-factor authentication (RFID and biometrics), CCTV camera surveillance covers all entrances and exits, and access for all staff is by the “least privilege” policy (including no public or customer access to data halls).

An onsite substation provides an ensured clean power feed into the facility, with 3MVA of power currently available (upgradeable to 15MVA). Separated redundant UPS systems feed power to each data hall, giving 10 minutes of battery reserve time before 2.5MVA diesel generators in N+1 configuration kick in, with 24 hours of fuel available onsite and an 8 hours SLA for additional fuel provisions.

Air cooled chillers are installed in N+1 configuration, and are all protected by generator back up power with dual power feeds to CRAC units. The data halls have a 700MM pressurized raised floor, hot/cold aisle cabinet layout, and leak detection system throughout the raised floor.

A dry pipe, pre-action, double-knock (water based) fire suppression system is in place, with smoke, heat and VESDA detection systems.

Qualified mechanical and electrical engineers maintain a full Building Management System (BMS) 24x7x365, providing human response verification to alerts from all environmental aspects of the facility (i.e. water sensors, air temperature, humidity, etc.).

Rackspace provides a fully resilient and redundant network infrastructure. The entirely switched network employs Cisco chassis based switches running HSRP (at least N+1 hot failover) to ensure that data can be routed even in the event of device or link failure. Network traffic is constantly monitored and usage remains significantly below capacity at all times (approximately 20%) to allow the network to accommodate even the largest spikes in traffic. As network utilisation reaches 30%, more network capacity is automatically added to ensure no network degradation.

Cardinus security policies are as follows:

- Maximum 15 users have access to each server (excluding service provider).
- Passwords must have minimum length and must meet complexity requirements.
- OS and software patches are applied by Rackspace on a monthly basis. Patches are normally applied at weekends unless the security threat warrants the patch being applied immediately (overnight). Application hot-fixes and patches are fully tested in an office environment before being authorised through the change management process, and applied to production systems.

Protection against viruses

All Cardinus servers are protected by Armor Anywhere endpoint protection software with automatic updates every 8 hours.

Protecting data from accidental or malicious loss

Multiple levels of protection are provided:

- Perimeter and inter-segment firewalls separate Internet-facing traffic in the demilitarized zone (DMZ segment) from the back-end databases and services (INSIDE segment)
- All traffic routed via Cloudflare, containing a Web Application Firewall (WAF) and Distributed Denial-Of-Service (DDoS) mitigation, monitored by Cloudflare 24x7x365
- An Intrusion Prevention System (IPS), using Armor Anywhere managed and monitored by Rackspace 24x7x365
- Centralised Security Information and Event Management (SIEM) log collection, also monitored by Rackspace 24x7x365
- Availability and health monitoring from HetrixTools, sending alerts 24x7x365 when capacity thresholds are met (disk space, CPU, memory, etc.)
- All infrastructure is fully resilient (at least N+1)
- Each customer has their own database on a shared SQL server cluster
- All data exchanged between a client/browser and Cardinus production servers is encrypted in transit (HTTPS, TLS1.2+, SHA256) and at rest (AES-256) using DELL EMC Data at Rest Encryption (D@RE).
- Daily backups (encrypted, and held offsite with 12-week retention)

Availability and quality of service

The Cardinus 'hosted' service is provided via a single outsourced service provider covered by a Service Level Agreement. These primarily cover the level of availability of the service. The availability and responsiveness of the service is continually monitored from multiple locations around the world using an external service. Monitoring provides:

- Detailed breakdowns for HTML page include DNS resolution time, TCP connect time, time to first byte, content download time, and redirect times
- Instant notification of website errors via email and phone notifications
- TCP trace routes on network failures

5.4 Business continuity

Cardinus has a comprehensive business continuity program in place. The plan covers loss of production server facilities, office environment and all other assets including people. The Business Continuity plan is under constant review and is updated at least annually. Mock disaster recovery scenarios are held at least annually to ensure our plans will work should an event occur.

5.5 Measures in place to ensure data is secure

Hosting environment:
This Technical Overview outlines technical measures at the server/data centre level.

Application security:
a) Password protection (see below)
b) Application level security (code designed to prevent OWASP vulnerabilities)

Procedures/documentation:
Cardinus have developed an ISMS accredited to ISO27001. This creates a framework for controlling access to server, system changes, incident management etc. Documents include Standard Operating Procedures (SOPs), policy documents and ISMS templates. Documents are available on request.

5.6 Restricting access to our customers data

Within the application, the following password protection options can be configured within PACE according to customer requirements:

- Minimum password length
- Alpha characters required
- Number characters required
- Symbol characters required
- Upper and lower case required
- Password history (so that passwords cannot be re-used)
- Maximum password age
- Lockout threshold for failed logins

Access to the production servers is restricted to authorised and vetted support staff from Cardinus and Rackspace.

A log management service from Armor Anywhere/Rackspace ensure protection and monitoring of the network infrastructure and devices, and quality of data required for any required forensic evidence.

Products are penetration/web application tested at least quarterly by Appcheck, designed and built by CREST and CHECK accredited penetration testers.

6.0 Data protection and privacy

Unless otherwise agreed, the customer is the “data controller” and Cardinus the “data processor”. Our registration number on the Information Commissioner’s Office register is Z658762X. Cardinus has self-certified to the EU-U.S. Privacy Shield framework”, however in light of the Schrems II decision by the Court of Justice of the European Union (CJEU), Cardinus now also uses Standard Contractual Clauses (SCCs) with individual clients when requested to do so and where it is deemed appropriate.
A copy of our privacy policy is available from http://www.cardinus.com/privacy.

During the training course login process Cardinus can display a privacy statement to the user. This is fully configurable to meet client requirements (provided that it does not conflict with Cardinus data protection/privacy policies).

Cardinus takes all reasonable steps to protect data (see section above) and has insurance in place as appropriate for a software provider.

It is the customer's responsibility alone to manage and process data accumulated on the Training Server including accessing and reviewing the results of exams, tests or assessments performed by customer's staff.

7.0 System and operating requirements

7.1 System requirements - client

Browsers supported
All access to the software is via a standard web browser, which must have JavaScript enabled.

Courses
Browsers supported are: Edge, Firefox, Chrome and Safari, which must have JavaScript enabled.

PACE
Browsers supported are: Edge, Firefox, Chrome. All access to the software is via a standard web browser, which must have JavaScript enabled.

Authoring tool and programme engine
Browsers supported are: Edge, Firefox, Chrome and Safari.

Hardware
There is no official 'minimum specification' for client PCs. Any hardware capable of running one of the supported browsers above should be acceptable.
The PC screen resolution should ideally be set at 1024x768 or above.

Mobile devices
Supported devices are 10” tablets with a minimum screen resolution of 1024 x 768 running the latest versions of Safari or Chrome.

8.0 Support and maintenance

8.1 Acceptance/upgrade testing

All development is carefully tested for backward compatibility. The development and testing teams complete detailed testing in the final stages of development including a period of OAT.
An evaluation system can be set up on the Cardinus production server. Any content changes could be viewed on this test environment prior to live implementation.

8.2 Support and service levels

Technical support information is provided by telephone and email as part of our standard Annual Support License. Please note that annual support applies to one nominated contact or team in one location for one PC or server and is effective from date of invoice. If a course has been customized there may be an additional fee for adding the customized information to each new version.

Reporting mechanism

Cardinus courses have a support feature which enables a course user to contact the administrator(s) with issues. This process will automatically send significant details to a nominated email address within the organization, relating to (amongst other details) the browser version, operating system and page within the course that may be causing the issue. The issue can then be escalated to Cardinus if required by telephone or email.

If an issue requires updated software to resolve it, a discussion process will take place to agree on a timescale. Development of a patch will then commence. A period of testing will follow which may include a phase of UAT. This internal testing followed by UAT will help ensure no further errors are introduced during the patch development.

Project and performance management

Project management plan:
At the beginning of a typical project, Cardinus will work with each customer to prepare a written plan. This will typically include:

- Project Team
- Project Controls
- Assumptions
- Project Deliverables
- Schedules
- Performance/Acceptance Criteria
- Communication Plan

At key agreed points in the plan, senior management review performance against the performance/acceptance criteria and intervene as appropriate. Formal reporting of performance levels may also be agreed with the customer.

A number of metrics are used to monitor general levels of service and specific service levels contained in client agreements. These include:

- Feedback forms from training sessions
- Hosted service monitoring
- Daily vulnerability tests

These metrics are collected monthly.

Support availability

First line support is available Monday to Friday excluding UK public holidays as follows:
09:00 – 17:30 (UK)
04:00 – 17:00 EST (USA)

Most requests are dealt with immediately with 95% being responded to within 1 hour. Issues that cannot be resolved immediately are escalated for further analysis before being referred to the development team if necessary. If the issue requires development work or configuration then a schedule for completion is agreed with the customer.

8.3 Help and documentation

The documentation supplied is comprehensive and readable. Cardinus supplies documentation for technical implementers, risk-assessors and PACE Administrators.
The documentation includes:

- PACE help files
- Product release notes covering recent bug fixes and outstanding issues

8.4 Escrow

Escrow is available as an optional service. The source code will be lodged in escrow subject to the necessary fees being paid by the client.

8.5 *Change control policy*

- If either the customer or Cardinus sees a need to make a change to the Specification, the Program, or the Support and Maintenance Service, such change shall be made in accordance with the requirements of this Schedule.
- Either party may recommend or request a Change to the other.
- Changes shall be requested and/or managed using Cardinus Change Control Form.
- Unless and until a Change is made in accordance with this Change Control Policy, Cardinus shall, unless otherwise agreed, continue to carry out the Services in accordance with the Contract as if the recommendation or request for a Change had not been made.
- The customer and Cardinus shall each appoint their own authorized person to approve or reject any recommendation or request for a Change and shall notify the other in writing of the identity of the authorized person appointed to act on their behalf hereunder.

- The party requesting or recommending a Change shall submit to the other in writing the request or recommendation with full details of the proposed Change and shall in such submission specify:
    i. a description of the proposed Change in sufficient detail as to enable the other party to analyse the impact of the Change on the Services in terms of the time, cost and other effects;
    ii. the increased cost, if any, likely to be incurred in making or as a consequence of the Change;
    iii. a timetable for the implementation of the Change;
    iv. the impact, if any, on the Specification, the Program, the Support and Maintenance Service, the Contract Price and any other effect on this Agreement or the matters referred to in this Agreement or any of them.

- If the proposed Change is rejected the notification shall contain an explanation of the reasons for the rejection.

- If the proposed Change is accepted by the receiving party the decision shall be notified and the Change shall on such notification be deemed to have been made and shall forthwith be implemented by the parties in accordance with the timetable for implementation.

- The sum stated for the Change shall be added to the Contract Price and shall be paid by the customer in accordance with standard payment terms agreed.

Version	Date	Author	Detail	Approved by	Approved Date
0.5	12th Oct 2015	Stephen King	Initial draft document– For Cardinus's new product range (replacing previous technical overview document)	Barbara Snape	29th April 2015
1.0	4th Nov 2015	Barbara Snape	First release - NG	Barbara Snape	10th February 2016
1.1	5th Jan 2017	Barbara Snape	Introduction of further features	David Tibbals	4/1/2019
1.2	19th Jun 2017	Barbara Snape	Support desk updates	David Tibbals	5/6/2020
1.3	18th Jul 2019	Matt Champ	Updated supported browsers	David Tibbals	20/7/2019
1.3	8th Jul 2020	Matt Champ & Jonathan Coates	Annual Review	David Tibbals	8/7/2020
1.4	2nd Feb 2022	Jonathan Coates	Update to reflect current infrastructure	Matt Champ	2/2/2022
1.4	8th March 2023	Jonathan Coates	Annual Review and changes to infrastructure	David Tibbals	9/3/2023
1.4	26th May 2023	Jonathan Coates	Annual Review	David Tibbals	26/5/2023
1.5	09th May 2024	Matt Champ	Annual Review & Update	David Tibbals	09/05/2024
1.6	01st May 2025	Matt Chamo	Annual Review & Update	David Tibbals	02/05/2025