Secure Development Process

STATEMENT | CATALYST IT

1800 595 252 | info@catalyst-au.net | catalyst-au.net

About the Catalyst IT Group

We are world leading open source and e-learning specialists.

Catalyst IT is a multi-region IT services group that provides enterprise-level technical support for open source software. Open source means freedom from licence fees, freedom from vendor lock-in and, most importantly, freedom to innovate.

Experts in open source development, cloud migration and cloud performance optimisation, the Group was first established in New Zealand in 1997. We now have locations across Australia, Europe, UK and Canada.

Together, we are able to provide 24/7 'Follow-the-sun' support to our clients.

With 350 specialists globally, including 200 Totara, Moodle, Mahara, Laravel and React developers, we are well positioned to provide custom solutions and service to enterprise level and growing organisations.

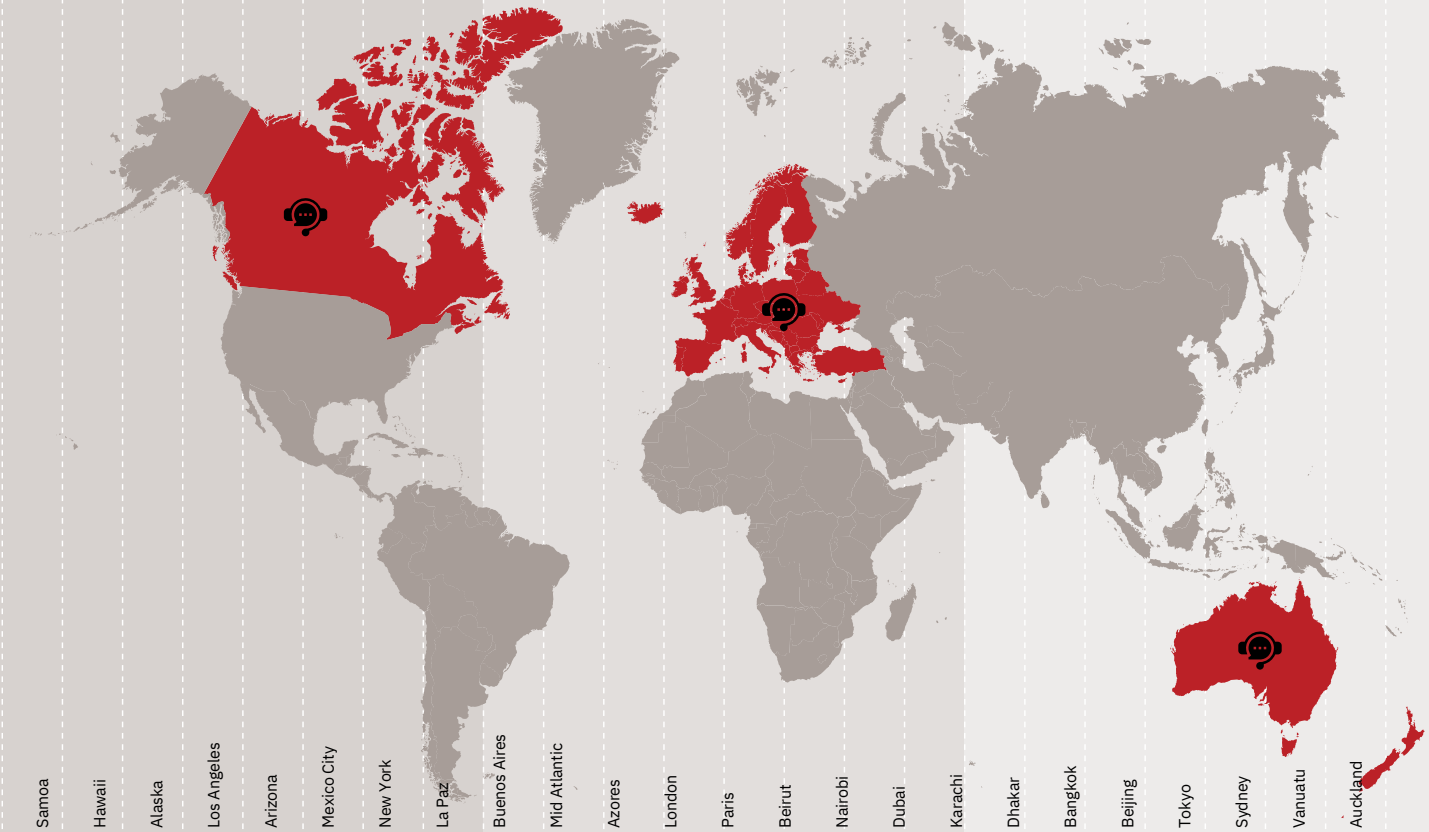
Our clients include major universities, colleges and other higher education providers. As well as Government and major organisations in the health, not-for-profit and commercial sectors.

Committed to open source and the freedom that it gives our clients, we have long-established partnerships with open source technology companies and are Premium Moodle Certified Partner since 2004, Premium Drupal Supporting Partner since 2008 and Platinum Totara Learning Partner since 2010. In support of our cloud services, we are also a certified Amazon Web Services Consulting Partner.

Our contributions to the Moodle and the broader open source community have been recognised with multiple awards over the last few years.

Catalyst IT Australia are **ISO27001** certified.

Catalyst IT Follow The Sun support model – providing 24/7 live response capability



Why Trust Catalyst IT with your Development Process

AGILE FRAMEWORK | QUALITY ASSURANCE | DESIGN AND DEPLYOMENT | SECURE CODE REVIEW | IMPLEMENTATION AND TESTING

SCRUM AGILE FRAMEWORK

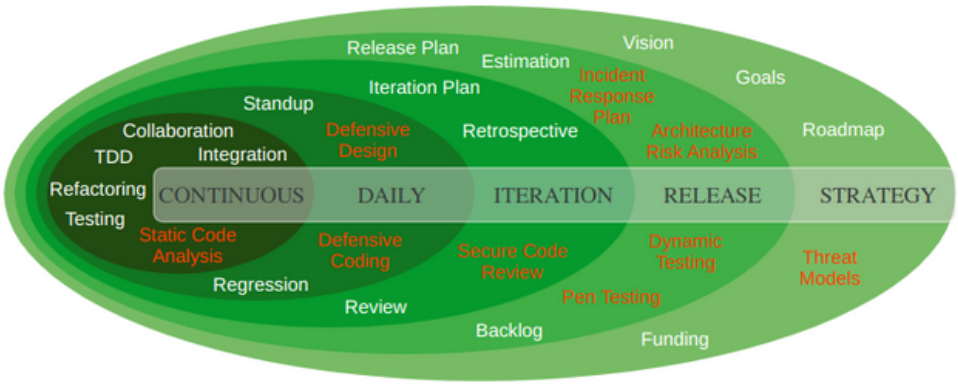
Catalyst IT Australia software development uses the Scrum Agile development framework. Scrum is an agile project management framework used primarily for software development projects with the goal of delivering new software functionality every 2-4 weeks.

Development is broken down into short Sprints, which start with a Planning Meeting and then include a daily stand-up where each member of the Scrum gets a chance to discuss their progress, achievements on the previous day and any blockers which impede further progress.

This gives a chance for the Scrum Master to ensure that assistance is rendered in relieving these blockers and thus development is streamlined. At the end of the the sprint there is a review and retrospective where the work is reviewed and assessed so that suggestions for future improvement can be made. This ensures that the process becomes more effective over time.

THE SCRUM APPROACH

Scrum is one of the approaches that influenced the Agile Manifesto, which articulates a set of values and principles to guide decisions on how to develop higher-quality software faster. Viewed as a diagram, the Catalyst Secure Development Process can be illustrated as shown (right).



Security is viewed as an integral part of each phase of the process.

Security is a priority during inital planning and is reassessed during all parts of the recurring cycles shown here. Security and operations engineers pair and work with(in) the development teams to deliver secure applications, and provide ongoing training/mentoring on evolving secure development strategies.

SECURITY IN CODE REVIEW

Security is an important part of our code review process. Experienced developers, who are extremely well versed in the OWASP secure coding practices, review all code and point out any potential security issues. Our use of Git (as described in section 3 below) ensures that all code is reviewed and a history of all changes is maintained. Catalyst maintains its own repositories for source code and its own instance of

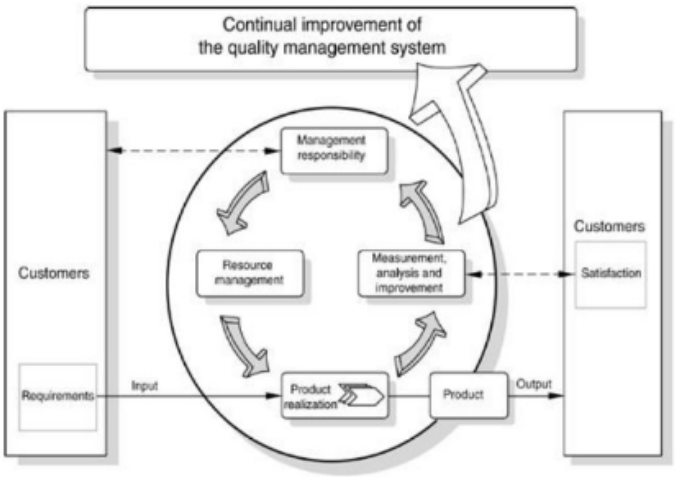
Gitlab, thereby ensuring that developers only access trusted versions of the resources (such as libraries) needed in their work.

Testing is undertaken throughout the development cycle, using tools such as Unit tests and Jenkins. Our Continuous Integration/ Continuous Deployment (CI/CD) system, GoCD, ensures that all the latest security releases and patches are automatically applied to all code in the testing environments, so that they too can be tested before deployments into Production systems.

Additional tools such as SonarQube (for static code analysis), Docker and Kubernetes (for containerised deployment) and Puppet (for applying updates, firewalls, virus scanners and configuration settings) are used to ensure that all aspects of each system are as secure as possible, without relying purely on humans manually applying security.

QUALITY ASSURANCE AND SECURITY

Catalyst is accredited with ISO9001:2015 compliance. Quality is managed throughout the company and throughout the lifecycle of all projects. It is built into our agile approach to software engineering and project implementation, as shown in the diagram below.



OUR QA PROGRAM

Our QA program manages quality at all stages of the project. Catalyst's workflows are structured to ensure a continual review process, utilising best practice to ensure that our work is state-of-the-art and incorporates the best possible security practices. The methods of ensuring quality and security vary according to each stage of the project, and are each matched to ensure best practice throughout.

Stages of a project include:

- Analysis of client business requirements;
- Specification of those Requirements in terms of the system architecture
- Design and development of the system;
- Implementation;
- Testing and Integration with other systems, as required; and finally
- Ongoing Operation and Maintenance once the system is deployed.

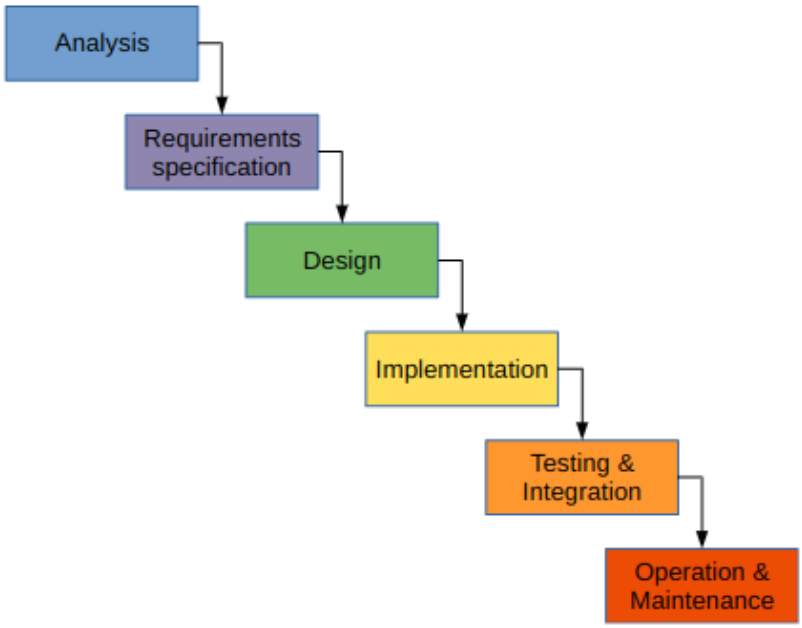
Catalyst's QA management operates throughout all of these phases to ensure that all the systems we develop are of optimal quality and security throughout the life of the system.

Catalyst IT Australia uses an issue management system called the Work Request Management System (WRMS), through which all requests for changes (either internal to Catalyst or externally, from clients) are processed. The WRMS contains settings which allow one to assign a significance and urgency rating to each request, ensuring that changes are triaged and processed according to these factors.

EFFICIENT SUPPORT SYSTEM

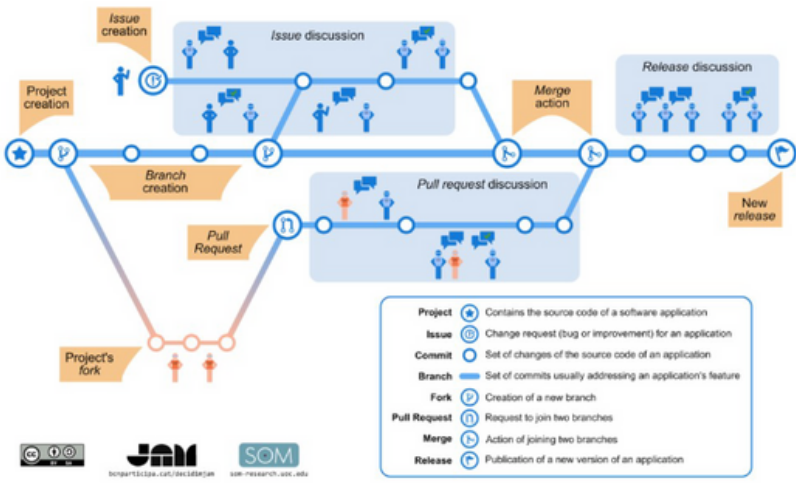
The WRMS provides a record of the process undertaken for each request, clarifying exactly which steps were taken, when and by whom. Thus, all changes are initiated when a work request is created detailing the nature of the required change, reasons for the change, the urgency with which the change is required and the significance of the requirement for this change.

Catalyst personnel (and others, including certain client contacts) are allocated to these work requests as required. The work request is assigned to one or more personnel for attention, whilst others whose input may be required can be subscribed. All updates to the work request are notified to all subscribers via email, ensuring that all stakeholders are informed promptly of all updates to the issue.



DESIGN AND DEVELOPMENT

Catalyst implements an agile workflow in the development and configuration of software. Tasks are allocated to team members with a daily standup check-in. Developers are allocated sections of code. Catalyst maintains a local Git environment for managing code (see diagram below).



Git is a distributed version-control system for tracking changes in source code during software development.

By using Git, a history of all changes is maintained and the changes can be linked back to the work request.

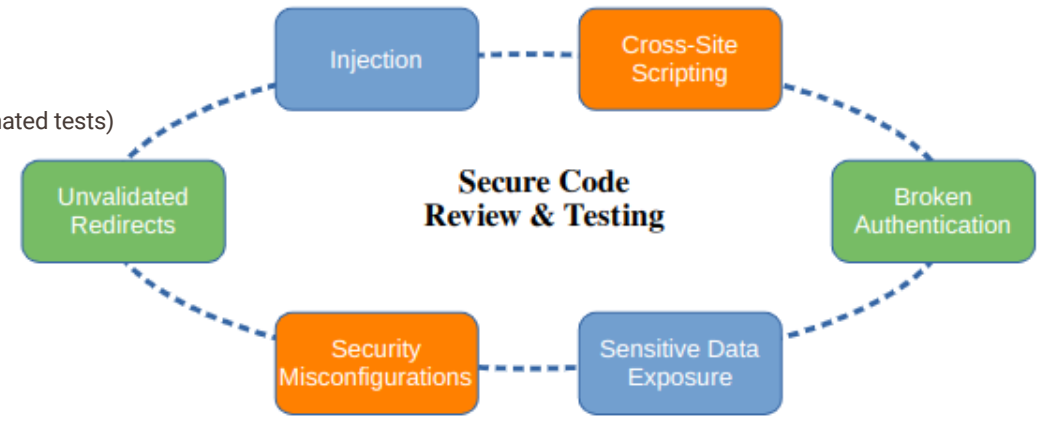
Code is regularly committed to a task-specific local Git branch, where it is reviewed by an experienced senior developer to ensure that it is both functionally correct as well as conforming to the coding standards for the product, before being integrated into the main code base. Thus security is reviewed as soon as code is written.

SECURE CODE REVIEW

Code review is a natural part of Catalyst IT's software development cycle, with the secure code review as part of that.

A code review checklist contains:

- [✓] Syntax
- [✓] Output
- [✓] Language
- [✓] Databases
- [✓] Testing (instructions and automated tests)
- [✓] Security
- [✓] Privacy
- [✓] Performing
- [✓] Clustering
- [✓] Documentation
- [✓] Git
- [✓] Third party code
- [✓] Sanity check
- [✓] Icons



Whilst throughout this document we focus on the specific security aspects highlighted in orange (above, left), it is clear that, for example, the iterative code review process before a merge request is accepted for integration has intrinsic security aspects to it.

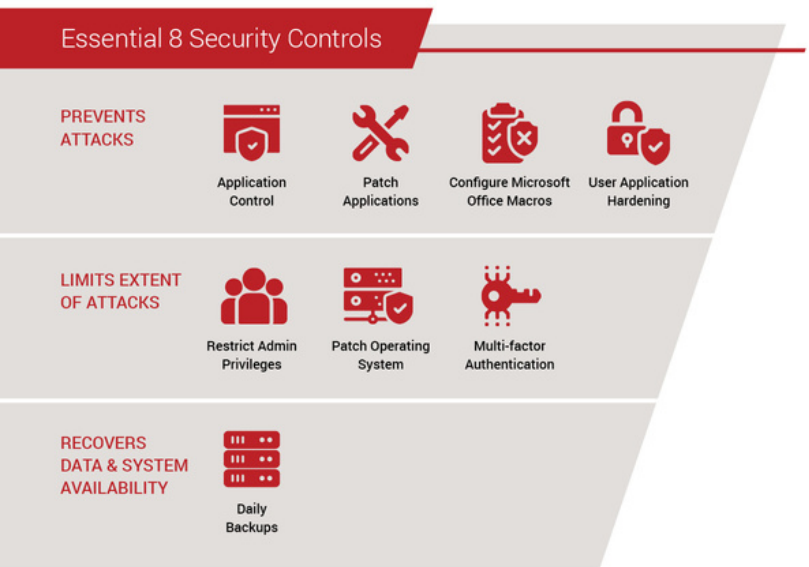
IMPLEMENTATION AND TESTING

Agile software engineering uses unit testing from the start of the development process. Unit testing is ongoing and occurs every time code is committed. As soon as system architecture has been developed, it is tested for stability, security and performance. As soon as the system has reached a sufficient stage of completion, the architecture is implemented by being deployed in the Staging environment.

Once in the Staging environment, the system is prepared for User Acceptance Testing (UAT). Clients are then able to start learning to use and test the system and provide their own feedback on the system and its quality. At this stage, Catalyst's change management policy is used to manage requested changes. Clients or staff testing the system in the Staging environment can use the WRMS to request changes or report issues with the system. These issues are then triaged for resolution

When changes require a change in code, the work request is assigned to a developer who writes the new code (or updates existing code), tests the code with local unit tests and commits the changes code to a task specific local Git branch. Usually changes are pushed to the Staging area, where they can also be reviewed by the client for further comments.

Security is inherent within this testing regime, ensuring that the system is fully tested and of the best possible quality before deployment.



DEPLOYMENT

Changes are deployed through Catalyst's Continuous Integration/ Continuous Deployment (CI/CD) system on GoCD.

There is a scheduled approach to deployment and there are several approval steps along the way. GoCD deploys to both the Staging and Production environments. Production environment deployment only occurs after unit testing and UAT in the Staging environment. Until deployed through CI, the changes are not finalised. By the time the code is finally released into Production it has been thoroughly tested and thus can be deployed all at once. The code is thus released with inherent change control – all deployed code has been through a process of review and testing, for which there is a history.

The latest security releases and patches are automatically applied to all code in the testing environments by GoCD, so that they too can be tested before deployments into Production systems. This ensures that all systems have the latest security releases and patches included as soon as possible. We often patch potential issues before official release of the notifications or CVEs, having received advance notice from our software partners.

IN SUMMARY

For Catalyst IT Australia, security is inherent within every aspect of our development and deployment process. We use best practice standards and methodologies in the design and implementation of all our systems to provide optimal security for both data and applications.

We recognise that the threat environment on the public Internet is constantly changing and that systems open to the public internet should ideally be regarded as compromised unless proven otherwise.

Therefore, we take a proactive approach to managing cyber security by assuming that a default position is that a system online be regarded as compromised and then managed to reduce the level of security risk to an acceptable residual level.

The fact that we take the issue of security very seriously, is reflected by the range of enterprise level clients who use our systems from major higher education providers to Government and not-for-profit organisations.

Our Clients

Catalyst IT Australia has significant experience implementing secure systems with clients in the following sectors:

Higher Education

- Monash University
- La Trobe University
- Macquarie University
- Central Queensland University (CQU)
- Federation University
- Australian National University

Colleges, Private Education Providers & Education Authorities

- Navitas, Global Education Provider
- Kaplan
- New South Wales Department of Education
- Victorian Department of Education

State and Federal Government

- Australian Electoral Commission
- Australian Department of Defence
- New South Wales Health
- Victoria Police
- Qld Shared Services

Corporate & Commercial

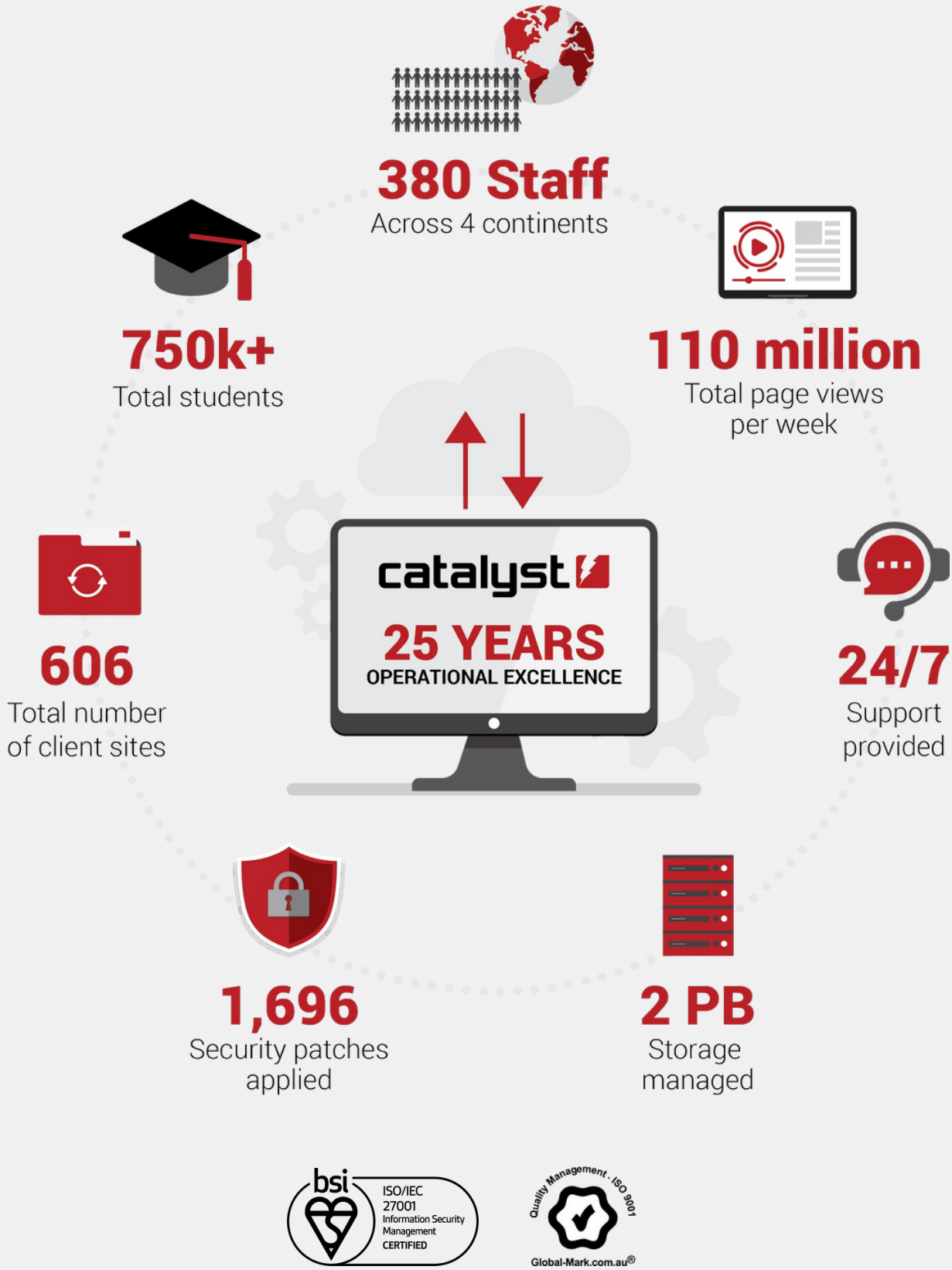
- Kmart Australia
- QBE Insurance
- PwC Australia
- The Tax Institute, Australia
- Victorian Barristers Association

Open2Study

- Moodle MOOC repository accessed by 1m+ students as of 2019

Please refer to the attached project sheets for individual case studies.

More reasons to trust Catalyst IT with your next project



Contact us

For more information about our projects and capabilities please contact:

Justin Beall

Business Development Manager

Catalyst IT Australia
Email: justinbeall@catalyst-au.net
Phone: 0488 218 363

24/7 Support

Catalyst IT is a multi-region IT services group that provides enterprise level technical support for open source software.

With a heritage of e-learning solutions, including Moodle and Totara, we are experts in open source development, systems integration, cloud migration and cloud performance optimisation. First established in New Zealand in 1997, we now have presence across Australia, Europe, UK and Canada.

Australia
W: catalyst-au.net
E: info@catalyst-au.net
T: +61 1800 595 252

New Zealand
W: catalyst.net.nz
E: info@catalyst.net.nz
T: +64 (0) 4 499 2267

UK
W: catalyst-eu.net
E: info@catalyst-eu.net
T: +44 (0) 1273 929 450

Canada
W: catalyst-ca.net
E: info@catalyst-ca.net
T: +1 416 216 4638