Queensland Department of Education and Training

OneSchool – Technology Review

16 October 2015

Deloitte.

Deloitte Touche Tohmatsu
ABN 74 490 121 060

Riverside Centre
Level 25
123 Eagle Street
Brisbane QLD 4000
GPO Box 1463
Brisbane QLD 4001 Australia

Tel: +61 7 3308 7000
Fax: +61 7 3308 7001

Hon Kate Jones
Minister for Education and Minister for Tourism, Major Events,
Small Business and the Commonwealth Games
Level 22
Education House
30 Mary Street
Brisbane 4000

16 October 2015

Dear Minister

Re: Review of the Student Protection Reporting module in OneSchool

I refer to our appointment from 3 August 2015, in which you have requested Deloitte Touche Tohmatsu (**Deloitte**) to assist the Department of Education and Training (**DET**) with a review of the Student Protection Reporting Module in OneSchool.

I am pleased to provide you with our report. If you have any questions please do not hesitate to contact me on 3308 7065.

Thank you for the opportunity to work with the Department of Education and Training on this important engagement.

Yours sincerely

RBradley

Ray Bradley
Partner, Technology Advisory
Deloitte Touche Tohmatsu

Contents

1 Executive Summary 3

1.1 Background 3

1.2 Scope and Objectives 3

1.3 OneSchool Technology Review Context 4

1.4 OneSchool Technology Review Summary 4

2 Summary of Findings and Recommendations 9

3 Background 13

3.1 OneSchool – Queensland online school management system 13

3.2 Queensland child protection regime 14

3.3 Child Protection Legislation 15

3.4 Implementation of the SPM into OneSchool - October 2013 and January 2015 16

4 OneSchool Technology Assessment 18

4.1 Introduction 18

4.2 Technology Assessment Structure 18

4.3 Summary of Recommendations 18

5 OneSchool IT Operations Review 23

5.2 Current State Analysis 26

5.3 Findings 44

6 OneSchool Technical Solution Review 53

6.1 Introduction 53

6.2 Objectives 54

6.3 Business Requirements 54

6.4 Application Functionality Review 57

6.5 Application Architecture and Infrastructure Review 60

7 Limitation of our work 75

Appendix A. Operations Review Hypotheses and Suggested Initiatives 76

Appendix B: Operations Review Document List 84

Appendix C: Operations Review Meeting List 86

Appendix D: Development and Testing Tools 87

Appendix E. Technical Review Document List 89

Appendix F. Technical Review Interview List 90

Appendix G. Detailed Code Review 91

Appendix H. Additional Suggestions for Code Structure Enhancement 99

Appendix I: Glossary of terms 100

This report has been prepared exclusively for the Department of Education & Training as per the purposes set out in the contract dated 17 August 2015. This report should be read in conjunction with the terms and conditions agreed in the Professional Services Panel Arrangement (QGCPO 878-13). This report is not intended to and should not be used or relied upon by anyone else and we accept no duty of care to any other person or entity.

1 Executive Summary

1.1 Background

Deloitte was engaged by the Director General of DET to review, assess and make recommendations relating to the technical design and implementation of the Student Protection Module (SPM) and the wider software and technology delivery capability of the OneSchool program within DET. This advisory work was conducted in parallel to the Deloitte investigation into the OneSchool Student Protection Module (SPM) incident.

1.2 Scope and Objectives

The scope and objectives for the advisory project are outlined below.

a. Review all development and changes made to the OneSchool system which relate to the three streams of Student Protection Reporting to:
   - Queensland Police
   - Department of Communities and joint Queensland Police
   - Department of Communities.

b. With specific regard to the delivery of email reporting, review:
   - the operation of the Departments email delivery system, including IT Security and firewall considerations, email filtering (e.g. spam/virus protection, etc.) and the interaction of this system with the Whole of Government email gateway and delivery system hosted at CITEC; and
   - the Department's processes and actions for monitoring and responding to Non-Delivery-Reports (NDR) and Failure-To-Send (FTS) notifications.

c. With regard to (a) and (b) the work is to include a full review back to the system go-live date of the 25 September 2013 release

d. Review 'other category of reports' to determine if OneSchool is allowing all reports entered into the system to reach the intended recipient (police, child safety and the school)

e. Provide recommendations to strengthen the notification and reporting to external agencies (QPS, Child Safety) and options for improving the confirmation and reporting from external agencies back to School Principals and the Department

f. Review the Department's application testing and quality assurance framework for all software releases

g. Review the process for business requirements gathering and the creation of software code against industry better practice

h. Review the Department's approval processes for IT system upgrades including change management and software release management

i. Provide recommendations for strengthening procedures and practices for IT system development and operations.

1.3 OneSchool Technology Review Context

OneSchool is a large application consisting of several million lines of software code and a number of functional modules which support thousands of distinct users and stakeholder groups. The application has evolved extensively since the first deployment in 2007, with two major releases prior to 2011 and regular large quarterly releases since then. There is a large variety of different stakeholders and users involved with the OneSchool application which leads to significant complexity when changes to the application need to be made.

According to the OneSchool stakeholders interviewed, the current OneSchool Operating Model used to develop, support and operate the OneSchool Application has historically been successful in delivering expected outcomes to the business.

The OneSchool Application transitioned to '*Business as Usual'* status in 2011. It is governed by the OneSchool Operating Model, which outlines the operational processes and procedures for implementing changes to the system.

1.4 OneSchool Technology Review Summary

Deloitte were engaged to review the design and implementation of the SPM and to review the wider software and technology delivery capability of the OneSchool program within DET. Note, the Deloitte technology review focussed specifically on the SPM within OneSchool, and did not undertake to consider the broader aspects of other ICT projects which are under management by DET Information & Technologies Branch (IT Branch).

The review was performed with the aim of identifying improvements in the following (where necessary):

1. The procedures and practices followed within OneSchool in order to develop and operate ICT systems
2. The OneSchool solution supporting the delivery of SPRs and notifications to external agencies.

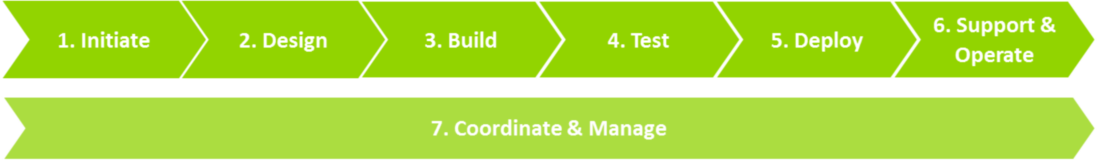
In order to address these objectives, the following aspects of OneSchool were examined and assessed:

Area	Detail
OneSchool Operational aspects	The processes, governance and organisational structure implemented by the OneSchool program and DET to gather requirements, design, build, test, deploy, manage, approve and quality assure the release of software functionality.
OneSchool Technical aspects	The OneSchool SPM technical design, software code and the underpinning ICT infrastructure supporting the email delivery of Student Protection Reports.

Approach to Review the Operational aspects of OneSchool

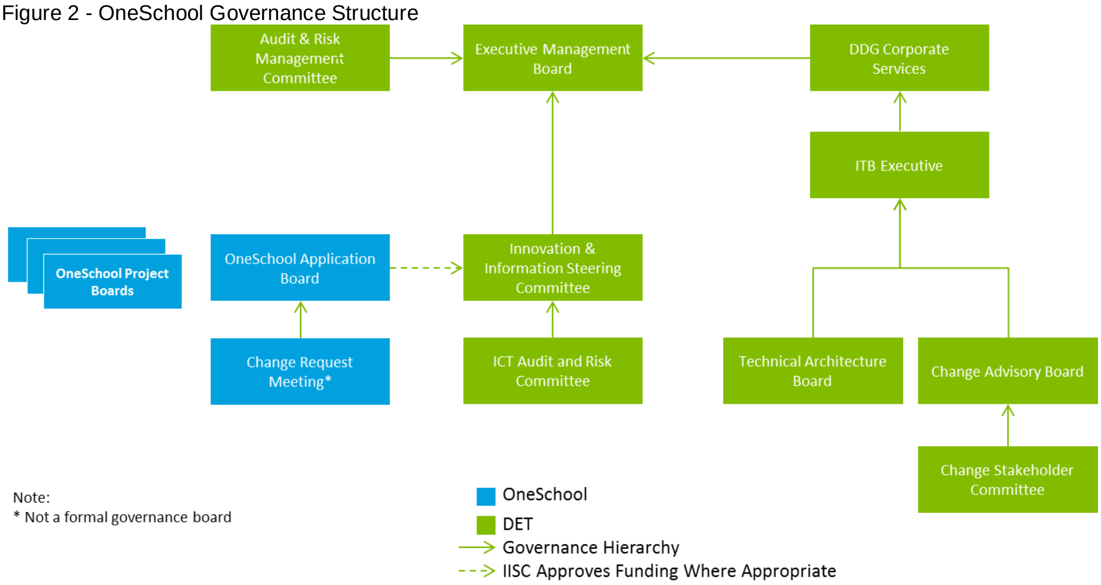
To perform the review, a number of interviews and documentation reviews were conducted in order to gain an understanding of the environment within which the OneSchool team builds, operates and supports the software application. To structure the review, the analysis was structured and reported against an industry recognised SDLC as shown below.

Figure 1 – Summarised SDLC Steps



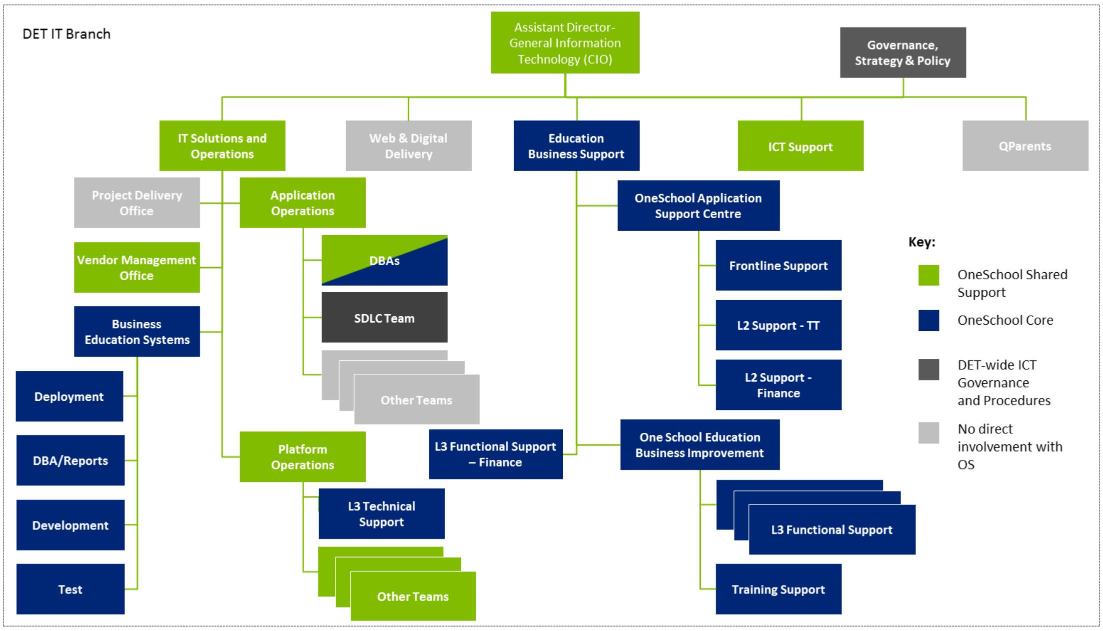
A review of the governance and decision making processes which affect operation and development of OneSchool was performed. A number of governance boards make decisions that affect OneSchool, the most relevant of which is the OneSchool Application Board. The OneSchool governance structure and decision making environment is depicted in the diagram below.

Figure 2 - OneSchool Governance Structure


Audit & Risk Management Committee
Executive Management Board
DDG Corporate Services
ITB Executive
OneSchool Project Boards
OneSchool Application Board
Innovation & Information Steering Committee
Change Request Meeting*
ICT Audit and Risk Committee
Technical Architecture Board
Change Advisory Board
Change Stakeholder Committee
Note:
* Not a formal governance board
OneSchool
DET
Governance Hierarchy
IISC Approves Funding Where Appropriate

A review of the specific development and operations teams within the OneSchool program that are directly involved in the day to day running and changes to the OneSchool application was completed. These are shown in the following diagram.

Figure 3 - OneSchool Development and Operational Teams



Approach to Review of Technical aspects of OneSchool

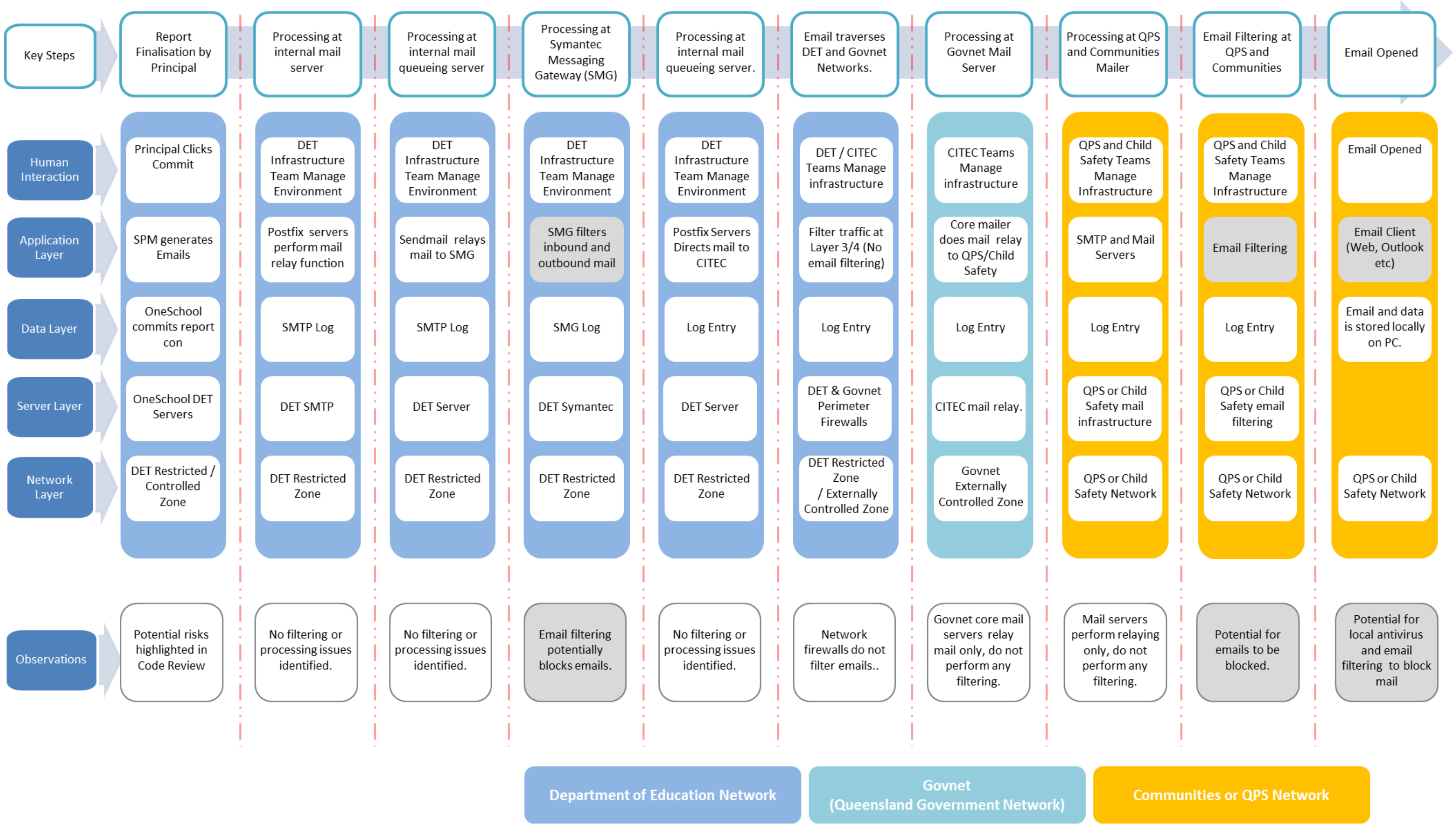
An assessment of the OneSchool SPM technical design, software code functionality and underpinning ICT infrastructure supporting the email delivery of SPR's was completed.

The diagram on the following page outlines the various components of ICT infrastructure involved in the transmission of an email message from the OneSchool application to either DCCSDS or QPS. The diagram highlights a number of areas within the wider ICT environment, outside of DET's control, which have the potential to contribute to the unreliability of sending SPRs via email. Deloitte undertook a review of the technical considerations of the OneSchool supporting ICT infrastructure and services.

In addition to the review of the SPM technical design and supporting ICT infrastructure, Deloitte undertook a review of specific aspects of the implementation of the SPM solution. This was undertaken in order to verify that the current application met the original intended core requirements of the Child Safety team within State School operations.

To complete this, Deloitte worked with the Child Safety Business stakeholders to agree the intended legislative and other core business functionality that should be provided by the SPM. A comparison of these requirements against the software code was undertaken in order to identify if any gaps exist in implemented functionality that could lead to a potential service failure in the future.

Figure 4 - Summary of ICT Email environment for the transmission of an email message from the OneSchool application to either DCCSDS or QPS



Key Steps	Report Finalisation by Principal	Processing at internal mail server	Processing at internal mail queueing server	Processing at Symantec Messaging Gateway (SMG)	Processing at internal mail queueing server.	Email traverses DET and Govnet Networks.	Processing at Govnet Mail Server	Processing at QPS and Communities Mailer	Email Filtering at QPS and Communities	Email Opened
Human Interaction	Principal Clicks Commit	DET Infrastructure Team Manage Environment	DET Infrastructure Team Manage Environment	DET Infrastructure Team Manage Environment	DET Infrastructure Team Manage Environment	DET / CITEC Teams Manage infrastructure	CITEC Teams Manage infrastructure	QPS and Child Safety Teams Manage Infrastructure	QPS and Child Safety Teams Manage Infrastructure	Email Opened
Application Layer	SPM generates Emails	Postfix servers perform mail relay function	Sendmail relays mail to SMG	SMG filters inbound and outbound mail	Postfix Servers Directs mail to CITEC	Filter traffic at Layer 3/4 (No email filtering)	Core mailer does mail relay to QPS/Child Safety	SMTP and Mail Servers	Email Filtering	Email Client (Web, Outlook etc)
Data Layer	OneSchool commits report con	SMTP Log	SMTP Log	SMG Log	Log Entry	Log Entry	Log Entry	Log Entry	Log Entry	Email and data is stored locally on PC.
Server Layer	OneSchool DET Servers	DET SMTP	DET Server	DET Symantec	DET Server	DET & Govnet Perimeter Firewalls	CITEC mail relay.	QPS or Child Safety mail infrastructure	QPS or Child Safety email filtering	
Network Layer	DET Restricted / Controlled Zone	DET Restricted Zone	DET Restricted Zone	DET Restricted Zone	DET Restricted Zone	DET Restricted Zone / Externally Controlled Zone	Govnet Externally Controlled Zone	QPS or Child Safety Network	QPS or Child Safety Network	QPS or Child Safety Network
Observations	Potential risks highlighted in Code Review	No filtering or processing issues identified.	No filtering or processing issues identified.	Email filtering potentially blocks emails.	No filtering or processing issues identified.	Network firewalls do not filter emails..	Govnet core mail servers relay mail only, do not perform any filtering.	Mail servers perform relaying only, do not perform any filtering.	Potential for emails to be blocked.	Potential for local antivirus and email filtering to block mail

Department of Education Network

Govnet (Queensland Government Network)

Communities or QPS Network

1.4.1 Limitations of this Work

When undertaking an advisory review of this nature, Deloitte would seek to collaborate with client (DET) technical teams to validate our detailed findings and test hypotheses with senior client stakeholders throughout the engagement.

In this instance, and specifically due to our completion of a parallel and independent incident investigation, it was not possible to validate our detailed findings and recommendations with senior DET stakeholders. We therefore completed this advisory review independent of DET input and without the opportunity to validate all information. This review has been based on interviews, workshops and available documentation.

1.4.2 Intended Use of Finding and Recommendations & Next Steps

A number of detailed observations, findings and recommendations are outlined within this report. These findings and recommendations are for the consideration of DET leadership who would evaluate whether all these are aligned for the needs of the Department.

The proposed next steps to validate and progress these findings and recommendations are therefore as follows:

1. Consider each recommendation provided within this report in order to assess the applicability to OneSchool and DET
2. DET should form their own view of the priority of each recommendation and seek approval for any agreed remediation actions from appropriate DET leadership
3. DET should then agree a set of initiatives to address the implementation of the priority recommendations. It is expected that DET will develop an implementation plan that is then approved and overseen by appropriate DET leadership.

2 Summary of Findings and Recommendations

The key findings were derived from the review of each of the operational and technical aspects of OneSchool previously described. Each finding has been documented within the context of ICT industry established good practice.

Key Findings

- **The formality of some OneSchool Operating Model processes have reduced since the system transitioned to 'Business as Usual':** Since the project transitioned to 'Business as Usual' status in 2011, the formality of some OneSchool Operating Model processes, which define the operation and processes for implementing changes to the application, has reduced, particularly for the development and release of smaller changes
- **A documented, well integrated SDLC is not consistently followed:** The OneSchool technology teams responsible for software development do not consistently apply a documented, integrated software development approach, in which all steps of the lifecycle are effectively linked. This raises the risk of a reduction in quality of key project artefacts which in turn may affect the final outcome and quality of delivered software and reliability of ICT services
- **Some team members have multiple roles, creating issues with the segregation of duties:** Some individuals within the OneSchool technology software and operations teams assume roles and responsibilities that would typically be divided amongst multiple individuals in line with accepted ICT industry good practice. This raises the risk of key steps within the SDLC not being completed to an adequate level of quality as key roles do not have an adequate segregation of duties. This may result in an increased risk of software faults reaching the live environment and potential future service failures
- **In some cases project team members without the appropriate skills and experience are performing key project roles:** In some cases non-technical staff are fulfilling roles typically conducted by personnel with more extensive ICT specific experience and training. This raises similar risks to the quality and reliability of live ICT services to those described above
- **The criteria used to assess the impact of changes to OneSchool SPM were insufficient to appropriately assess risk:** The criteria used by the OneSchool Application Board, when assessing application enhancements, may be biased toward the size, cost and complexity of delivery. For example, when a new release is documented for approval the information provided to the board describes the relevant module, the number of days' effort and the funding details. A more holistic assessment of the risks and impacts associated with the changes is not undertaken. The criteria should allow for an assessment of the potential business, stakeholder and technical implications of the changes, in addition to the size, cost and complexity
- **High risk and impact changes are not assessed and treated individually:** When the individual changes constituting a quarterly release are assessed as part of the wider DET change governance process, they are grouped together under a single master change. The individual changes within the release are not considered individually

despite the release potentially containing ‘small’ yet high risk changes. These changes could warrant additional scrutiny throughout the development and release process

- **The OneSchool Application Board has no final approval for the components of the quarterly release:** The Application Board provides approval of the initial scope of all proposed application changes and enhancements within a quarterly release. After initial approval, it has no further visibility of the final scope and functionality included within the release. It is therefore possible that decisions made after board approval may affect the final functionality and risk or impact of changes to be released to the live environment without the awareness or approval of some key stakeholders
- **The original SPM design did not consider the wider business and information security implications of adopting email for transmitting SPRs:** The solution design options assessment performed by the OneSchool Program prior to the implementation of the SPM did not fully consider the wider business and information security implications of adopting email as the preferred approach. Email as a communication mechanism does not guarantee delivery and so can result unpredictable behaviour in the wider email distribution environment, much of which is outside of the control of DET
- **No evidence of other solution options being considered to support the SPM other than email:** There was no evidence to indicate the solution design process considered the a broader range of technical options available to address the challenges and deficiencies inherent in the email distribution approach
- **No evidence of an information security classification being completed on OneSchool SPM data:** There was no evidence to indicate an information security classification was completed for OneSchool SPM data, including the sensitivity of information transmitted within the SPR emails. The absence of this classification may have contributed to other design decisions that have the potential to add risk to the wider environment. For example, a school principal currently receives a copy of the SPR via their Office 365 email account
- **OneSchool application code contains the logic to address the requirements:** We found the software code underpinning the SPM does contain logic to address each of the legislative and other core business requirements specified by the DET Child Safety business stakeholders.

Summary Recommendations

As described earlier, due to the objective and independent parallel incident investigation into SPM reporting, there was limited opportunity to review and update the findings and recommendations with senior DET ICT staff. Below are the key recommendations arising from this work.

- **Reinforce control and quality of the SPM with short term improvements:** Implement additional control and quality assurance mechanisms for any change impacting the SPM. This should be in addition to the current process followed to develop, operate and support OneSchool.
- **Update the OneSchool SDLC framework adopting risk based approach to change:** Update changes to the OneSchool SDLC Framework aligned with DET standards that clearly define the practices and procedures to be followed by OneSchool teams. The new framework should adopt a risk based approach where the risk profile of each change request dictates the level of rigor, control and quality assurance mechanisms required across the SDLC.

- **Review the OneSchool Operating Model and appoint key outstanding roles:** Review the Operating Model to ensure roles and responsibilities are clearly defined and aligned within the revised SDLC and consider implementing the components of the model that have not been implemented so far (e.g. operational split between Application Delivery and Application Support). Finally, consider appointing some full-time roles that are not full-time roles in the current model, particularly Technical Project Managers, Business Analysts and Release Manager.
- **Implement stronger operational governance mechanisms for releases:** Stricter operational governance mechanisms should be implemented to monitor progress and manage risks during the release. This will improve the alignment of the future product development with business requirements and DET standards and will ensure that the OneSchool Application Board is more actively overseeing the delivery of each release.
- **Refine the ICT Project Management Framework (ICT PMF) and improve usage by OneSchool:** The ICT PMF should be updated to clearly define what should be considered a “Project” and thus define which activities need to follow the framework. Additionally, the framework should provide clearer indication of the documents to be consistently produced at each phase and the sign-offs that are required. Finally, the ICT PMF should be fully adopted by OneSchool for the management of the end-to-end release and individual change requests (as appropriate).
- **Develop better quality assurance, proactive monitoring and problem management procedures during support of the OneSchool Application:** Review the current support procedures to ensure monitoring activities are well defined and responsibilities are clearly understood. Processes should be reinforced for high risk areas (e.g. SPM) to increase quality of issue resolution and eliminate re-occurrence of issues. Problem management should be formalised to proactively address the root-cause of issues.
- **Improve usage of tools across OneSchool SDLC:** OneSchool should implement a tool to holistically support the OneSchool SDLC and cover areas that are currently poorly supported such as requirements management, quality assurance and defect management. Further analysis is required to assess if the current tool (i.e. Microsoft TFS) is appropriate, and perhaps not fully utilised, or if an alternative should be considered. Additionally, a tool to support the automation of regression testing could also be implemented.
- **Stop sending SPRs to Principals via email:** The SPM currently sends a copy of the SPR to the principal that finalised the report. DET should consider whether this message could be replaced by a simple alert notification email. This change will avoid unnecessarily transmitting potentially confidential information via email.
- **Arrange for additional email whitelisting with QPS and DCCSDS:** Engage with QPS and DCCSDS to arrange for any additional configuration of email filters within their infrastructure to ensure messages from the OneSchool application are permitted to pass through to recipients without being blocked. This will reduce the risk of OneSchool SPR being incorrectly blocked by email filters and not reaching the intended destination at QPS and DCCSDS. DET, QPS and DCCSDS should collaborate regularly regarding changes to their own email infrastructures which may impact the future transmission of Reports via email.
- **Perform an Information Security Classification for OneSchool data:** An information security classification exercise should be completed for the data processed by the OneSchool application. This should take into account relevant QGCIO standards and policies. This will allow DET to understand the security requirements of data processed

by OneSchool and adjust the technology architecture of OneSchool appropriately in line with those requirements.

- **Investigate short and long term alternatives to email:** Within section 6 a number of alternative conceptual solution options are provided. These may be further investigated and implemented by DET to address the issues inherent in the email distribution of SPRs.

3 Background

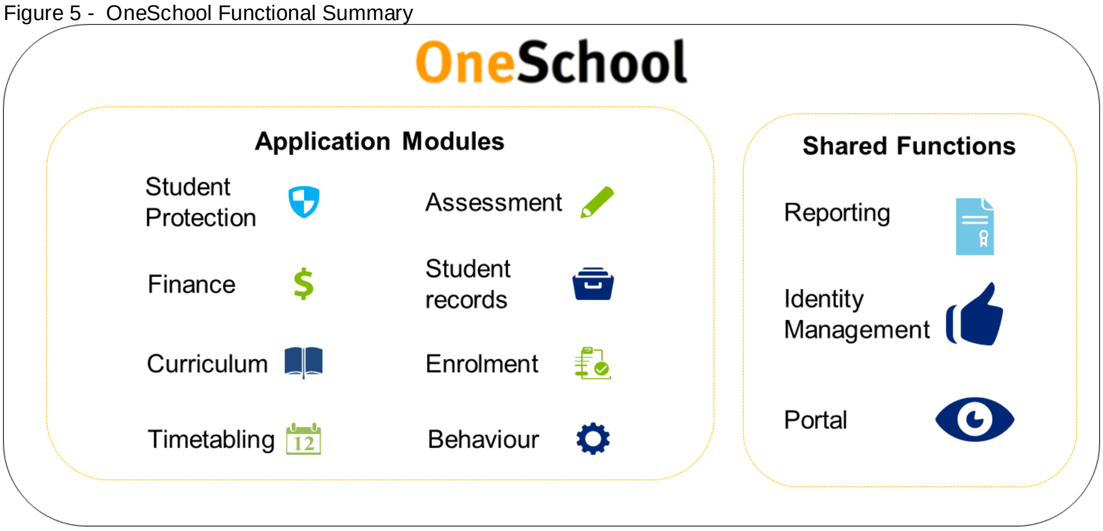
3.1 OneSchool – Queensland online school management system

In 2003 DET identified the need for a state wide school management system to support teachers, administrators and students and commenced planning for a centralised solution. Prior to this, each state school across Queensland was responsible for its own individual records which highlighted issues of standardisation, retention and accessibility for DET.

As DET could not identify an off-the shelf solution, a decision was made to build a school management system using the department's own system development team and ICT partners. This was the genesis of the OneSchool program.

The first release of OneSchool was deployed to all state schools across Queensland in 2008. Further releases occurred in 2009 and 2011 to broaden the services to schools through the online system. Today, OneSchool is used extensively by every teacher in every state school in Queensland. The platform currently comprises the modules outlined in the diagram below:

Figure 5 - OneSchool Functional Summary



3.1.1 DET student protection reporting module (SPM): A Brief History

The OneSchool SPM is a standalone module within the wider OneSchool system that enables the reporting of student protection information to DET, the DCCSDS and QPS. Prior to the implementation of the SPM in OneSchool in October 2013, the student protection reporting was undertaken manually, with a paper document completed and attached to either email or fax. This was then sent directly to the relevant agency/s.

The decision to integrate the student protection reporting process into OneSchool, and transform it into an online electronic reporting process was made following the issue of two internal reports on the subject in 2008 and 2009. These are described in the following table:

Table 1 - SPM Development Milestones

Year	Key developments
2008	In 2008, a DET Internal Audit review recommended: '*a review to be undertaken to address short-comings in student protection reporting of policy SMS-PR-012. This review should cover the content of the policy itself, staff training, resourcing, design of reporting forms, and also any other concerns staff may have.'*
2009	In 2009, the Director General commissioned an internal investigation into the handling of student behaviour. It recommended that '*consideration be given to enabling all student protection reporting forms to be completed and sent electronically via OneSchool.'* Furthermore, the report found the existing manual student protection reporting process to be time intensive and lacking safeguards surrounding privacy, security and confidentiality.
2010	In September 2010, a business case was submitted to DET management to address the future of student protection reporting. The report outlined possible approaches to address the manner in which the 'end to end' process of student protection reporting was handled and recommended that '*DET leverage the OneSchool single point of truth of student data*' ensuring all reports are housed within a single application. The business case was endorsed by DET senior management. However, following this decision, due to a lack of funding and other priorities the implementation into OneSchool of student reporting did not occur until October 2013.

DET IT staffing

For reference, we note at August 2015 the DET Information & Technologies Branch (**IT Branch**) was 476 staff which comprised 463.23 FTE employees. The OneSchool staff numbers are included in these figures.

These can be further broken down into the following sub groups:

- Permanent -153.52 FTE
- Temporary -172.51 FTE
- Performing Duties – 137.2 FTE

A five year analysis of IT Branch staffing numbers provided by DET can be found in the table below. OneSchool is reliant on some services from IT Branch for infrastructure, governance and some operational support activities. We note throughout this period there have been variations in headcount of IT Branch staff.

Table 2 - IT Branch Staffing Numbers

	June '11	June '12	June '13	June '14	June '15
Performing Duties	184	207.96	144.9	119.4	138.3
Permanent	137.9	135.48	139.6	129.3	169.86
Temporary	226.23	276.53	169.86	142.81	171.96
Total FTE	**548.13**	**619.97**	**454.36**	**391.51**	**480.12**

3.2 Queensland child protection regime

The Queensland child protection regime exists to protect at-risk children from abuse and neglect. A portfolio of Queensland Government Departments have involvement in the protection of vulnerable children, however, the issues central to this report focus on DET, DCCSDS and QPS.

- DET primarily administers state school education across Queensland encompassing 1,234 Schools, approximately 500,000 students being taught by approximately 40,000 teachers with a budget in excess of $5.4 billion
- DCCSDS is the lead agency for child protection in the State and is dedicated to protecting children and young people who have been harmed, or are at risk of harm
- The QPS are the primary law enforcement agency in Queensland and in their child protection role, investigate and prosecute criminal allegations of physical and sexual abuse of children.

This report focuses on the child protection reporting requirements of DET, however all three agencies have interconnecting roles prescribed by two Queensland Acts of Parliament:

- Queensland Child Protection Act
- Queensland Education Act.

DCCSDS are the lead agency for the Child Protection Act which specifies mandatory reporting requirements where a child has suffered, is suffering or is at unacceptable risk of suffering significant harm caused by physical or sexual abuse and does not have a parent able and willing to protect the child from harm. DET frontline staff, specifically teachers and principals, also have 'mandatory reporting requirements' under the Education Act to report sexual abuse to QPS.

3.3 Child Protection Legislation

To better understand the purpose and design of the OneSchool SPM, we have outlined the mandatory reporting requirements of the Child Protection Act and Education Act below along with the changes introduced as a result of the Queensland Child Protection Commission of Inquiry final report findings (**Carmody Report**).

3.3.1 Queensland Child Protection Commission of Inquiry

Table 3 - Carmody Report Key Milestones

Key Development	Description
Establishment of Carmody Enquiry July 2012	The Queensland Child Protection Commission of Inquiry was established in July 2012 under the leadership of the Honourable Tim Carmody QC to *'develop a roadmap for the next decade to produce the best possible system for supporting families and protecting children that our state can afford.'*
Carmody Report issued July 2013	On 1 July 2013 the Carmody Report was publicly released. One of the report's findings, relevant to this review, related to the student protection reporting framework and the increasing volume of actual or suspected physical or sexual abuse reports that were being created by staff within DET.
Report recommendations	The Report proposed a consolidation of child protection arrangements which are outlined below. a) Recommendation 4.2 - the DPC and DCCSDS lead a whole of government process to review and consolidate all existing legislative reporting obligations into the Child Protection Act 1999, develop a single standard to govern reporting policies across core Queensland

	Government agencies and provide support through joint training. b) Recommendation 4.3 - the QPS revoke its administrative policy that mandates reporting to DCCSDS and replace with a policy reflecting the standard in recommendation 4.2. c) Recommendation 4.6 - the Minister for DCCSDS propose amendments to the Child Protection Act 1999 to allow mandatory reporters to discharge their legal reporting obligations by referring a family to the community based intake gateway and afford them the same legal and confidentiality protections currently afforded to reporters.

3.3.2 Key Legislation

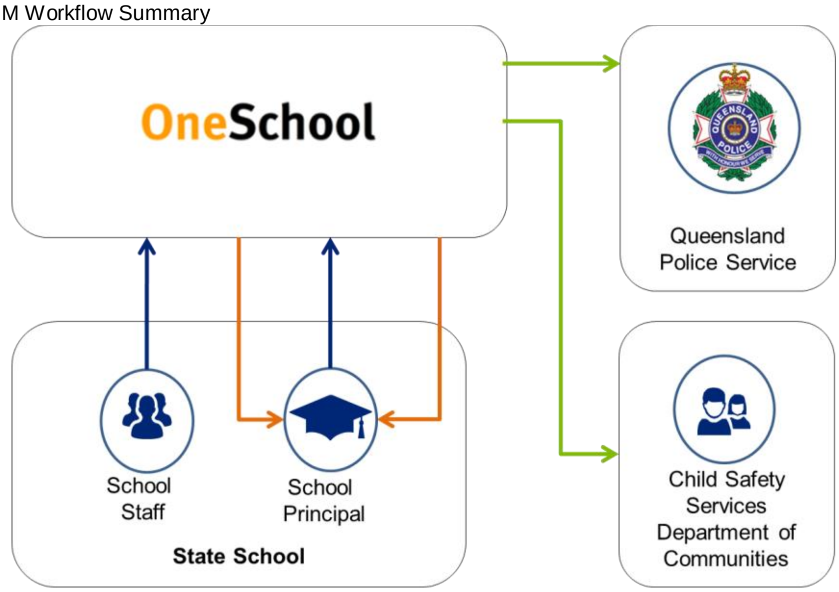
Table 4 - Key Legislation Relevant to SPM

Key Agency/ Requirements	Description
Child Protection Act 1999	The *Child Protection Act* upholds the principle that all children have the right to be protected from harm or risk of harm. The mandatory reporting requirement for school staff, outlined in section 13E of the Act, requires that a teacher or registered nurse must make a report when they reasonably suspect that a child: a) has suffered, is suffering, or is at unacceptable risk of suffering, significant harm caused by physical or sexual abuse; and b) may not have a parent able and willing to protect the child from the harm.
Education (General Provisions) Act 2006	The *Education (General Provisions) Act 2006* regulates the education of children living in Queensland. The mandatory reporting requirement for a school staff member of a State school states that a written report must be made to QPS if *'a staff member becomes aware, or reasonably suspects, that a student under 18 has been sexually abused, or is likely to be sexually abused by another person.'*

3.4 Implementation of the SPM into OneSchool - October 2013 and January 2015

The first release of the SPM into OneSchool went live in October 2013 following a staff training and awareness program. The SPM provided state school staff with online functionality to submit student protection concerns directly to DCCSDS and QPS which is illustrated in the following diagram.

Figure 6 - SPM Workflow Summary


OneSchool
Queensland Police Service
School Staff
School Principal
State School
Child Safety Services Department of Communities

The SPM workflow follows a creation and approvals process which is routed from either teacher or principal as the initiator, through to principal or principal supervisor as the approver, followed by the transmission of the student concern report, via email, to either or both of the QPS and DCCSDS, depending on the nature of the concern.

Hypothetical example: The initiator of the student concern logs in to the OneSchool SPM and completes a narrative relating to the particular report being made and confirms the type of activity they suspect is happening (sexual abuse, physical harm or other).This report is then routed within the OneSchool SPM to the approver, usually a principal, for ultimate editing and approval. Once approved, the OneSchool SPM creates an email and appends a Microsoft Word document containing the student protection concern details. Once finalised, the email is sent to a predefined QPS and/or DCCSDS email address, based on the location of the report initiator.

The Carmody report was released on 1 July 2013 after the first prototype of the SPM had already been completed, presented and endorsed by the OneSchool Principals reference group. It was therefore decided to release the initial version of the SPM as part of the October 2013 OneSchool system changes and then follow up with a further upgrade once the operational implications of the Carmody report recommendations were fully understood.

Those recommendations were subsequently implemented into the SPM with the January 2015 SPM update. Under the legislation, the Principal is required, when notified of a student protection concern via the receipt of a SPR, to forward the report to:

- the QPS only when the content of the report indicates that a student may have been sexually abused, or is at risk of being sexually abused
- the DCCSDS only when the content of the report indicates that a student may have been significantly harmed or may be at risk of significant harm as a result of physical, sexual or emotional abuse and may not have a parent who is willing and able to protect them from harm
- both QPS and DCCSDS when the content of the report indicates that a student may have been significantly harmed or may be at risk of significant harm as a result of sexual abuse and the child may not have a parent who is willing and able to protect them from harm.

4 OneSchool Technology Assessment

4.1 Introduction

Deloitte were engaged to review, assess and make recommendations relating to the technical design and implementation of the SPM and the wider software and technology delivery capability of the OneSchool program within DET.

As part of this review the following aspects of the OneSchool program and technology solutions were examined and assessed:

- The OneSchool SPM technical design, software code and the underpinning ICT infrastructure supporting the delivery of SPR's
- The processes and governance followed by the OneSchool and DET team to specify, build, test, deploy and manage OneSchool software functionality
- The structure, roles and responsibilities of the relevant technology delivery and management teams within the OneSchool program and DET.

The governance, teams, processes and technologies within the wider DET ICT environment that do not directly contribute to the delivery and operation of the OneSchool program and application were out of scope for this review.

4.2 Technology Assessment Structure

In order to further delineate the scope of the review and provide structure to the findings and recommendations, the technology assessment has been divided into two key areas of focus as follows.

4.2.1 Operational Review

The operational review considers the roles and responsibilities of OneSchool and wider DET operations in relation to end to end software development, documents any associated risks and provides relevant remediation actions. The operational review also assesses the governance and processes in place within the OneSchool program and wider DET operations that guide the enhancement and operation of the OneSchool application.

4.2.2 Technical Solution Review

The technical solution review considers the SPM design, software code and underpinning ICT infrastructure. Any identified technical risks are categorised and mitigation recommendations are provided. The mitigation recommendations include activities that should be considered immediately in addition to more strategic enhancements that can be further investigated by DET in the longer term.

4.3 Summary of Recommendations

Throughout this report we have made a number of recommendations, some of which can be implemented sooner than others.

4.3.1 Short term recommendations

The following table sets out those recommendations that we believe can be implemented by DET in the short term (referred to here as short and long term recommendations).

Table 5 - Short Term Recommendations

Area	Recommendation	Outcome
Governance	Appoint a single person with direct responsibility for OneSchool releases including scoping, planning, design, build, testing and to seek final approval of the release scope.	This will ensure that a single point of accountability for the delivery exists and will allow for better risk, issue and dependency management.
Governance	Ensure the OneSchool Application Board has direct insight into all elements of a release and oversight of the results of the test phase providing final approval for the release of agreed and tested scope and functionality.	This will increase the accountability of the board for the outcome of the release and will ensure a final point of review and control by the senior stakeholders.
Governance	Formalise the weekly change request meeting and create mechanisms to escalate risks, changes of scope or issues requiring executive approval from Project Board or OneSchool Application Board.	This will allow for improved control over the scope of each change request and quicker escalation of significant risks/issues to delivery.
Governance	The DET Technical Architecture Board is primarily focussed on the high level architectural governance of the entire DET environment rather than the review of individual technical designs and product development. Oneschool could benefit from the establishment of an architectural governance body with the responsibility of owning the technical vision and long term development of the Oneschool product	This will provide a mechanism by which proposed technical solutions, to address business requirements, are designed in the most appropriate way and align with DET architectural standards.
Organisation	Ensure that personnel with appropriate technical experience are assigned to work with priority business projects to fulfil key technical delivery roles including Technical Project Management, Business Analysis and Solution Architecture.	This will ensure that technical activities are appropriately managed and coordinated, that the business requirements are understood and translated into a language that is easily comprehended by technical teams and that designs are validated by suitably trained and experienced ICT architects with a broader view of technical implications than the development team.
Organisation	Agree the minimal set of technical artefacts to be consistently produced by project teams during software specification, delivery and testing and ensure appropriate peer review of these artefacts occurs.	This will align the documented approach with industry standard practices and support informed project decision making. This would also reduce the dependency on key individual resources and also the likelihood of errors being

		released in the live system.
Process	Individually assess the changes to OneSchool functionality proposed with the major quarterly releases in order to understand the specific risks and implications associated with each new piece of planned functionality. An assessment criteria framework should immediately flag proposed systems changes involving SPR to a default high risk category. A single high risk change in a release should default the entire release to the same high risk level.	This will facilitate increased scrutiny of the risks associated with individual changes before they are deployed into the live environment. This in turn will reduce the likelihood of faults reaching the live environment.
Process	Increase the level of quality assurance mechanisms associated with the resolution and closure of incidents associated with the SPM.	This will improve the identification and resolution of the root causes of incidents reducing the likelihood of them recurring.
Process	Increase the involvement of Business Unit representatives in designing and executing tests including the business itself, particularly for high risk / impact changes.	This will ensure that changes to OneSchool are tested by end business users and will reduce the risk of unexpected faults in the live environment and of solutions failing to meet business expectations.
Technical	Engage with QPS and DCCSDS to arrange for any additional configuration of email filters within their infrastructure to ensure messages from the OneSchool application are permitted to pass through to recipients without being blocked.	This will reduce the risk of OneSchool SPR being incorrectly blocked by email filters and not reaching the intended destination at QPS and DCCSDS.
Technical	An information security classification exercise should be completed for the data processed by the OneSchool application. This should take into account relevant QGCIO standards and policies. The implications of this review should be factored into all future planning and design related to the SPM.	This will allow DET to understand the security requirements of data processed by OneSchool and adjust the technology architecture of OneSchool appropriately in line with those requirements.
Technical	The SPM currently sends a copy of the SPR to the principal that finalised the report. DET to consider whether this message should be replaced by a simple alert notification email	This change will avoid unnecessarily transmitting potentially confidential information via email.
Technical	Investigate the implementation of an SPR download portal approach based on the distribution of simple download links ‘One time URLS’.	This will avoid the transmission or loss of potentially confidential information via email and will provide an audit log for the tracking of report access and avoid the non-delivery of SPRs via email.

4.3.2 Long term recommendations

In addition to the short term recommendations above, the following table sets out those that we believe DET should also consider for implementation. We note that in some cases these will require partnering with other agencies and also may require a larger scale reform and investment.

Table 6 - Longer Term Recommendations

Area	Recommendation	Outcome
Governance	Assign a person or group with clear responsibility for capturing, assessing and managing business and technical risks relating to changes and ensure that these risks have been appropriately assessed against a consistent and agreed framework.	This will allow the business and technical risks of each OneSchool change to be assessed by staff with the right skills, through following a standard approach that can be tested and repeated.
Governance	Ensure that all projects involving OneSchool have appropriate project boards to which the relevant project manager can escalate if they are experiencing material scope changes or risks / issues with OneSchool delivery or engagement.	This will facilitate quicker issue resolution, proactive risk management and will increase the involvement and accountability of senior stakeholders in delivery of OneSchool projects.
Organisation	Provide additional training to business project managers in Project Management and in the ICT Project Management framework.	This will allow for the business project managers to be able to consistently and effectively manage projects.
Organisation	Update the existing OneSchool operational plan clarifying the steps and roles and responsibilities that need to be included within a business project's engagement with the program	This will ensure that roles and responsibilities are clearly understood and the risk of key activities being missed is reduced. This will also facilitate improved knowledge sharing and reduce dependency on key resources.
Process	Define a consistent and integrated end-to-end OneSchool software development process outlining practices and steps to be followed by the relevant teams. Roles and responsibilities of all team members should be clearly outlined.	This will increase the efficiency and quality of the delivery and will ensure each person clearly understands his/her role in the process and what this entails. This will also increase knowledge sharing and communication within the organisation and reduce dependencies on key personnel.
Process	Adopt a risk based approach where the profile of individual changes dictates the level of rigor, control and quality assurance required across	This will ensure high risk changes are appropriately and rigorously designed, developed

	the end-to-end software development process described above.	and tested without compromising the pace at which lower risk changes can be delivered. This will also reduce the likelihood of major issues occurring in production.
Technical	Investigate the feasibility of implementing a Portal with Identity Management (Refer to option 1 as described in section 6.5.6). Implement portal access and SPR download for QPS and DCCSDS with identity management.	This will avoid the transmission of potentially confidential information via email and will allow OneSchool to gain additional insight as to whether the SPR generated has been accessed. This would improve the traceability of report access and would facilitate improved analysis of outstanding reports for all stakeholders.
Technical	Investigate the feasibility of implementing a technical solution enhanced with increased System Integration (Refer to option 2 as described in section 6.5.6). This would require the system integration between OneSchool and the various systems in use within QPS and DCCSDS.	In addition to the benefits offered by Option 1, this should also increase the overall level of data consistency and quality and realise a corresponding improvement in the reliability of Student Protection Reporting across the various agencies
Technical	Investigate the feasibility of implementing an end to end Case Management solution (Refer to option 3 as described in section 6.5.6). It has been noted that Student Protection information within Queensland is distributed across a number of systems within numerous government agencies and as a result, no single source of information exists. In order to address the challenges this presents, Queensland Government could seek to implement a holistic end–to-end Child Protection solution at a state level. This implementation would require the deployment of a single case management information system to manage child reporting as cases allowing for all parties to contribute to individual cases.	In addition to the benefits offered by Options 1 and 2, this should provide further reliability and quality improvements in Student Protection Reporting from the implementation of a single consistent student protection business process and case management solution.

5 OneSchool IT Operations Review

5.1.1 Overview

The OneSchool system provides Queensland State Schools with a range of business functionality. The system consists of a number of integrated software modules which work together in order to provide schools with support for the following:

- Student management
- Curriculum and learning management
- Finance and asset management
- Resource management
- Performance, reporting and analysis
- Student protection

Specifically, the OneSchool SPM facilitates electronic submission of student protection information to DCCSDS and the QPS as required by legislation and DET student protection policies.

The initial release of the OneSchool application was deployed in 2007 followed by two additional major releases in 2009 and 2010. In 2011 the application transitioned into Business as Usual (BAU) mode and has been managed by internal resources from the IT Branch team. Since then, changes to the application are managed in quarterly releases that are overseen by the OneSchool Application Board.

5.1.2 Objectives

As part of the SPM review, Deloitte was tasked with conducting a holistic review of the current practices in place to develop and operate the OneSchool Application in order to address the following objectives:

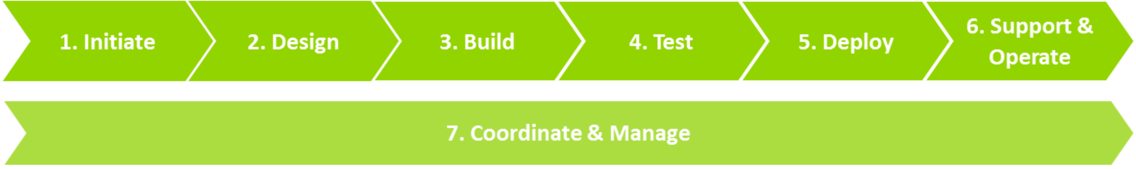
- Identify any weaknesses and constraints of the current practices with particular focus on:
  - Application Testing and Quality Assurance Framework
  - Business Requirements and the creation of software code
  - Approval of IT upgrades / changes to the OneSchool application
- Propose recommendations for strengthening procedures and practices.

5.1.3 Approach

The process of software development typically involves the completion of a number of industry standard practice steps in order to translate a request for system functionality into a live operational system. This sequence of steps is referred to within the ICT industry as the ‘Software Development Lifecycle’ (SDLC). Deloitte conducted a review of the practices in place to develop and operate the OneSchool application across each of the individual steps of the SDLC.

Due to the fact that different representations of the SDLC steps exist within DET, Deloitte agreed with key stakeholders a common set of key steps to be used as a reference framework for the review. These steps are explained in more detail within the diagram and bullet points below.

Figure 7 – Common SDLC Steps



1. **Initiate:** Identify the need for change in the functionality of the application, collate high level business requirements, seek funding approval and plan development
2. **Design:** Document detailed requirements, design the solution, plan the execution of tests and design test cases/scripts
3. **Build:** Build the solution based on the business requirements defined in the initiate and design phases by developing the required software code and performing unit testing
4. **Test:** Perform the required tests to ensure the solution operates in accordance with the defined requirements
5. **Deploy:** Prepare and deploy the solution into live production including appropriate training to users and support teams
6. **Support & Operate:** Support, operate and monitor the OneSchool application in the Production Environment
7. **Coordinate & Manage:** Coordinate, report progress and manage risks of the end-to-end process to develop an ICT solution.

In order to provide further structure to the review, the observations, findings and recommendations are aligned to four key scope dimensions commonly used within the ICT industry to subdivide the operational aspects of ICT capabilities:

- **Organisation:** Organisational structure, roles & responsibilities in place to manage OneSchool.
- **Governance:** Governance mechanisms that exist to oversee the management of the OneSchool application
- **Process:** Processes and procedures followed by the teams to develop, operate and support the OneSchool application
- **Tools:** Tools used to support the processes.

To support this analysis Deloitte obtained and reviewed relevant available documentation and met with a number of key OneSchool and DET stakeholders. Although the review is not intended to be nor structured as a compliance audit, the following industry good practices were considered when documenting findings and developing recommendations:

- CMMI: Capability Maturity Model Integration – a guide for process improvement in projects, divisions or organisations
- COBIT: Control Objectives for Information and Related Technology – a framework and toolset for IT management governance and control
- ITIL v3 and ISO 20000: Information Technology Infrastructure Library – a set of practices for IT service management that focus on business requirements
- ISO 12207 Systems and Software Engineering – Software Lifecycle Processes: International Standard for software life cycle processes for developing and maintaining software
- ISO 14764 Systems and Software Engineering – SDLC Maintenance: Framework for software maintenance planning and execution
- ISO 9126 Software Engineering – Software Quality: Quality model for software development and operation

- International Software Testing Qualification Board - Testing qualification certification organisation
- V-Model - Software development process similar to the waterfall method where testing of the product is planned in parallel with a corresponding phase of the development.

5.2 Current State Analysis

This section summarises the current practices in place guiding the development and operation of the OneSchool application across the various steps of the SDLC and is sub-divided in alignment with four dimensions of the analysis described in Section 5.1.3: Organisation, Governance, Process and Tools.

5.2.1 Organisation

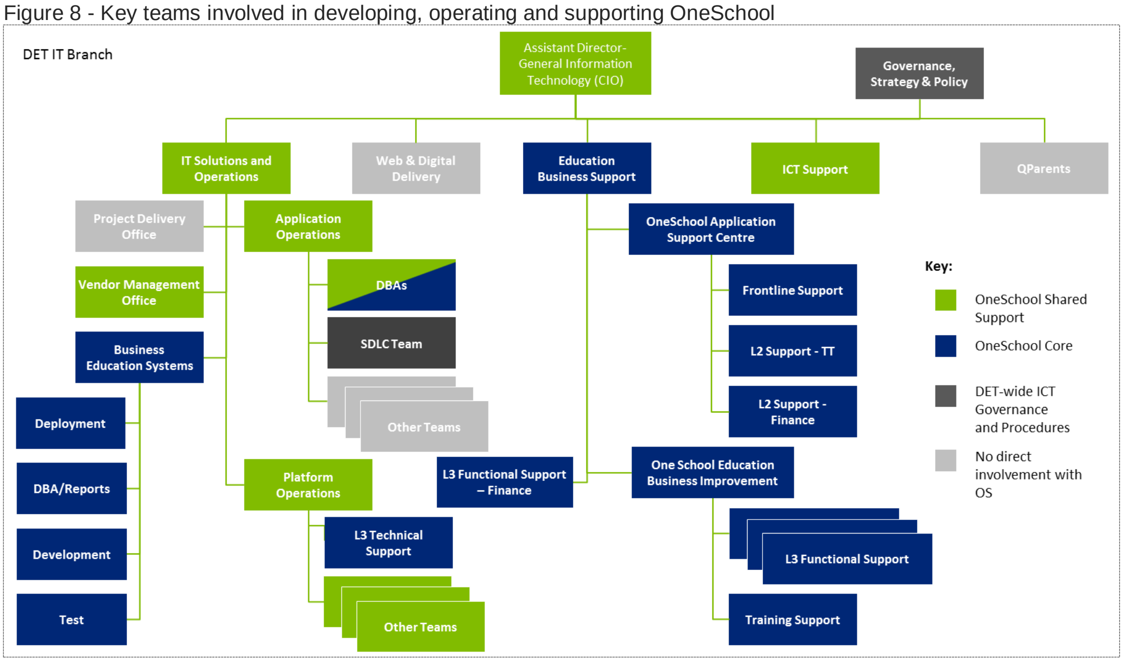
This section describes, from an organisational perspective, the functional groups and people involved in developing, supporting and operating the OneSchool application.

The teams can be classified into four levels of involvement with the OneSchool application:

- **OneSchool Core:** Teams who develop, support and operate OneSchool
- **OneSchool Shared Support:** Teams that provide support for OneSchool, in addition to supporting other DET ICT applications or functions
- **DET-wide ICT Governance and Procedures:** Teams that support the creation and execution of DET-wide ICT frameworks and methodologies that need to be followed by OneSchool teams
- **No direct involvement with OneSchool:** Teams not involved with OneSchool directly.

The structure and function of each unit is depicted in the diagram below. The diagram is focused on the OneSchool program and therefore does not provide an exhaustive view of all DET teams involved in wider ICT delivery.

Figure 8 - Key teams involved in developing, operating and supporting OneSchool



The key responsibilities are described in the table below. An outline is provided of each unit or team's role in relation to the SDLC and the OneSchool development, operation and support model.

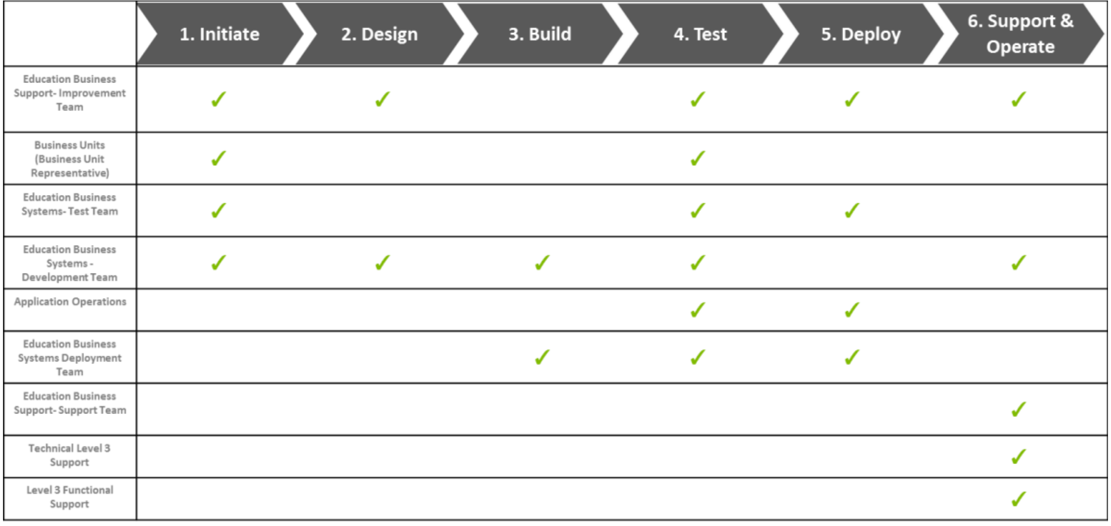
Table 7 - Organisation Functional Descriptions

Team	Key Responsibilities (not exhaustive)
Business Units	Act as the business application owner of OneSchool. In particular these teams are responsible for the following activities: • Identifying new functionality to be developed and define the associated business requirements • Obtain funding for development of new functionality • Approve changes to be included in releases • Project management, from a business perspective, of the delivery of new functionalities • Accept successful deployment of new functionality into live Production Environment • Report issues and provide feedback for the OneSchool application.
Education Business Support	Provide day to day support to the OneSchool end-users and act as business representatives and SME during the development of OneSchool releases. In particular this team is responsible for the following activities: • Support: ○ Level 1/ Level 2 support to end-users • Education Business Improvement: ○ Level 3 SME support to end-users ○ OneSchool training of end-users ○ OneSchool business reporting and improvement ○ Manage functional aspects of change requests to OneSchool (i.e. gather requirements, testing) ○ Co-ordinate OneSchool releases ○ Secretariat of OneSchool Application Board. • Level 3 Functional Support – Finance: ○ Same as Education Business Improvement but for the Finance module of OneSchool (i.e. Agresso).
Education Business Systems	Design, develop and test changes to the OneSchool application and provide Level 3 support. In particular this team is responsible for the following activities: • Development: ○ Application development (technical design, build and unit testing) ○ Application monitoring ○ Level 3 Technical Support • Testing: ○ Application testing • Deployment: ○ Build package coordination • DBA/Reports: ○ Report development ○ Database tuning.
Application Operations	Develop, test and support all DET applications with the exception of web and digital apps, OneSchool application and other applications managed outside

	the IT Branch (i.e. SAP) However, this team does provide some support to OneSchool namely: • Database Administration (DBA) team that deploy OneSchool code to Training and Production Environments following instructions from Education Business Systems team and provide necessary support • SDLC team that manages the tools that are used by OneSchool to develop software and owns the recommended DET SDLC methodology.
Platform Operations	Maintain, support and update the DET ICT infrastructure (i.e. operating systems, networks, storage, and datacentre) excluding the application layer. This team has two FTEs dedicated to OneSchool covering: • Infrastructure support • Day to day support of the development teams from an infrastructure perspective (i.e. set up new virtual servers).
IT Solutions and Operations - Vendor Management Office	Process and manage ICT procurement of both goods and services, including: • Procurement policy and standards • Tender design and coordination and support • Contract management. This includes any 3rd party vendor associated with OneSchool application (e.g. Microsoft, Agresso).
Governance, Strategy and Policy	• Develop DET's ICT strategy, governance frameworks (e.g. Risk Management) and policies (e.g. Information Security Policy). • Manage the ICT Project Management framework and conduct project gate reviews for higher impact projects and project health checks for other projects. • Manage the ICT Portfolio by assessing business cases and co-ordinate approval by the Information & Innovation Steering Committee. • This team does not have day-to-day responsibility for managing the OneSchool application. However, the governance frameworks and policies defined by this team are intended to be followed by OneSchool teams.
ICT Support	Provide Level 1 & 2 support to DET users with the exception of SAP and OneSchool which have their own dedicated support teams. This team also defines the DET Incident Management process (including major incidents), knowledge management process and associated tools (e.g. ServiceNow). These processes need to be followed by OneSchool support teams. This team can receive calls/requests related to OneSchool. In this case, the calls/request will be redirected to the Education Business Support team.

The Education Business Systems and Education Business Support teams have a varied degree of involvement throughout the SDLC steps. For example, the Education Business Systems Development team contributes a large amount during the 'build phase'. The following diagram represents the key involvement of each team across the SDLC. Additional detail is provided in section 5.2.3.

Figure 9 - Business unit involvement in SDLC phases



	1. Initiate	2. Design	3. Build	4. Test	5. Deploy	6. Support & Operate
Education Business Support- Improvement Team	✓	✓		✓	✓	✓
Business Units (Business Unit Representative)	✓			✓		
Education Business Systems- Test Team	✓			✓	✓	
Education Business Systems - Development Team	✓	✓	✓	✓		✓
Application Operations				✓	✓	
Education Business Systems Deployment Team			✓	✓	✓	
Education Business Support- Support Team						✓
Technical Level 3 Support						✓
Level 3 Functional Support						✓

5.2.2 Governance

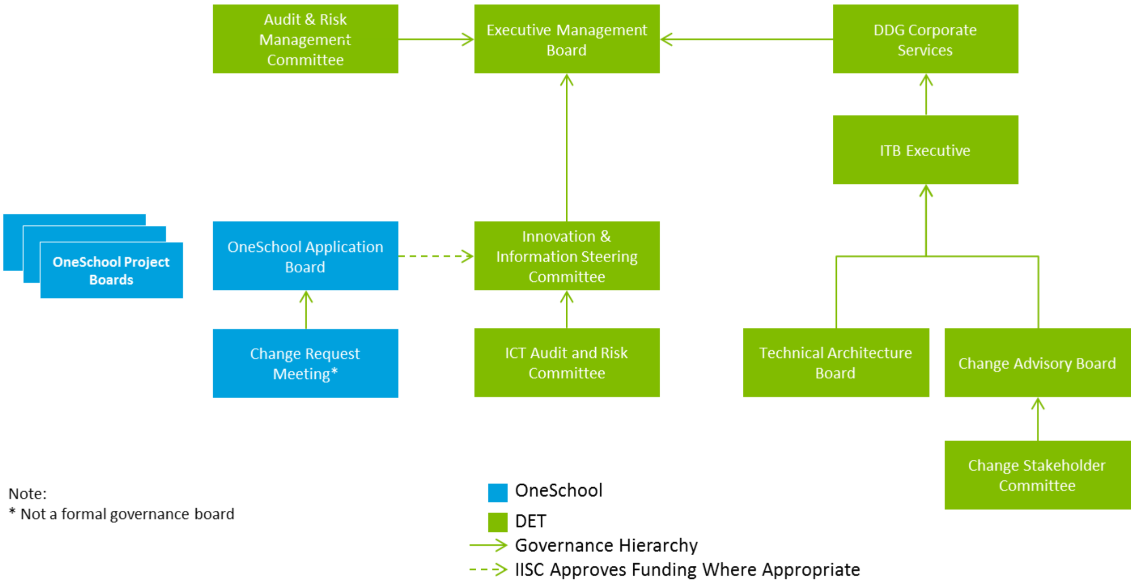
This section outlines the bodies, frameworks and methodologies that govern the key decisions relating to the OneSchool application and program.

Governance Boards

There are a number of boards that measure and monitor the performance of OneSchool with the authority to make decisions guiding the direction of the program and OneSchool application.

A summary of the OneSchool governance structure is depicted in the figure below.

Figure 10 - OneSchool Governance Structure



Audit & Risk Management Committee
Executive Management Board
DDG Corporate Services
ITB Executive
OneSchool Project Boards
OneSchool Application Board
Innovation & Information Steering Committee
Change Request Meeting*
ICT Audit and Risk Committee
Technical Architecture Board
Change Advisory Board
Change Stakeholder Committee
Note:
* Not a formal governance board
OneSchool
DET
Governance Hierarchy
IISC Approves Funding Where Appropriate

The boards mentioned in the previous diagram are formal bodies with powers and responsibilities defined within relevant Terms of Reference, with the exception of the informal Change Request Meetings. A summary of the responsibilities of the boards are described in the following table and are divided into two groups – OneSchool specific and DET wide boards.

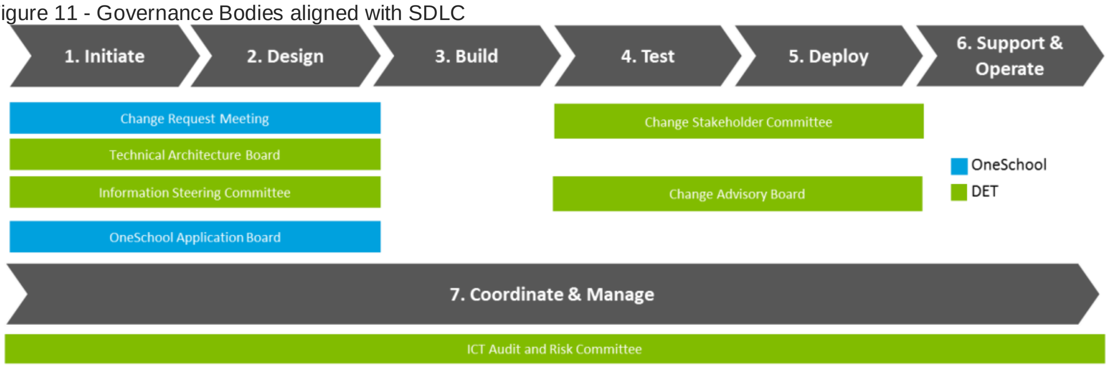
Table 8 - Governance Responsibilities

Board	**Key Responsibility** (not exhaustive)	Frequency
OneSchool Specific		
OneSchool Project Boards	• Provides direction, guidance and decision making to support the successful delivery of the project for the Sponsor. • These boards are only in place for the OneSchool large changes and are run by the business unit that is sponsoring the change. IT Branch teams will attend as appropriate and as defined by the Project Sponsor.	Varies
One School Application Board	• Provides governance across the development, operation and support of OneSchool. Approves the change requests that will be included in a OneSchool release. Monitors key metrics of the OneSchool Application (i.e. number of users) and reviews OneSchool risks.	Quarterly
Change Request Meeting *(informal)*	• Reviews and prioritises the development of all OneSchool change requests and decides which changes need to go to the OneSchool Application Board for approval. Also decides which small changes/bug fixes can be delivered within the current release. • At the end of the meeting, a report is extracted from TFS listing the decisions made and is shared with the people that attended the meeting. Note: This meeting does not have a defined Terms of Reference nor does it produce formal minutes.	Weekly
DET Wide		
Executive Management Board	• Supports the Director-General with the overall ICT governance and provides final approval on any investment recommendations of its sub-committees.	Weekly
Innovation & Information Steering Committee (IISC)	• Oversees strategic direction and proactively manages investment in innovation, information management and ICT within the department. • Change requests to OneSchool that require funding for delivery will come to this board for funding approval. The funding request is presented by the business unit requesting the change • Provides portfolio management capability, monitors project delivery and provides input into Whole of Government ICT dashboard reporting.	Monthly
ICT Audit and Risk Committee	• Proactively manages risk for the ICT portfolio within DET. • OneSchool risks are escalated to this board for management and oversight.	Quarterly
IT Branch Executive	• Oversees the management of the IT Branch of DET.	Fortnightly
Technical Architecture Board	• Provides governance for DET ICT Architecture and ensures any new technology/application/module is aligned with ICT Strategy and Architecture Standards.	Monthly

	- This board is focused on reviewing architecture of projects that will have a significant impact to the overall ICT architecture and/or are implementing new technologies. Any OneSchool change requests that fit this description will need to come to this board for endorsement prior to funding approval at IISC.	
Change Advisory Board (CAB)	- Assists the Change Manager in assessing, prioritising and scheduling complex and high risk changes (classification Level 1 (major) and escalated Level 2 (significant) changes).[1]	As Required
	- Reviews and approves all Level 3 (minor) and Level 4 (operational) changes, and provides initial review of Level 1 (major) changes prior to submission to the CAB.	Twice Weekly

These bodies provide governance and approval for progression through the SDLC phases. The following diagram represents the involvement of the key governance bodies throughout the SDLC.

Figure 11 - Governance Bodies aligned with SDLC


1. Initiate
2. Design
3. Build
4. Test
5. Deploy
6. Support & Operate
Change Request Meeting
Technical Architecture Board
Information Steering Committee
OneSchool Application Board
Change Stakeholder Committee
Change Advisory Board
OneSchool
DET
7. Coordinate & Manage
ICT Audit and Risk Committee

Methodologies & Frameworks

DET mandates a number of methodologies and frameworks that should be followed by teams within the department including OneSchool, in order to manage, operate and support applications.

The table below provides additional information regarding the relevant DET Methodologies and Frameworks and a summary of how they are currently leveraged by the OneSchool teams.

[1] From the "*ICT Change Management Process Specification V4.4"*

Major (Level 1): Major Changes have potential to affect the entire organisation. They may affect multiple CIs, all services and/or clients, or VIP level customers (i.e. political visibility is high). Notification is needed to all affected stakeholders.

Significant (Level 2): These changes may affect key services or CIs and have a significant impact. Notification is needed to all affected stakeholders.

Minor (Level 3): These changes affect a small group of users, or a single non-critical service or CI.

Operational (Level 4): These changes are low risk and adhere to a typically well tested procedure or work instruction, are relatively common and are the accepted solution for a specific requirement.

Table 9 - Frameworks and Methodologies

Framework/Methodology	Description	Relationship with OneSchool
DET ICT Governance Framework	Provides direction for ICT investment and ongoing activities to ensure: • Alignment with business strategy and objectives • Use of ICT to enable department transformation and efficiency • Responsible use of ICT resources • Appropriate management of ICT related risks • Identification of business benefits and realisation.	This is the framework followed by OneSchool
DET ICT Project Management Methodology	Defines the processes that must be followed to initiate and manage an ICT Project.	This methodology is only followed for large OneSchool change requests that require additional funding. For some projects (e.g. SPM) it is only formally used during the 'initiate' and 'design' phases and for monthly reporting. The project manager within the Business Units coordinates this process and seeks support from the IT Branch when required.
DET Software Development Life Cycle Methodology	Describes the software development practices to be used within DET from the idea and initiation phases through to support and operation. This methodology is mainly focused on software coding standards.	OneSchool follows its own SDLC methodology which was defined when the application was still managed as a project. This methodology is not formally documented.
ICT Risk Management Framework	Defines how risks are captured and managed in order to minimise adverse impact on DET ICT.	This is followed by OneSchool. OneSchool risks are also discussed at the OneSchool Application Board
ICT Change Management	Defines the process to manage all changes to the DET architecture, applications, network, infrastructure and environments, and associated services and documentation, both within ITB and vendor managed ICT.	This is followed by OneSchool
ICT Incident Management	Defines the process used by support teams to log and resolve issues identified by the ICT users.	OneSchool follows this process (and associated tools) but has additional OneSchool specific procedures that need to be followed.

5.2.3 Process

This section describes the steps typically followed to develop, support and operate the OneSchool application across the different phases of the SDLC. These steps have been synthesised during our review from a combination of interviews and are not currently documented as an integrated process within DET.

Changes to the OneSchool application are typically grouped into quarterly releases linked to school terms. The majority of new functionality deployed to the OneSchool application is included within these regular releases. Exceptions to this include urgent bug fixes which can be deployed immediately and minor changes (e.g. changes to text fields) which can be deployed to the Production Environment fortnightly.

The key activities and decision points involved in developing and deploying changes as part of the OneSchool release cycle aligned to the SDLC are described in the following section.

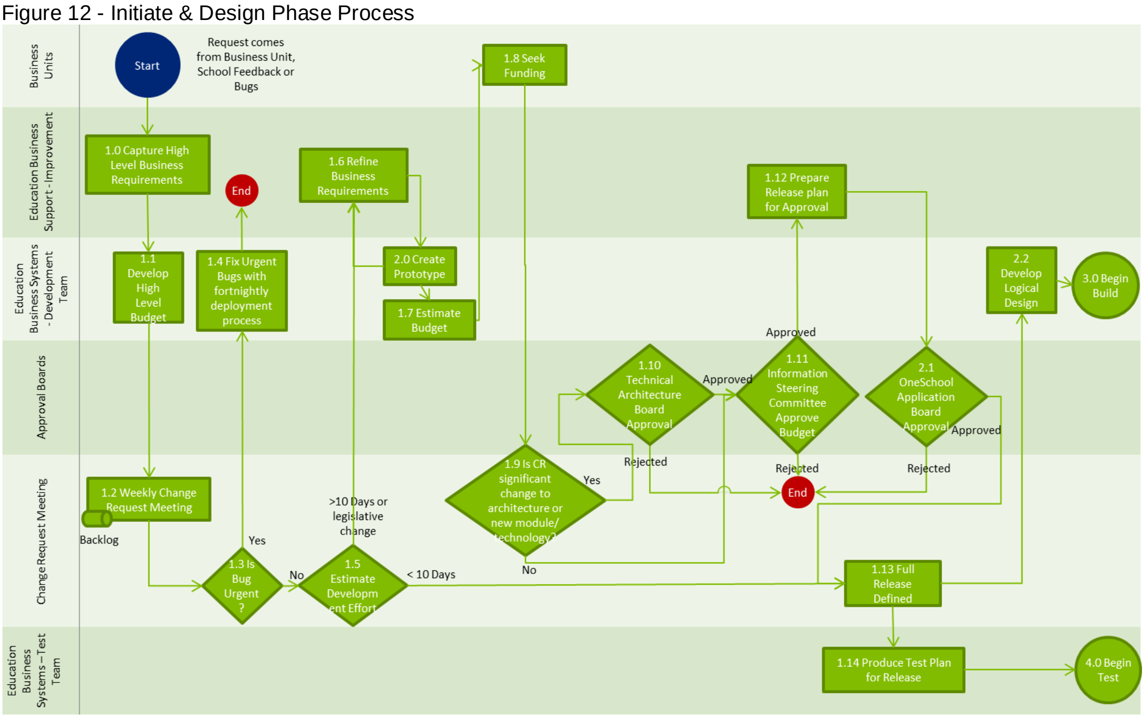
Initiate and Design

The 'initiate' and 'design' phases are intertwined in the beginning of the SDLC process as approval is attained as the design and requirements are refined.

The 'initiate' phase focuses on working with stakeholders to gather, identify and collate requirements and estimate the effort involved in each change. The budget is developed and approved by the Innovation & Information Steering Committee.

The 'design' phase focuses on transforming the business requirements into detailed logical design and prototyping. After final approval is attained to develop the changes from the OneSchool Application Board, the development of the test plan starts in parallel with the Build phase.

Figure 12 - Initiate & Design Phase Process



Business Units
Education Business Support - Improvement
Education Business Systems - Development Team
Approval Boards
Change Request Meeting
Education Business Systems – Test Team
Start
Request comes from Business Unit, School Feedback or Bugs
1.0 Capture High Level Business Requirements
End
1.6 Refine Business Requirements
1.8 Seek Funding
1.12 Prepare Release plan for Approval
1.1 Develop High Level Budget
1.4 Fix Urgent Bugs with fortnightly deployment process
2.0 Create Prototype
1.7 Estimate Budget
2.2 Develop Logical Design
3.0 Begin Build
Approved
1.10 Technical Architecture Board Approval
Approved
1.11 Information Steering Committee Approve Budget
2.1 OneSchool Application Board Approval
Approved
Rejected
Rejected
Rejected
1.9 Is CR significant change to architecture or new module/ technology?
Yes
No
End
1.2 Weekly Change Request Meeting
Backlog
Yes
1.3 Is Bug Urgent ?
No
>10 Days or legislative change
1.5 Estimate Development Effort
< 10 Days
1.13 Full Release Defined
1.14 Produce Test Plan for Release
4.0 Begin Test

The steps shown in the figure above are described in further detail in the following table.

Table 10 - Initiate & Design Process Activities

ID	Activity	Description of Activity
1.0	Capture High Level Business Requirements	New change requests can be originated from the Business Units directly, via feedback from the schools or as a bug raised through the Support & Operate process. The Level 3 Support/SME teams will work with the business to understand the requirements. For large changes a requirements document is produced by a Business Analyst from the business units external to OneSchool or the internal OneSchool Education Business Support team. Requirements for smaller changes are typically documented via emails and word documents exchanged by email and then logged into TFS.
1.1	Develop High Level Estimation	High level effort estimates are provided by the development team. Additional conversations with the originator of the request can occur to provide further clarity and accuracy for the estimates.
1.2	Weekly change request	Weekly change requests are held to review and prioritise the development of all change requests and to decide which changes need to go to the OneSchool Application Board for approval. Small changes that do not require board approval will be discussed, prioritised and planned for delivery. Depending on urgency and capacity to deliver they will be included in the current release or postponed for future releases.
1.3	Is Bug Urgent?	If the request is a 'bug' that needs to be fixed as a matter of urgency then the fix will be developed by the Development team and deployed into production as part of the fortnightly deployment process.
1.4	Fix urgent bugs using fortnightly deployment process	The development team will develop and test a fix and deploy into production as part of the fortnightly deployment process. This process is an expedited version of the overall SDLC.
1.5	Estimate Development Effort	The development team refines the effort estimation based on the refined requirements and additional prototype (if appropriate). If development takes less than 10 days, it will be prioritised and planned by the change request meeting. If a change is expected to take longer than 10 days, or requires a legislative change, it will need to follow the Application Board approval process.
1.6	Refine business requirements	If required, the business requirements will be refined before final estimation of effort is provided. For new functionalities/modules, prototyping can be done by the development team to facilitate understanding of requirements. The business unit will generally be requested to formally approve documented requirements. However, the maturity of the business unit involved in ICT projects can at times constrain the ability of Education Business Support to obtain formal approval.

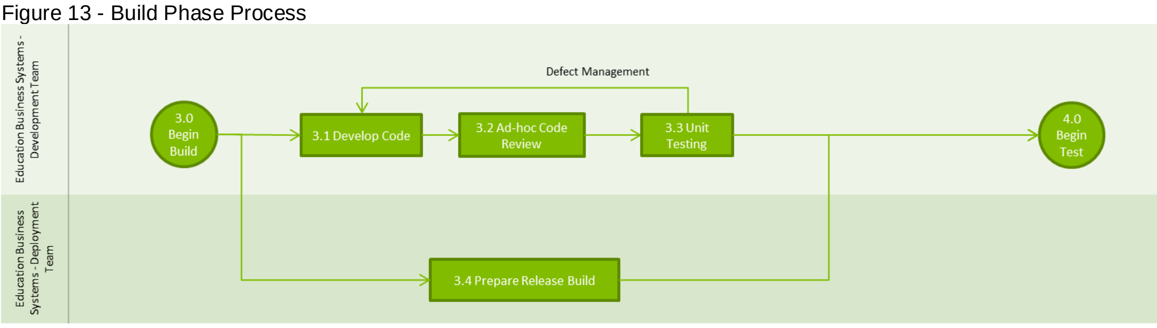
1.7	Develop prototype	If the change request will deliver significant new functionalities or modules, a prototype might be created and socialised with users to support requirements definition and validation. This prototype is also used to support the development team defining the logical design. This will occur iteratively with the refinement of the business requirements.
1.8	Seek Funding	Business requirements and budget are provided to the requesting business unit so they can submit a funding request to the Innovation & Information Steering Committee. Alternatively projects can be self-funded by the business.
1.9	Is change request significant change to architecture or new module/ technology?	If the change has a significant impact on the DET ICT architecture or requires the implementation of a new architecture, the change will need to be endorsed by the Technical Architecture Board prior to submission to the Innovation & Information Steering Committee. This board will be focused on reviewing the high level solution design and how it aligns with the overall DET architecture.
1.10	Technical Architecture Board Approval	Technical Architecture Board approves or rejects change design.
1.11	Innovation & Information Steering Committee Approve Budget	Innovation & Information Steering Committee approves or rejects budget request for change. If approved the committee will commence monitoring project delivery and providing input into Whole of Government ICT dashboard reporting.
1.12	Prepare release plan for approval	Release plan for new large changes is created and submitted to the OneSchool Application Board for final approval to implement.
1.13	Full Release Defined	After OneSchool Application board approval is provided, the change request defines the next full release to be built, tested and deployed adding any small change request/bug fixes are added to the release plan that did not require OneSchool Application Board approval.
1.14	Produce Test Plan for Release	As soon as the release is approved the Testing team commence the preparation of the Test Plan and Test Scripts to test the functionalities that have been approved. The Test Plan will outline which change requests will be tested (and any that might not be tested), the test approach, the Test Pass/Fail criteria and the testing responsibilities (i.e. who is going to test each change request). The testing responsibilities are assigned based on capacity within the Testing team. Given the limited capacity, some change requests are assigned to the Education Business Support team for testing.
2.1	OneSchool Application Board Approval	OneSchool Application Board provides final approval for change to be developed.
2.2	Develop logical	The Development team develops the logical design based on the

	design	business requirements determined and approved by the OneSchool Application Board. The logical design is not formally reviewed by the business unit or Education Business Support team. However, if appropriate, it might be socialised with these teams to ensure the development team correctly understands the requirements. Depending on the size, type of functionality and urgency or other criteria, the requirements gathering, prototyping and logical design can occur before board approval or can be phased across different releases. For example, during one cycle only the requirements of requirements might be completed for a specific change, for the next cycle prototyping might be complete and for the next cycle a logical design might be delivered. For a typical change, however, Requirement Gathering and Prototyping (if required) will occur before board approval and logical design will be completed after board approval.
3.0	Begin Build	Build Phase begins.
4.0	Begin Test	Test Phase begins with preparation of plans and scripts while Build Phase is executed.

Build

The ‘build’ phase focuses on building the required functionality whilst adhering to the specification and design created in the ‘design’ phase. This phase includes software code development, build preparation and deployment to the User Acceptance Testing (UAT) Environment (see ‘test’ phase for further information).

Figure 13 - Build Phase Process


Education Business Systems - Development Team
Education Business Systems - Deployment Team
Defect Management
3.0 Begin Build
3.1 Develop Code
3.2 Ad-hoc Code Review
3.3 Unit Testing
4.0 Begin Test
3.4 Prepare Release Build

The steps shown in the figure above are described in detail in the following table.

Table 11 - Build Process Activities

ID	Activity	Description of Activity
3.0	Begin Build	Build Phase Begins.
3.1	Develop Code	New code is written and old code is modified to implement new functionality or fix bugs.
3.2	Ad-hoc Code Review	New and modified code is reviewed by peer developers on an ad-hoc basis. This review does not happen in every instance, nor is it a

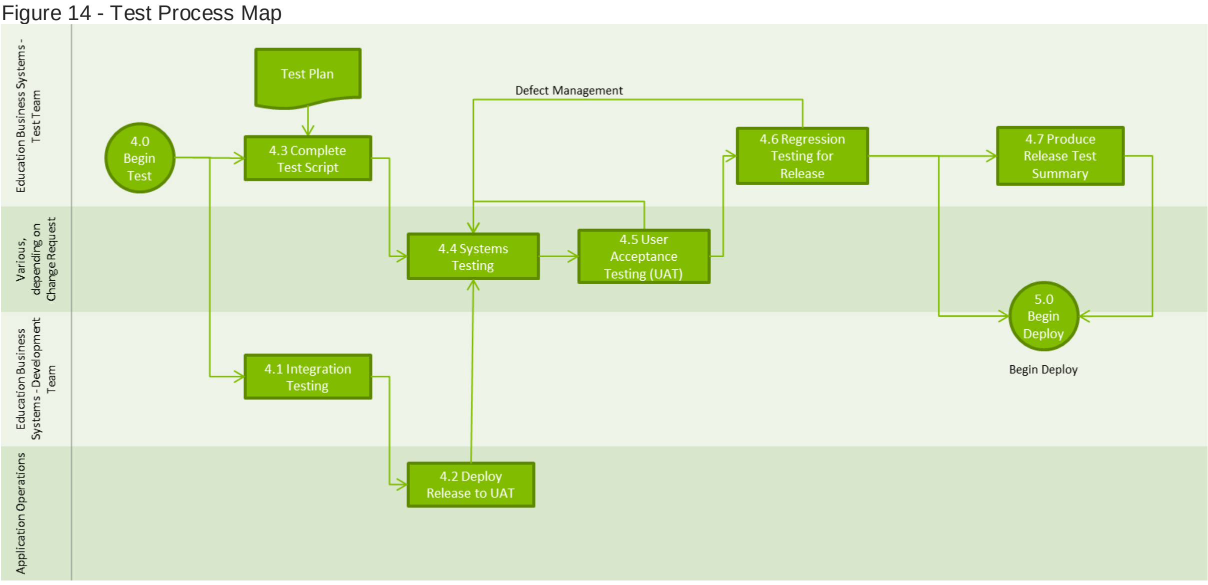
		formalised process. Code review does typically occur when the functionality has been developed by junior resources.
3.3	Unit Testing	After development has finished, the developer begins their own testing of the components changed, this is referred to as “Unit Testing”. Unit testing does not follow a formal testing process nor is it always documented or evidenced.
3.4	Prepare Release Build	The release build is compiled in parallel with the code development to prepare for deployment to the relevant testing environments.
4.0	Begin Test	Begin Test Phase.

Test

This phase focusses on the execution of testing activities and collation of test results into an approved test summary in order to ensure the developed system complies with the specifications and design. The tests performed include:

- **Integration Testing:** Ensures that the individual components and modules interact and perform as expected by the requirements and specifications
- **Systems Testing:** Ensures that the application as a whole complies with the requirements and specifications as a system
- **User Acceptance Testing:** Ensures that the application supports the functionality expected by the end users
- **Regression Testing:** Ensures that there have been no adverse effects on other parts of the application as a result of the changes and bug fixes applied.

Figure 14 - Test Process Map


Education Business Systems - Test Team
Various, depending on Change Request
Education Business Systems - Development Team
Application Operations
Test Plan
Defect Management
4.0 Begin Test
4.3 Complete Test Script
4.6 Regression Testing for Release
4.7 Produce Release Test Summary
4.4 Systems Testing
4.5 User Acceptance Testing (UAT)
5.0 Begin Deploy
Begin Deploy
4.1 Integration Testing
4.2 Deploy Release to UAT

The steps shown in the figure above are described in detail in the following table.

Table 12 - Testing Process Activities

ID	Activity	Description of Activity
4.0	Begin Test	Testing Phase Begins.

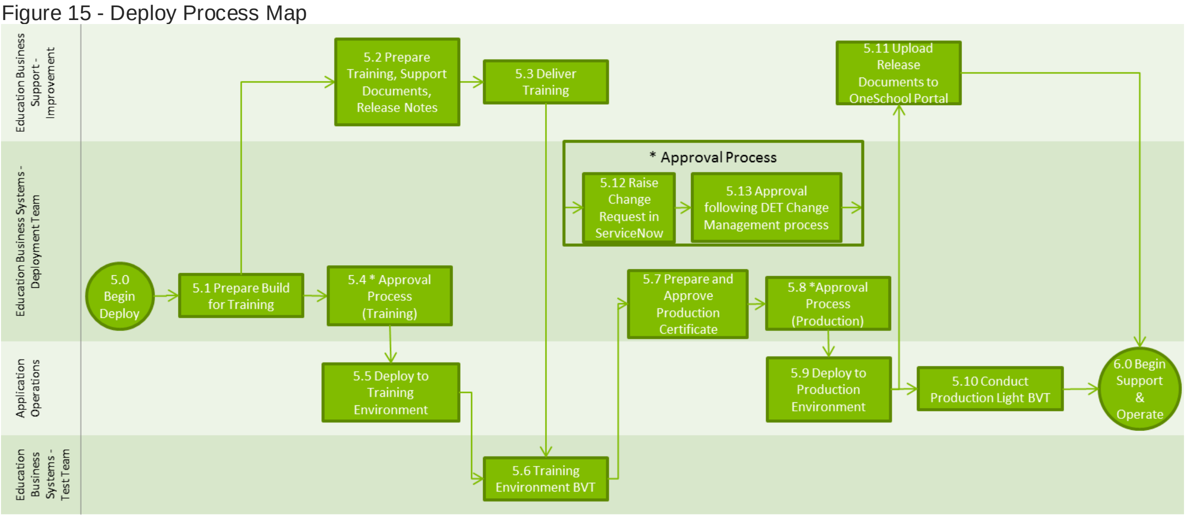
4.1	Integration Testing	For larger/more complex releases additional integration tests can be conducted by the development team manager after all individual unit tests are finalised to ensure that the components and modules interact and perform as expected.
4.2	Deploy Release into UAT	Release is deployed into UAT to begin Test Phase.
4.3	Complete Test Scripts	The testers prepare test scripts for the change requests assigned to them describing what functionality needs to be tested, how it is to be tested and the expected results of the tests. The tester uses the documented requirements and additional conversations with the Development team, L3 Support/SMEs and/or business unit to define the test scripts. The test scripts are not reviewed by the test lead, the business units external to OneSchool or the internal OneSchool Education Business Support team. Test Scripts are not formally developed for change requests that are tested by teams other than the Testing team (e.g. the ones that are tested by the internal OneSchool Education Business Support team).
4.4	Systems Testing	Systems testing is performed to ensure that the different changes that have been developed comply with the requirements and specifications as a system. The execution of system testing follows the test scripts previously prepared if they are executed by the Test team. If they are executed by the Education Business Support Team or Business Units no formal scripts are typically followed. No evidence of the execution of the tests is formally collected or documented.
4.5	User Acceptance Testing (UAT)	UAT is performed by the Business Units to ensure that the application is aligned with requirements. Sometimes UAT is performed by the Education Business Support team or the Testing team. No formal scripts are defined or followed, neither is test evidence collected. The Testing team will seek acceptance of the UAT from the Education Business Support team.
4.6	Regression Testing for Release	Regression testing is performed to ensure there have been no adverse effects on other parts of the application as a result of the changes and bug fixes applied. Regression Testing is manually performed by the testing team and typically takes 1-2 weeks.
4.7	Produce Release Test Summary	Test results from the integration testing, UAT and regression testing are compiled into a document to demonstrate that the tests have been completed and the application adheres to the requirements and specifications. Test summaries are reviewed and approved as part of the Production Certificate approval (see deploy phase). However,

		neither the Business Units nor the OneSchool Application Board are requested to approve the Test Summary.
5.0	Begin Deploy	Begin Deploy Phase.

Deploy

During this phase, the application is initially deployed to the Training Environment for training and Build Verification Testing (BVT). The application is then deployed to the Production Environment after a production deployment certificate and appropriate change management approval has been attained.

Figure 15 - Deploy Process Map


Education Business Support - Improvement
Education Business Systems - Deployment Team
Application Operations
Education Business Systems - Test Team
5.0 Begin Deploy
5.1 Prepare Build for Training
5.2 Prepare Training, Support Documents, Release Notes
5.3 Deliver Training
5.4 * Approval Process (Training)
5.5 Deploy to Training Environment
5.6 Training Environment BVT
5.7 Prepare and Approve Production Certificate
5.8 *Approval Process (Production)
5.9 Deploy to Production Environment
5.10 Conduct Production Light BVT
5.11 Upload Release Documents to OneSchool Portal
* Approval Process
5.12 Raise Change Request in ServiceNow
5.13 Approval following DET Change Management process
6.0 Begin Support & Operate

The steps shown in the figure above are described in detail in the following table.

Table 13 - Deploy Process Activities

ID	Activity	Description of Activity
5.0	Begin Deploy	Begin Deploy Phase.
5.1	Prepare Build for Training	Prepare build and release notes for deployment into Training Environment.
5.2	Prepare Training, Support Documentation and Release Notes	Prepare training material to educate support staff and end users on new or altered functionality. Prepare support documentation to help support teams assist end users as part of their day to day activities. Release notes are also produced to inform end users and the support team of the new functionality constituting the new release. Links to additional information and support documentation are included within the release notes.
5.3	Deliver Training	Deliver training either in person or electronically. Training can sometimes be delivered directly by the Business Units. Depending on the readiness of the impacted users, training can sometimes be delivered in the Production Environment after the release

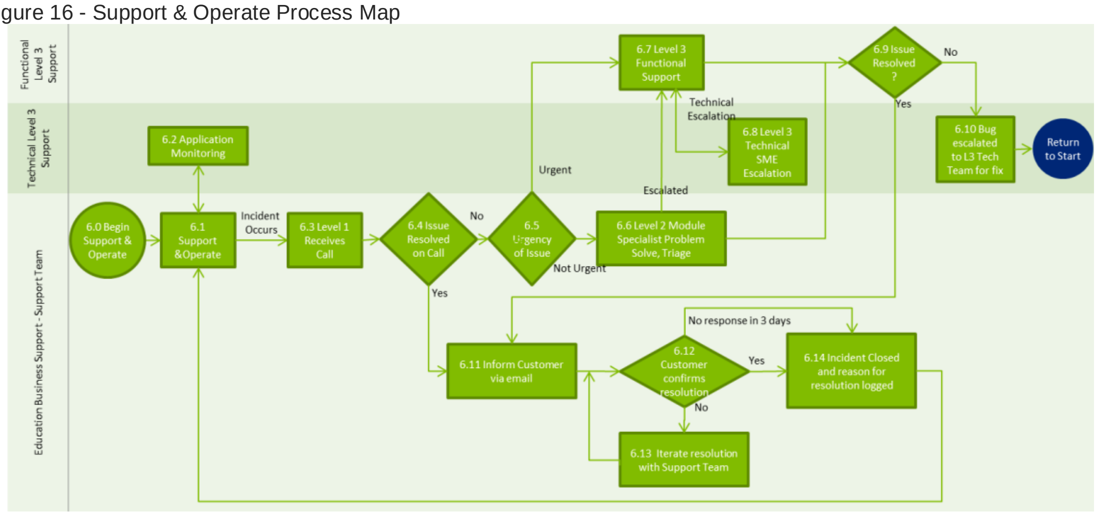
		is deployed.
5.4	Approval Process (Training)	Follow the formal DET change management process for deployment into the Training Environment. A change request is logged in ServiceNow to start the approval process for the OneSchool release (the release is approved as a whole). The Change Manager will review the change request and identify any missing information. The change request will be submitted to the correct Change Management Board for approval. OneSchool releases are typically classified as Level 2 changes that require Change Advisory Board approval.
5.5	Deploy to training Environment	Updated application is deployed to the Training Environment.
5.6	Training Environment BVT	BVT is performed to verify if the build has been correctly deployed into the Training Environment. The BVT is a subset of the regression testing and is focused on testing to ensure the key modules and main functionalities are working.
5.7	Prepare and Approve Production Certificate	A Production Certificate is produced before approval for production deployment is obtained. This certificate is prepared by the Development team and covers the following areas: • Has the release been approved by the OneSchool Application Board? • Has system testing been completed with no outstanding critical/high/normal bugs? • Has the deployment process been agreed and documented and the right resources exist to execute the process? • Has the release time been agreed and dependencies from other releases managed? • Have the application users been notified of proposed outages? • Has a roll back plan been defined? • Are the right resources in place to support the change and have they been appropriately trained? The Production Certificate needs to be ultimately approved by the CIO after the impacted ICT Directors have provided their approval.
5.8	Approval Process (Production)	Formal DET Change Management process followed for deployment into Production Environment. This is similar to the approval process for training described above.
5.9	Deploy to Production Environment	The updated application is deployed to the live Production Environment.
5.10	Conduct Production Light BVT	A small subset of BVT is executed to test the key modules are working.
5.11	Upload Release Documents to OneSchool Portal	Release documents are uploaded to the OneSchool portal to inform end-users and support teams of release details.
5.12	Raise Change Request in	Change request submitted via ServiceNow to begin the Change

	Service Now	Management process that applies to ICT changes across DET.
5.13	Approval following DET Change Management Process	Change request must follow approval process as defined by DET in 'ICT Change Management Process Specification'.
6.0	Begin Support & Operate	Begin Support & Operate Phase.

Support & Operate

This phase involves the operation and maintenance of the application including Level 1, 2 and 3 support, incident management and resolution management. The application is monitored and issues are proactively detected and managed as part of this process.

Figure 16 - Support & Operate Process Map


Functional Level 3 Support
Technical Level 3 Support
Education Business Support - Support Team
6.0 Begin Support & Operate
6.1 Support &Operate
6.2 Application Monitoring
Incident Occurs
6.3 Level 1 Receives Call
6.4 Issue Resolved on Call
No
Yes
6.5 Urgency of Issue
Urgent
Not Urgent
6.6 Level 2 Module Specialist Problem Solve, Triage
Escalated
6.7 Level 3 Functional Support
Technical Escalation
6.8 Level 3 Technical SME Escalation
6.9 Issue Resolved ?
No
Yes
6.10 Bug escalated to L3 Tech Team for fix
Return to Start
6.11 Inform Customer via email
No response in 3 days
6.12 Customer confirms resolution
Yes
No
6.13 Iterate resolution with Support Team
6.14 Incident Closed and reason for resolution logged

The steps shown in the figure above are described in detail in the following table.

Table 14 - Support & Operate Process Activities

ID	Activity	Description of Activity
6.0	Begin Support & Operate	Begin Support & Operate Phase.
6.1	Support & Operate	Business support and operation of OneSchool.
6.2	Application Monitoring	Different levels of application monitoring are performed by the Education Business System team: • Batch processing results are monitored in the beginning of the day and technical and/or functional activities are triggered in case any issue is identified • The OneSchool email inbox is monitored for any Non Delivery-Reports and Failure-to-send notification. If any notification is received it is forwarded to the Education Business Support team for follow up with the business • The Compuware monitoring tool is used to monitor in real time

		the performance of the application. Technical activities are triggered when issues are identified. Infrastructure monitoring is also performance by the Platform Operations team.
6.3	Level 1 Receives Call	All calls are first received by the Level 1 Support team who log the call, try to resolve and, if not able to resolve, escalate the issue to Level 2. Issues are logged and tracked in ServiceNow.
6.4	Issue Resolved on Call?	If the issue is resolved on the first call it is considered "fixed on first contact" and the user is notified of the resolution.
6.5	Urgency of Issue	Urgency is assessed by using criteria based on the type of phone call, nature of call, release version and time of year. Some issues are automatically escalated to Level 3 support, such as administration and security in the Finance module.
6.6	Level 2 Module Specialist Problem Solve, Triage	If the issue is not urgent it is passed to the Level 2 support team which is staffed by SME specialists for the various OneSchool modules. They either fix the issue or escalate to Level 3 Support.
6.7	Level 3 Functional Support	Level 3 support consists of further OneSchool module SMEs who will either resolve the issue or escalate to the technical support team (i.e. Education Business Systems) for further diagnosis and resolution.
6.8	Level 3 Technical SME Escalation	The Level 3 Functional Support will try to fix the issue. If the resolution requires input from a technical SME, it will be escalated to the Level 3 Technical Support for further assessment or resolution.
6.9	Issue Resolved?	If the issue is resolved, the business user will be informed. If not, it is escalated to the technical team (i.e. Education Business Systems) for further diagnosis. Depending on complexity and duration of investigation, a solution might be published on the support website describing a temporary workaround or bug fix.
6.10	Bug escalated to L3 Tech team for fix	The Level 3 Functional Support will try to fix the issue. If the resolution requires change to the application code, then a bug fix will be raised in in MS Team Foundation Server (TFS) for discussion in the Weekly Change Request Meeting. The process progresses to the 1. Initiate & Design phase.
6.11	Inform Customer via email	Customer is contacted via email to notify them that the problem has been fixed.
6.12	Customer Confirms Resolution	If the customer is satisfied with the resolution, or if no response is received within 3 days, the issue is logged and closed. If the customer is not satisfied with the resolution, there is a follow up to attempt to try to fix the issue to their satisfaction or to refer elsewhere.
6.13	Iterate resolution with Support team	If the customer is not satisfied, the issue can be iterated together with the Support team until an appropriate resolution is reached.
6.14	Incident Closed and reason for resolution logged	Issue is closed in ServiceNow and the description of the issue and resolution is logged within the relevant ticket. If a pattern of similar issues has been observed, a Knowledge Base Article (KBA) will typically be created to support the resolution of future

	similar issues. Team leaders are responsible for reviewing incident closures. However, this is not a formal process step or responsibility. The user that raised the issue also has the opportunity to confirm if the resolution steps provided solved the particular issue. If not, the user can revert back to the support team asking for further help.

Coordinate & Manage

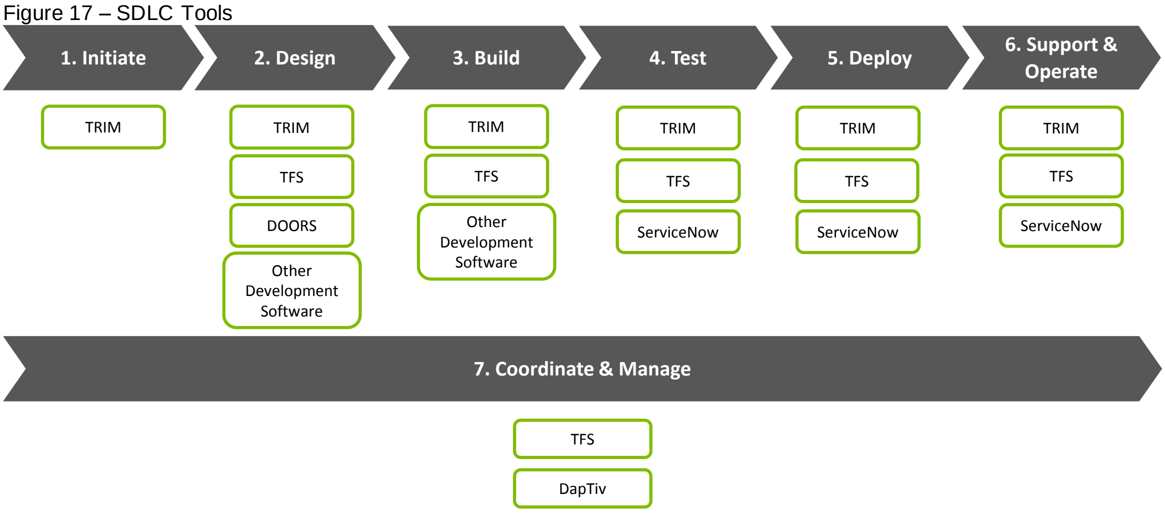
For smaller changes categorised as “Business as Usual” the overall coordination of the development of a OneSchool release is performed by the Education Business Support and System team. This does not follow a documented procedure as there are no formal mechanisms to track progress and/or escalate risks/issues.

Individual change requests can be managed as projects if they are large enough and require additional funding (see ‘initiate’ and ‘design’ phases). In this case, the business unit performs the Project Management role and is responsible for the end-to-end coordination and reporting of the specific change request and for following the steps described in the ICT Project Management Framework. Education Business Support and System teams support the Business Units in their Project Management role and provide technical documentation as requested.

5.2.4 Tools

The SDLC was assessed from this perspective by examining the software tools used throughout the life cycle including those involved in testing, document management, requirements gathering, and service management. These tools are used across the SDLC phases as shown in the following diagram. The main tools used throughout the SDLC are outlined below, and a complete list of the tools in use is provided in Appendix D.

Figure 17 – SDLC Tools



Key tools used in the SDLC:

- **TRIM*:*** Document management system used across the Queensland Government for workflow tracking, approval documentation and version control. It is used across the SDLC phases to track the various approvals involved in the change request process.
- **IBM Rational DOORS*:*** Requirements management application used for requirements communication, collaboration and verification. DOORS can be used for both requirements management and logical design. This tool is not currently being used for requirements management but logical designs are still being updated.

- **Microsoft Team Foundation Server (TFS):** Provides source code management, release management, change request workflow management and management of development team pipeline of work across the SDLC. TFS is used from the design phase onwards.
- **ServiceNow:** IT Service Management, workflow management and change management tool used across the OneSchool SDLC phases. ServiceNow is used in the Test, Deploy and Support & Operate phases to manage the changes required to implement the new code releases and to track support requests.
- **DapTiv:** Project Management tool that is used to report progress of OneSchool projects. Reporting within Daptiv is performed by the relevant business unit project manager. It is understood that Daptiv has been relatively recently implemented in 2015.
- **Other Development Software:** A range of tools used in development, debugging, testing and code management. See Appendix D for further detail.

5.3 Findings

The findings presented in this section were derived from the analysis of the current operating model against DET standards and industry good practices (see section 5.1.3 for further details). Similar to the current state section the findings are organised in accordance with the following four dimensions of analysis, Organisation, Governance, Process and Tools.

5.3.1 Organisation

Table 15 - Organisation Findings

ID	Finding	Implication
F1.1	There is no individual within the OneSchool team with responsibility for the coordination and end-to-end delivery of a OneSchool release	The lack of an individual with the responsibility of the coordination and end-to-end delivery of the OneSchool release may result in misalignment between the developed solution and business expectations, ineffective risk management, delays and higher costs to deliver the release.
F1.2	No dedicated Business Analysts or Technical Project Managers roles have been identified within the OneSchool team. For larger change requests some of these roles are occasionally filled by external resources contracted specifically for the project and typically funded by the business.	Absence of a dedicated Business Analyst capability can lead to: • Risk of business needs not being well understood or appropriately translated and captured into business requirements and functional specifications in a manner that can be clearly understood by the development team to inform their build activities • Inefficient functional validation of business requirements during testing phases. Absence of a dedicated Technical Project Management capability can lead to: • Poor alignment to and management of ICT projects in accordance with good practice SDLC • Technical aspects of the change not being managed with the appropriate rigour which in turn can lead to cost, budget and quality deviations. • Inefficient hand-overs and limited end-to-end accountability due to lack of appropriate

		management and coordination of technical teams.
F1.3	Responsibilities between the Education Business Support, Education Business System and the Business Unit teams are not always clear (i.e. who is responsible for the end-to-end delivery and who is responsible for systems testing and UAT).	Without clear responsibilities and accountabilities for the OneSchool release inconsistencies can potentially arise in the management of the development and the resultant quality of the software delivered. This can lead to delays, delivery misalignment with business requirements and the risk of key SDLC steps not being executed or executed without appropriate quality and structure (e.g. UAT).

5.3.2 Governance

Table 16 - Governance Findings

ID	Finding	Implication
F2.1	Limited formal governance mechanisms have been identified to monitor the delivery of the OneSchool releases and monitor the delivery of individual change requests (i.e. project board).	There is potential for late identification of risks and issues that ultimately, if not solved in time, may lead to impacts on cost, timelines and quality of delivery. There is potential for misalignment between what the release will deliver and the business/sponsors expectation.
F2.2	Limited formal governance mechanisms have been identified to review and approve the functional and technical design of the solution.	There is potential for the solution to be designed in a way that does not fully address business requirements, is not aligned with DET ICT architecture principles or fails to be technically robust, secure, and easy to interoperate and/or maintain.
F2.3	There is no documented end-to-end procedure for delivering OneSchool releases that outlines clear responsibilities, documentation requirements and necessary approvals.	There is potential for inconsistency, inefficiency, key person dependencies and key steps being missed through the different development phases. Budget over-runs, delays and or unanticipated business impacts due to lack of consistency and accountability.
F2.4	Some DET wide frameworks and methodologies are in place (i.e. ICT Project Management, DET SDLC) but it is not clear how they should be followed by OneSchool.	There is potential for different frameworks, or no frameworks to be followed by OneSchool. This may lead to inconsistent and inefficient development and miscommunications between DET ICT teams. This could consequently impact the quality, cost and budget of OneSchool development.
F2.5	The DET SDLC Framework is focused on coding/architectural standards and provides limited guidance for the execution of the process itself (i.e. what steps need to be followed by who, what documentation needs to be provided, what approvals need to exist, etc.). This framework has not been updated since 2011 (even though there is an update process ongoing) and is not clearly mandated for use by OneSchool.	There is potential for decreased oversight, accountability, traceability and overall lack of quality of process outcomes. This also increases the likelihood of dependency on key personnel. The fact that these documents are not currently up to date with current industry good practices reduces their likelihood of adoption by the teams. This in turn could increase the gap between documented and actual processes, leading to confusion of responsibility and accountability.
F2.6	The ICT Project Management Framework doesn't provide clear direction for the level of documentation and sign-off required for different projects of different sizes and risk profiles. This is left to the	There is potential for reduction in clear project direction, oversight, traceability and consistency that can lead to overall reduction in quality of delivery.

	discretion of the Project Board and therefore applied inconsistently.	

5.3.3 Process

Initiate

Table 17 - Process Findings: Initiate

ID	Finding	Implication
F3.1	Formal risk assessments do not appear to be consistently performed for all change requests, despite this being mandated by the OneSchool Application Board guidelines.	There is potential for limiting the ability of OneSchool Application Board to adjust the level of formal governance required, assure quality and monitor progress of each change request. Similarly, this limits the ability of the OneSchool teams to adjust the operational processes to the perceived risk of each change request.
F3.2	The mechanism in place for the prioritisation and endorsement of small change requests (less than 10 days of development effort), lacks formality and governance.	There is potential risk of approving changes that are not aligned with broader DET strategic goals or allowing lower priority changes to take precedence over more important business requests. There is potential for limited business change impact analysis that could lead to issues impacting business unit operations. There is potential for lack of control and governance derived from the limited visibility of the Application Board over these approvals.

Design

Table 18 - Process Findings: Design

ID	Finding	Implication
F3.3	There is not a documented process describing how to define, document and sign-off requirements (both functional and technical). Requirements are created with varying degrees of detail and with inconsistent formats that are not well understood by business and IT. For example, many requirements are captured within emails.	There is potential to affect the ability of other teams involved in the process (e.g. developers, testers) to clearly understand the business requirements and design, develop and validate them effectively and efficiently. This can potentially lead to inefficiencies, miscommunications and ultimately to solutions that don't meet business requirements. Constrains the ability to trace other software development artefacts (e.g. design, code, tests) back to requirements that in turn limits the ability to ensure the solution is accurate and complete (i.e. meets all business requirements).
F3.4	The Business Units find it difficult to understand and sign-off the logical design because it is written using highly technical language.	There is potential risk that the proposed design does not align with the business requirements. This might result in re-work or in a solution that does not meet business requirements and therefore introduces risks into business processes.
F3.5	There is no design documentation for small change requests (less than 10 days of development effort) and bug fixes.	Constrains the ability of having appropriate governance mechanism to confirm if the technical solution is the most appropriate one. There is potential for limiting the maintainability and traceability of the overall application due to lack of documentation for all changes.
F3.6	The review of the logical design is solely conducted by the Education Business Systems team and fails to leverage any independent governance processes to ensure that the design aligns with DET requirements, ICT architecture principles and good practices. The DET Technical Architecture Board is primarily focussed on the high level architectural governance of the entire DET environment rather than the review of individual technical designs and product development.	There is potential risk that the proposed design does not align with the business requirements or is not aligned with DET architectural standards. This might result in re-work, in a solution that does not meet business requirements or a solution that is not constructed in accordance with DET architectural and security standards.
F3.7	The requirements documentation (when	Requires re-validation of requirements by the development and test teams before and during their work. This leads to

	produced), is not always updated to reflect requirement changes during the development of the release. This should be considered a live document for final approval.	inefficiency and increases the risk of errors due to development/test of incorrectly documented requirements.

Build

Table 19 - Process Findings: Build

ID	Finding	Implication
F3.8	No formal criteria exist which describe when code reviews should occur.	Without a formal code review (in-particular for the high risk change requests), there is an increased chance that mistakes made in the initial ‘build’ phase are overlooked, reducing the overall quality of the application and resulting in bugs needing to be identified and resolved in later phases of the release.

Test

Table 20 - Process Findings: Test

ID	Finding	Implication
F3.9	An inconsistent approach is followed for the delivery of the different types of testing (i.e. integration, system and UAT). This varies per change request and in some instances is not done at all.	Without a clearly documented responsibility matrix for the delivery of testing, there is an increased likelihood that the test objectives will not be met and that the approach taken to conduct the tests is inconsistent, resulting in incorrect results.
F3.10	There is no consistent process to execute and document testing. The process varies depending on the team conducting the test.	Without a consistent approach taken to execute and document testing, there is an increased chance of misleading test results (such as false-positive results) and an inability to track test results and validate that test cases were successfully executed.
F3.11	Formal test cases (i.e. description of acceptance criteria, test scenarios and expected results) are only done for the tests executed by the test team (i.e. not done for tests executed by the Education Business Support team) and are not reviewed by anyone apart from the tester that wrote the test and conducted the test case.	Limits the ability to verify if the tests have the appropriate level of quality and enough coverage. Increased difficulty of independent review and provision of confirmation that tests are being correctly executed.
F3.12	Evidence is not consistently collected to demonstrate that tests have been executed and to support the test results	Increases difficulty of independent validation of test execution and results. This can lead to unexpected bugs in the live Production Environment and a solution that is not aligned with business expectations.

F3.13	External business unit involvement in testing is limited and varied. When the external business units are involved, the testing that takes place is typically unstructured and limited to exploratory testing (i.e. limited testing and focused on experimenting the system without a structured script).	In the instances where User Acceptance testing cannot be handled by the internal Oneschool Education Business Support team, this could constrain the ability of the external business to confirm if the system is operating in accordance with their expectation and is aligned with the documented and agreed requirements. Furthermore, this may lead to a higher risk of unexpected bugs being migrated into the live Production Environment.
F3.14	The test summary document which outlines the results of the different phases of testing is not being reviewed and formally endorsed by the OneSchool Application Board despite being mandated by the *"OneSchool Application Board – Operating Guidelines and Procedures."*	Prevents the board from having visibility and oversight over the quality and completeness of the tests performed and relevant outstanding bugs. This also limits the accountability of the board regarding the quality of the changes that are deployed in the Production Environment.
F3.15	There is no formal post deployment testing completed for high priority change requests. Only a limited release verification test is conducted to confirm that the key modules are working and that records can be accessed.	Potential risk for bugs in Production Environment to be discovered late if the functionalities are not used for a period of time or if undesired system behaviours are not easily detectable.
F3.16	Regression testing is performed manually and, in some instances, regression testing needs to be done incrementally to account for delays in the completion of system and user acceptance testing (i.e. partial regression testing might be performed due to late changes in software functionality)	A significant amount of time is spent on conducting manual regression testing (approximately 2 weeks for every release) that could be used for additional system testing and support of UAT if the level of testing automation was increased. Incremental regression testing (as opposed to a full regression test before deployment) increases the chance of faults being missed which may lead to failures in the live Production Environment.

Deploy

Table 21 - Process Findings: Deploy

ID	Finding	Implication
F3.17	The Change Advisory Board approval (including Production Readiness) of deployment occurs at the release level without explicit review of the individual change requests within the release.	There is potential risk that issues associated with high-risk changes are overlooked due to the fact the assessment is performed at the release level and does not explore the individual change requests within the release. It is not expected that the Change Advisory Board would be able to ascertain if a change had incorrectly passed testing.

F3.18	The OneSchool Application Board does not approve a release (including final scope and proposed changes) before it is deployed into the Production Environment.	Prevents the board from providing a final set of checks and balances regarding readiness and level of business impact for the release to be deployed.

Support & Operate

Table 22 - Process Findings: Support & Operate

ID	Finding	Implication
F3.19	There is some technical monitoring of the operation of the OneSchool application. However this is performed without procedures formally defined/followed and responsibilities clearly assigned.	Decreases the chances of proactively identifying issues that could be addressed before they impact end users.
F3.20	No documented quality assurance process exists to validate the resolution of incidents. Despite this being the responsibility of the Level 3 support team there are no mechanisms in place to ensure that quality assurance is conducted.	Increases the risk of re-occurring incidents due to the fact that the solution might be addressing the symptoms but not the root cause of the issue.
F3.21	There is no consistent problem management process in place to identify recurring incidents and conduct root-cause analysis.	Increases the risk of re-occurring incidents due to the fact the solution might be addressing the symptoms but not the root cause of the issue.

Coordinate & Manage

Table 23 - Process Findings: Coordinate & Manage

ID	Finding	Implication
F3.22	There is no clear accountability or a specific role responsible for the end-to-end delivery of the OneSchool release	The coordination between the SDLC phases can cause misalignment between the solution and business requirements, ineffective risk management and increases the chance of budget overrun and delays in delivery.
F3.23	There are no formally documented procedures in place to report on progress and formally manage risks and issues during a release.	Limited oversight or accountability for effective, timely and functionally correct delivery of the release can lead to significant adverse impacts on budget, cost and quality.
F3.24	The ICT Project Management	The ICT project management framework exists to

	framework is only followed to obtain funding approval for change requests if needed. For the remaining phases, the ICT Project Management Framework doesn’t appear to be followed.	ensure that projects within DET IT Branch are executed effectively with sufficient oversight and planning. By only adhering to the process for the initial phases, the remainder of the project will lack governance and oversight that may lead to ineffective delivery and/or business expectations not being met.

Tools

Table 24 - Tools Findings

ID	Finding	Implication
F4.1	The DOORS tool does not appear to still be consistently used to manage requirements and is now primarily used to store the logical designs for change requests.	Not using a consistent tool to support requirements management may lead to inefficiencies and quality issues in requirements management. These types of tools, when used correctly, typically enhance communication, collaboration, verification and traceability of the requirements management process. This is important in ensuring technology solutions are delivered in line with business expectations.
F4.2	No automated regression testing tools are used.	Without the use of automated regression testing tools, a significant amount of time is spent on conducting manual regression testing (approximately 2 weeks for every release) and the chances of unidentified bugs existing increases. See 3.16 for further implications of manual regression testing.

6 OneSchool Technical Solution Review

6.1 Introduction

The OneSchool system provides Queensland State Schools with a range of information management functionality. The system consists of a number of integrated software modules that work together in order to provide schools with support for:

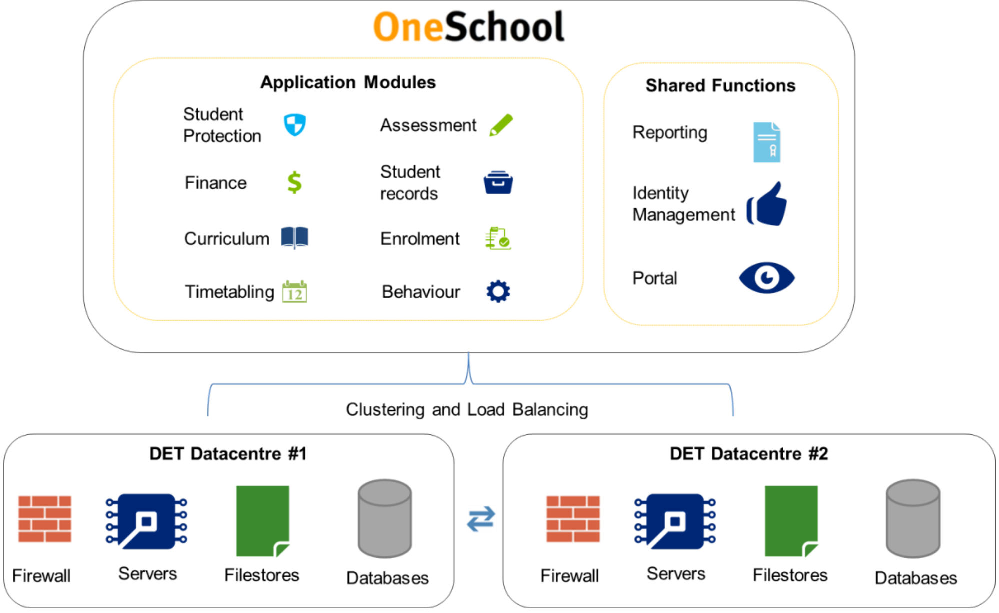
- Student management
- Curriculum and learning management
- Finance and asset management
- Resource management
- Performance, reporting and analysis
- Student Protection

Specifically, the OneSchool SPM facilitates electronic submission of student protection information to the DCCSDS and the QPS as required by legislation and DET's student protection policies.

OneSchool facilitates the automatic pre-population of the SPR's with student information already present within OneSchool. End users access OneSchool via an integrated portal with federated identities managed by the DET. All application actions are performed through the integrated portal.

From an ICT infrastructure perspective, the SPM shares the OneSchool application hosting infrastructure, which includes a cluster of servers physically located across two data centres. Application requests are load balanced across multiple servers. In addition to a reporting server farm, databases and fileservers provide information repository functions which are used by the SPM.

Figure 18 - OneSchool High-Level Technical Overview



6.2 Objectives

Deloitte reviewed the design and implementation of the SPM technical solution with the following specific objectives:

- Consider how the current application meets the core requirements of the DET Child Safety team within State School operations
- Review the application architecture and provide recommendations relating to the manner in which the system:
  - Notifies and records the distribution of child protection reports to external agencies
  - Manages confirmation of receipt of reports from external agencies
  - Records and manages reporting and notification information for audit purpose.

The scope of this review has been restricted to the current functionality of the SPM and excludes any historical changes or review of the wider functionality provided by the other OneSchool Application modules. The objectives listed above are addressed in order within the remainder of this section as follows:

- **Business Requirements:** The functionality that the SPM should provide in order to meet the expectations of the appropriate business stakeholders
- **Application Functionality Review:** Comparison of the SPM software code against the business requirements with associated findings and improvement recommendations
- **Application Architecture and ICT Infrastructure Review:** Assessment of the overarching SPM technical application architecture and underpinning ICT infrastructure with associated findings and improvement recommendations

6.3 Business Requirements

In order to understand whether the SPM currently provides functionality that meets the expectations of the business it was necessary to agree a documented set of requirements (referred to here as the ‘requirements baseline’) with the Department of Education Child Safety stakeholders.

Prior to the construction of the requirements baseline, Deloitte obtained and reviewed available system documentation and met with a number of key OneSchool and DET business stakeholders in order to gain an initial understanding of the technical context of the SPM’s functionality, design and implementation.

The documents reviewed as part of this initial phase are described within Appendix E.

As a result of the document review and the interviews, three different categories of requirements relevant to the SPM were identified:

- **Legislative Requirements:** The business requirements that must be met in order for DET to be compliant with relevant Queensland and Federal legislation. These requirements are divided further into two sub-groups:
    - **Report Generation**: Requirements relating to the creation of SPR’s
    - **Report Delivery:** Requirement relating to the distribution of SPR’s.
- **Core Business Requirements:** Other key pieces of functionality that facilitate the operational activities associated with delivery of the legislative requirements
- **Supporting Requirements:** Additional functionality desired by the business in order to facilitate additional quality assurance and internal reporting but that does not contribute directly to the satisfaction of core business and legislative requirements.

This review has focussed on the exploration of the software code in order to form an understanding of whether the Legislative and Core business requirements described above are met by the SPM. The supporting requirements have been validated with the relevant stakeholders but have been excluded from the detailed application software code review as they are considered lower priority from a business perspective.

6.3.1 Legislative Requirements

Although Deloitte reviewed the relevant legislation and key procedures in order to understand the resultant requirements relevant to the SPM, this review excluded the validation of whether these requirements fully satisfy the legislation.

It should be noted there is a degree of repetition across these requirements as they were derived from different regulatory requirements which occasionally overlap. In the interests of clarity, simplicity and traceability, duplicate requirements have not been merged. A reference identifier (ID) has also been provided for all requirements outlined in this section. This is used throughout this report to provide a link back to the original requirement specifications.

Report Generation Requirements

The table below lists the requirements that guide the categories of data that should be included as part of the generation of a SPR.

Table 25 – Legislative Report Generation Requirements

Legislation reference	Reference	Requirement
Education General Provisions Act 2006 : s.68 Report about sexual abuse—Act, ss 365(3) and 366(3)	**LR1.(a)**	The name of the person giving the report (the first person)
	LR1.(b)	The student’s name and sex
	LR1.(c)	Details of the basis for the first person becoming aware, or reasonably suspecting, that the student has been sexually abused by another person
	LR1.(d)	Details of the abuse or suspected abuse

	LR1.(e)	Any of the following information of which the first person is aware (i) the student's age (ii) the identity of the person who has abused, or is suspected to have abused, the student (iii) the identity of anyone else who may have information about the abuse or suspected abuse.
Education General Provisions Act 2006 s.68A Report about likely sexual abuse—Act, ss 365A(4) and 366A(5)	**LR2.(a)**	The name of the person giving the report (the first person)
	LR2.(b)	The student's name and sex
	LR2.(c)	Details of the basis for the first person reasonably suspecting that the student is likely to be sexually abused by another person
	LR2.(d)	Any of the following information of which the first person is aware – (i) The student's age (ii) The identity of the person who is suspected to be likely to abuse the student (iii) The identity of anyone else who may have information about the suspected likelihood of abuse.
Child Protection Act 1999 - s.13G Report to the chief executive	**LR3.(a)**	State the basis on which the person has formed the reportable suspicion
	LR3.(b)	Include the information prescribed by regulation, to the extent of the person's knowledge
Child Protection Regulation 2011 – s.10 Information to be included in report to chief executive	**LR4.(a)**	The child's name and sex
	LR4.(b)	The child's age
	LR4.(c)	Details of how to contact the child The address at which the child usually lives The name and address of the school the child attends
	LR4.(d)	Details of the harm to which the reportable suspicion relates
	LR4.(e)	Particulars of the identity of the person suspected of causing the child to have suffered, suffer, or be at risk of suffering, the harm to which the reportable suspicion relates
	LR4.(f)	Particulars of the identity of any other person who may be able to give information about the harm to which the reportable suspicion relates

Report Delivery Requirements

The recipients of individual SPR's are determined by the answers to three specific questions that the principal must answer prior to finalising the report.

As previously described, the table below illustrates the business logic that determines the recipients of the SPR's based on the Principal's responses to the three questions. This provides a requirement reference to be used as part of the functionality review.

Table 26 – Legislative Report Delivery Requirements

Question	Action							
Reference #	**LR5.(a)**	**LR5.(b)**			**LR5.(c)**	**LR5.(d)**		
1. Is this report in relation to suspected sexual abuse or likely sexual abuse?	Yes	Yes	Yes	Yes	No	No	No	No
2. Does the information indicate that the student has been significantly harmed or is at risk of significant harm?	Yes	Yes	No	No	Yes	Yes	No	No
3. Based on the available information, do you suspect a parent may be willing and able to protect the child from harm?	No	Yes	Yes	No	No	Yes	No	Yes
Recipient	DCCSDS & QPS	QPS only.			DCCSDS only.	Report will NOT be sent.		

6.3.2 Core Business Requirements

The table below lists additional core business requirements which, although not directly derived from legislation, facilitate operational activities associated with the fulfilment of the legislative requirements.

Table 27 - Core Business Requirements

Reference	Requirement
CR1.(a)	Email reminders to the staff member who commenced the report but have not yet completed it.
CR1.(b)	Email reminders to principal for approval and transmission of the report
CR1.(c)	Acknowledgement to the originator and details of the final status of the report (monitor at school, sent to child safety, sent to QPS or send to both)

6.4 Application Functionality Review

The objectives of the application functionality review of the SPM software code include:

- Validate and provide evidence as to whether the legislative and core business requirements are addressed by the software code
- Highlight any potential gaps in software logic or programming practices
- Identify potential improvements in reporting, notification and audit functions.

6.4.1 Scope

The SPM is an integrated component of the overall OneSchool Application. This means that the module relies on the wider OneSchool application for certain functionality (e.g. internal reporting and retrieval of student demographic information).

In order to constrain the scope of this review and provide the appropriate level of focus on the SPM implementation, it has been assumed that the wider functionality of the OneSchool application is functioning adequately.

6.4.2 Approach

A software code review in isolation does not guarantee that all business requirements are adequately satisfied. Additional QA activities such as unit, regression, integration and user acceptance testing should also be executed in order to provide additional assurance. This has not been undertaken for this review.

Once the business requirements described above were agreed with the Child Safety stakeholders the following steps were undertaken to review the software:

- Review of application design documentation
- Step by step review of SPM software code with OneSchool software development Subject Matter Expert (SME) including:
    - Cross-check of the business requirements against relevant software code
    - Additional review of code fix that was deployed on 30 July 2015 and a high level review of recent changes
- Further detailed review of an extract of the current application software code.

The findings and recommendations resulting from this review are provided here. The detailed analysis with appropriate code references is documented within Appendix G.

6.4.3 Application Code Review Findings and Recommendations

As outlined by the table below, all the legislative and core business requirements appear to be addressed by the SPM software code.

In terms of the functionality of the software, the only additional risk identified is associated with requirements LR5.(a-c) whereby enhancement of the internal error handling may mitigate against future report delivery failures.

There is no evidence that this identified aspect of the software code (LR5.(a-c)) has at any time contributed toward report delivery incident. However, as the software is further developed in the future, the additional rigour will provide an extra level of mitigation against further issues arising (in addition to other software quality assurance and testing steps).

The software review findings are described in detail within Appendix G.

Table 28 - Summary of Requirements Analysis

Reference #	Requirement Addressed
LR1.(a-d)	YES
LR2.(a-d)	YES
LR3.(a-b)	YES
LR4.(a-f)	YES
LR5.(a-c)	YES*
LR5.(d)	YES
CR1.(a)	YES
CR1.(b)	YES
CR1.(c)	YES

* If certain conditions are met there is a risk of requirement not being satisfied. These conditions are listed in the Appendix G

Additional findings and recommendations relating to the Application Code review have been summarised in the table below and grouped into two categories:

- **Business Requirements:** Findings regarding the ability of the software code to meet the requirements
- **Good Practices:** Generic findings regarding how the software code has been structured.

Table 29 - Findings and Recommendations Relating to Application

ID	Category	Area	Finding	Recommendation
1.1	Business Requirements	Report Delivery	The application code in its current state appears to fulfil the legislative and business requirements. However, for requirement LR5(a-c), there is a risk that the application, under specific error circumstances, might fail to perform as desired due to limited error handling code. Refer to Appendix G (Report Delivery) for further information.	Review the software code and test the scenarios identified in Appendix G. Additionally, the error handling within the software code should be enhanced to address the scenarios described.
1.2	Good Practices	Report Generation	Usage of references to obtain mandatory data for the report can increase query complexity and reduce performance.	Consider replicating data in the database to reduce query complexity (and increase query performance) through reduced usage of JOIN commands. This should be assessed on a case by case basis.
1.3	Good Practices	Report Delivery	The review of the code suggests that automated unit tests have not been created to validate business logic. Additionally, the design of the solution doesn't seem to prepare for modular testing.	The solution would benefit from having more automated unit tests to validate key business logic. This would maximise the chances of early defect identification through better regression testing and would also accelerate the testing phase.
1.4	Good Practices	Report Delivery	Maintenance of the software code could be simplified through additional modularisation and increased clarity. Refer to Appendix H for further information	Consider adopting the suggested improvements to increase ease of maintenance.
1.5	Good Practices	Core Requirements	Some of the stored procedures reviewed are extremely complex and include multiple queries with many JOINS, extensive use of temporary tables, cursors and complex string concatenations. This will likely lead to increased maintenance complexity over the lifetime of the system.	Consider having a clearer code design structure to make use of an object relational mapper for interfacing with the database, which will better support a modular design model and improve maintainability.

6.5 Application Architecture and Infrastructure Review

This section summarises the review of the overall application architecture of the SPM and the underpinning email ICT infrastructure.

This review was undertaken in collaboration with DET ICT application and infrastructure SME's. The following sections document recommendations relating to the manner in which the SPM has been architected and how it interacts with various pieces of email infrastructure between OneSchool and the other agencies.

6.5.1 Scope & Objectives

The scope and objectives of this part of the review are as follows:

- **ICT Application Architecture**: Review of the application architecture of the OneSchool SPM with the aim to identifying improvements in security posture, reporting, notifications and audit capability.
- **ICT Infrastructure**: Review of the underlying ICT infrastructure that supports the distribution of SPR's and notifications in order to identify risks relating to these communications.

There are numerous supporting ICT services upon which the OneSchool application is reliant in order to maintain service delivery to school users. Failure of these services could lead to further wide-spread failure of other DET ICT infrastructure and applications, which have not been included within the scope of this review. Examples of these supporting services include:

- Capacity and performance management
- Continuity, disaster recovery and availability
- Shared ICT infrastructure services such as storage and compute.

There is no evidence to suggest there are any aspects of these services could specifically contribute to undetected issues in the distribution of SPR's and so they are not covered in detail within the scope of this review.

6.5.2 Approach

The remainder of this section is structured around the sequential approach taken to address the scope items and objectives described above as follows:

- **Technical Overview of OneSchool System:** A summary of current system synthesised from:
    - Review of high level design and architecture documentation (as detailed within Appendix E)
    - Collaborative workshops with key DET technical staff including OneSchool application SMEs, Infrastructure (networks, storage, security, email) SMEs and ICT operational team leads (as detailed within Appendix F).
- **Report Creation and Finalisation Workflow:** A summary view of the key interaction steps leading up the finalisation of a SPR for distribution to the other Queensland Government Agencies
- **Infrastructure Walkthrough:** An overview of the key pieces of ICT infrastructure involved in the transmission of SPR's between the OneSchool application and the other Queensland Government Agencies.
- **Findings & Recommendations:** Summary of the key observations, risks and resultant remediation recommendations.

For the purposes of the objectives of this report we have subdivided the workflow and system interaction steps involved in the end-to-end creation and delivery of a SPR into two areas which are described in detail in the following sections:

- **Report Creation and Finalisation Workflow:** A summary view of the steps the key interaction steps leading up the finalisation of a SPR for distribution to the other Queensland Government Agencies.
- **ICT Infrastructure Walkthrough:** An overview of the key pieces of ICT infrastructure involved in the distribution of SPR's between the OneSchool application and the other Queensland Government Agencies.

The key stakeholders that interact with the OneSchool system from an end user perspective that should be considered as part of the processes described above are as follows:

Table 30 - Key OneSchool End User Stakeholders

Stakeholder	Interaction
School Staff including principals	Create report of suspected/actual student protection concerns
School Principal (or delegate)	Approval authority for report finalisation and sending to intended recipients
Child Safety Regional officers	Collate reports and perform functions delegated by the chief executive officer of the DCCSDS
Queensland Police Staff	Queensland police staff in relevant CPIUs who are recipients of SPR's

6.5.3 Report Creation and Finalisation Workflow

The key steps involved in the creation and finalisation of a SPR for distribution to the other Queensland Government Agencies are depicted in the diagram below, and are described in detail in the following table.

Figure 19 - Report Creation and Finalisation Workflow

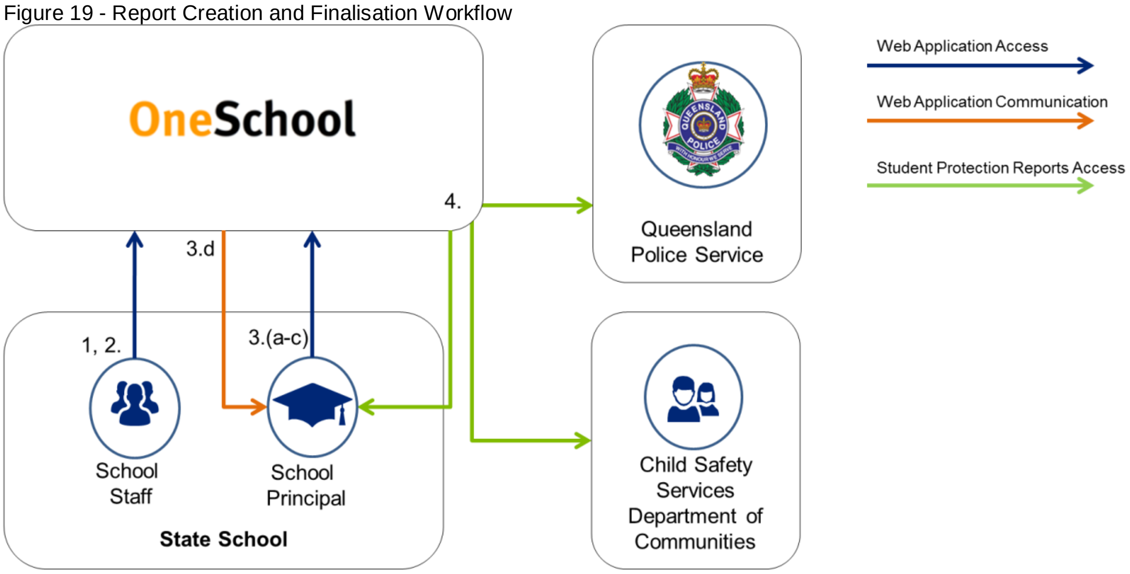

OneSchool
4.
3.d
1, 2.
3.(a-c)
School Staff
School Principal
State School
Queensland Police Service
Child Safety Services Department of Communities
Web Application Access
Web Application Communication
Student Protection Reports Access

Table 31 - Current State report creation and finalisation workflow

Ref #	Action	Steps
1	Create Report	a) Upon knowledge/suspicion of abuse or concern, staff members use the OneSchool SPM to enter necessary information as mandated by legislative requirements. Staff complete the SPR or save an incomplete SPR as part of a multi-step process.
2	Submit Report	a) Upon completion of a report, the system workflow submits the report to the principal for further action. b) Email notifications are issued at various stages in the report workflow to prompt relevant school staff (initiator) to complete any remaining workflow steps.
3	Principal review and Finalisation	a) Once the report is completed, OneSchool generates an email to the principal to notify them that a student protection concern has been submitted. b) Reports transition through a workflow whereby an approval process is delegated to the school principal. The principal or an authorised delegate is responsible for the finalisation of the report. c) Finalisation involves the principal responding to a set of questions, which determine the final recipients of the email report under the criteria defined by the business requirements of the Child Safety team within DET. Based on the principal's responses, the SPR might not be distributed to external agencies but instead be categorised as 'monitor at school' d) Regular reminders are sent to principals in case the principal has not finalised the report.
4	Report Email/Monitoring	a) Once the report is finalised for external agencies, the application generates the SPR as a word document and sends it via email to ○ Either QPS, DCCSDS or both ○ The principal receives a CC of email sent for their own records (including a word format version of the SPR). ○ A separate email is generated without attachment to inform the initiating staff member about the status of the SPR.
5	Reporting and QA	a) The current design of the SPM also incorporates a search feature for display and management of previously raised SPR's, and a multi-step form for the creation of new reports and review of existing reports. This is primarily used by DET student protection staff for reporting, QA or for follow up of cases.

6.5.4 Infrastructure Walkthrough

The diagram below shows the key pieces of ICT infrastructure that are involved in the transport of the finalised email SPR from the OneSchool application to the other external third party recipients.

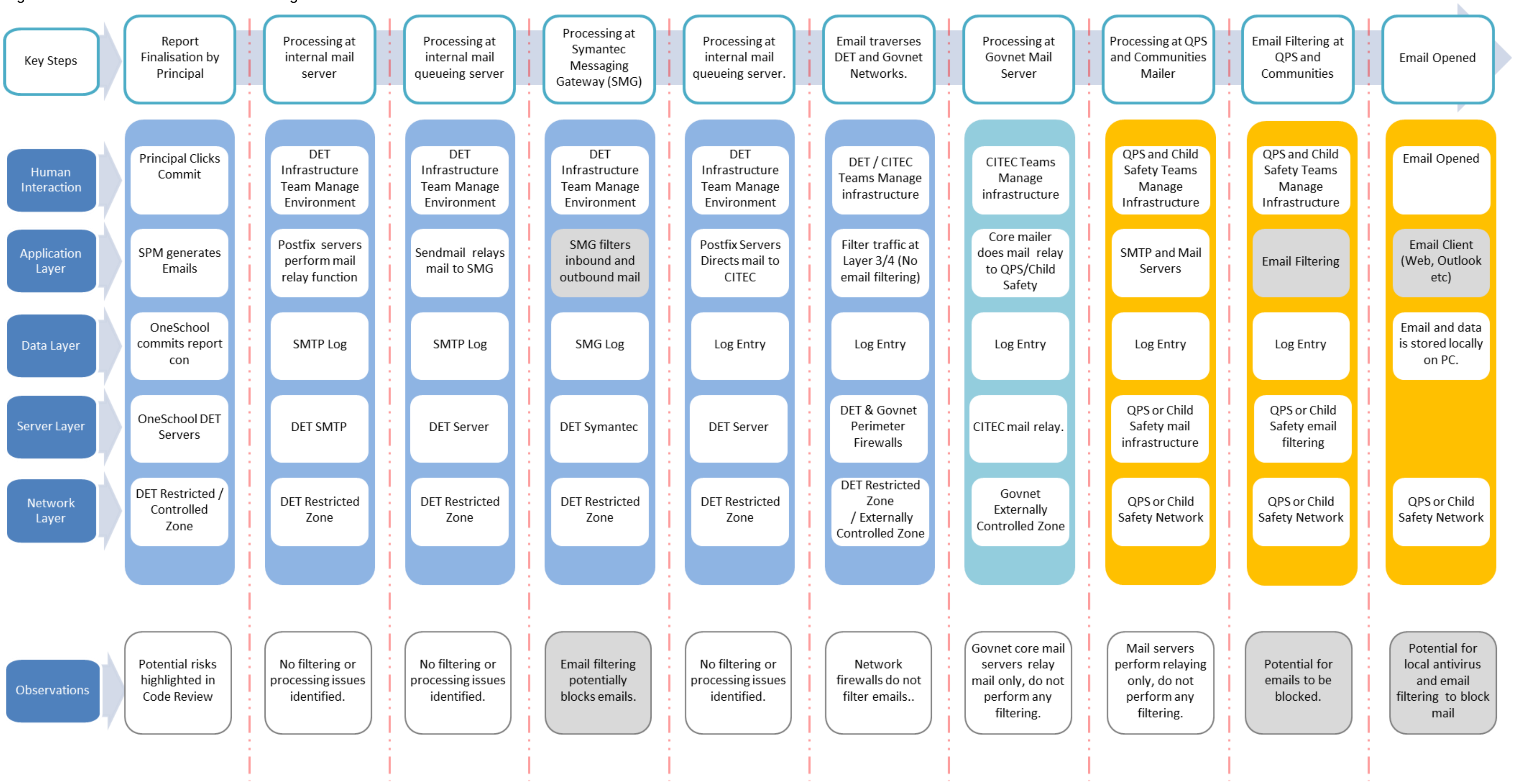
For clarity, the infrastructure components have been divided into categories based on a typical technology 'stack' with the additional inclusion of a human interaction layer as follows:

- **Human Interaction** – Specific actions or monitoring activities undertaken by stakeholders

- **Application Layer** – Forwarding, filtering or processing performed on the email messages
- **Data Layer** – Local storage and logging of information
- **Server Layer** – ICT infrastructure providing physical or virtual processing capability
- **Network Layer** – The zoning and key ICT infrastructure supporting the transport of information.

Any potential observations or risks are highlighted within observations in the following diagram and are discussed in further detail later in this report.

Figure 20 – ICT Infrastructure Walkthrough



Key Steps	Report Finalisation by Principal	Processing at internal mail server	Processing at internal mail queueing server	Processing at Symantec Messaging Gateway (SMG)	Processing at internal mail queueing server.	Email traverses DET and Govnet Networks.	Processing at Govnet Mail Server	Processing at QPS and Communities Mailer	Email Filtering at QPS and Communities	Email Opened
Human Interaction	Principal Clicks Commit	DET Infrastructure Team Manage Environment	DET Infrastructure Team Manage Environment	DET Infrastructure Team Manage Environment	DET Infrastructure Team Manage Environment	DET / CITEC Teams Manage infrastructure	CITEC Teams Manage infrastructure	QPS and Child Safety Teams Manage Infrastructure	QPS and Child Safety Teams Manage Infrastructure	Email Opened
Application Layer	SPM generates Emails	Postfix servers perform mail relay function	Sendmail relays mail to SMG	SMG filters inbound and outbound mail	Postfix Servers Directs mail to CITEC	Filter traffic at Layer 3/4 (No email filtering)	Core mailer does mail relay to QPS/Child Safety	SMTP and Mail Servers	Email Filtering	Email Client (Web, Outlook etc)
Data Layer	OneSchool commits report con	SMTP Log	SMTP Log	SMG Log	Log Entry	Log Entry	Log Entry	Log Entry	Log Entry	Email and data is stored locally on PC.
Server Layer	OneSchool DET Servers	DET SMTP	DET Server	DET Symantec	DET Server	DET & Govnet Perimeter Firewalls	CITEC mail relay.	QPS or Child Safety mail infrastructure	QPS or Child Safety email filtering	
Network Layer	DET Restricted / Controlled Zone	DET Restricted Zone	DET Restricted Zone	DET Restricted Zone	DET Restricted Zone	DET Restricted Zone / Externally Controlled Zone	Govnet Externally Controlled Zone	QPS or Child Safety Network	QPS or Child Safety Network	QPS or Child Safety Network
Observations	Potential risks highlighted in Code Review	No filtering or processing issues identified.	No filtering or processing issues identified.	Email filtering potentially blocks emails.	No filtering or processing issues identified.	Network firewalls do not filter emails..	Govnet core mail servers relay mail only, do not perform any filtering.	Mail servers perform relaying only, do not perform any filtering.	Potential for emails to be blocked.	Potential for local antivirus and email filtering to block mail

The following table describes in further detail the email transmission steps illustrated in the previous diagram. For the purposes of this description a hypothetical scenario in which a report will be sent to both QPS and the DCCSDS has been described. Based on the principal's responses to the relevant questions, the application has determined the target recipients within the Department of Education and QPS.

Table 32 - Description of ICT Infrastructure Steps for Email Transmission

Key Steps	Description
Report Finalisation by Principal	• Application reporting server generates email with appropriate target recipients • The content of the report is converted to a word document and attached to the email
Processing at internal mail server	• The OneSchool application establishes an SMTP connection to one of the internal mail servers • This postfix server logs the transaction and passes the email to the sendmail queueing server
Processing at internal mail queueing server	• One of the Internal queuing servers will process the email in the inbound queue • The server will pass the email to the Symantec messaging gateway (SMG)
Processing at Symantec messaging gateway	• The Symantec messaging gateway receives email and performs spam checking based on predefined non-configurable rules within the product There are two possible outcomes; • Mail is considered as spam and is quarantined, no notification to originator is sent • Mail is not considered as spam and is returned to internal queueing server
Processing at internal mail queueing server.	• Mail is processed in the outbound queue. The following actions take place. • Mail for QPS and communities is sent to GovNet core mailer through a secure TLS connection • Principal's email is sent to MelbourneIT mail relay which passes the email to Office 365 through a secure TLS connection end to end.
Email Traverses DET and Govnet.	• Emails for QPS and DCCSDS are sent via DET and GovNet perimeter firewalls using Queensland Government Network to reach Core mailer. • Email for principal traverses DET and MIT perimeter firewall to MIT mail relay (mxa.edu.au).
Processing at Govnet mail Server	• GovNet Core mailer performs lookup based on destination and forwards email to QPS Mailer and Communities mailer. No Email filtering is performed in GovNet.
Processing at QPS and Dept. Communities Mailer	• QPS and DCCSDS mailers receive inbound mail. • The mailer re-directs the email to spam filtering.
SPAM Filtering at Dept. Communities and QPS	• Communities and QPS both perform mail filtering on inbound emails. • Emails not considered as SPAM are forwarded to respective mailboxes.
QPS and/or Dept. Communities staff open report.	• Staff at QPS and DCCSDS receive email in their mailboxes and perform appropriate function as per job role. • Staff are able to copy reports to their PC and/or leave them in mailbox.

6.5.5 Findings and Recommendations

The following findings and recommendations relate specifically to the SPM system design and underpinning ICT infrastructure. However these findings are also informed by the preceding business requirements and application code review which provides additional technical context.

During the course of the review it became apparent there are a number of aspects of the system that could be enhanced through a number of tactical measures in order to reduce the short term risk of failure. Additionally there are a number of more strategic activities that DET could undertake in the longer term to improve the overall consistency and quality of end to end Student protection reporting across the agencies.

In order to assist DET with planning and prioritisation we have categorised the findings and recommendations relating to the Application Architecture and ICT Infrastructure review as either ‘tactical’ or ‘strategic’.

It is noted that the recommendations and options presented within this report may be affected by the outcome of a risk assessment and security classification recommendation, which is outlined below.

Table 33 - Findings & Recommendations Relating to SPM Technical Design and ICT Infrastructure

ID	Finding	Implication	Recommendation
1	• The architecture documentation reviewed makes reference to the principles of the Queensland Information Privacy Act 2009. However, there seems to be no reference to a formal security classification assigned to student protection record during application architecture and design • The security risk assessment conducted by DET does not appear to reference the information classification level of information being transmitted.	The absence of a security classification introduces the following potential risks; • The application design may not cater for requirements set out for that particular classification level • The security risk assessment has the potential of being incorrect if it's not based on correct classification level • If the security classification is assumed to be 'protected' or 'highly protected' as per criteria set out in DET's security classification framework , the following areas are potentially not correctly addressed as per the Queensland Government information security classification framework (QGISCF): • Preparation and filing • Removal from workplace, and monitoring • Electronic transmission • Storage and archival and retention policies. For example, for 'protected' information, the policy requires that • *'Email May be passed over appropriately classified internal networks. Must be encrypted when sent between agencies'* and • *'May be passed over appropriately classified internal networks as defined in the NTSAF'.*	**Tactical: Security classification and risk assessment.** It is recommended that DET complete the following activities: 1. Conduct a data security classification exercise and assign a data classification rating to the information stored and transmitted by the SPM 2. Undertake a security risk assessment taking into account the: • Queensland Government Information Security Classification Framework(QGISCF) • Queensland Government Network Transmission Security Assurance Framework (NTSAF) • DET Information Security Classification and Handling Guideline • QGCIO Information Security Policy – IS18.
2	• Once a SPR is finalised by the principal, a copy of the email with the report attached is sent to principal via email.	Based on discussion with the DET Child Safety business stakeholders, the message to the principal is used as a mechanism for acknowledgement of email delivery, which due to nature of email technology is not guaranteed. Other considerations relating to this include the following:	**Tactical: Application/Business process** It is recommended that the system should be updated so that the principal only receives an email from the system notifying them that a SPR and email has been generated. This is

		• The email traverses the internet and may be stored on the principal's local computer upon receipt. This increases the risk of data loss and potential security breaches. • The stringent controls that are in place for information residing within the OneSchool data repository are unlikely to be replicated at end user computers/mobile devices.	similar to the notification email currently received by school staff. This is not expected to impact any existing business process as the information contained within the attachment is already available to principals from within the SPM.
3	• Emails between DET, CITEC, QPS and DCCSDS mailers is encrypted use 'opportunistic TLS encryption' • The email attachment is not separately encrypted.	'Opportunistic encryption' means that the secure channel is set up without verifying the identity of the remote end. This approach is considered 'best effort' and only provides security if the remote end also supports the protocol. If the remote end is not configured correctly or if encryption fails, the sender reverts to un-encrypted communication. Implications of this include: • Opportunistic TLS does not guarantee end to end encryption of emails between the agencies at all times • This approach may not satisfy the requirements of the information classification review against NTSAF and QGISCF described above.	**Tactical: Encryption** 1. It is recommended that 'enforced TLS' be implemented end to end in conjunction with QPS, CITEC and the DCCSDS 2. Certification of end-to-end TLS should be attained from all providers and independent technical testing for audit and compliance purposes should be undertaken 3. Alternatively, if the infrastructure cannot be altered as described above, DET is advised to investigate the option of encrypting the SPR prior to transmission.
4	• Email filtering is implemented in DET, QPS and the DCCSDS.	DET has recently undertaken steps to reduce the risk of inadvertent blocking of reports by "whitelisting" the OneSchool sending email address, thereby allowing all email from that address to pass through the DET email filter unblocked. The following additional observations have been made in relation to email filtering: • Currently DET only whitelists emails from the OneSchool application email address (outbound). The potential exists that a recipient may reply to this address with requested clarifications. Although it is understood that this may not strictly be in accordance with agreed business process, there is potential for sensitive emails to be filtered	**Tactical: Email Filtering** • It is recommended that DET, in consultation with DET Child Safety business stakeholder, considers 'whitelisting' inbound emails to the application email address if emails have been received via this address historically • DET should work with QPS and the DCCSDS to ensure that the "whitelisting" of emails from OneSchool also be implemented within their email infrastructure • A change policy between the three departments

		if someone replies to a SPR notification. • Due to the use of spam filtering by other agencies, there is a possibility that emails may be inadvertently blocked by filters within DCCSDS and QPS (in case of QPS the risk is potentially lower as QPS has advised they only perform filtering of executable files). • DET cannot control nor maintain visibility of various areas of technology involved in end to end delivery of reports. e.g. CITEC does not currently perform any spam filtering, however this may change in future.	should be agreed so that other agencies are informed of any significant change to the email filtering environment.
5	• Email has been chosen as the mechanism for delivery of SPR's and notifications • Neither the business process nor the application architecture ensures that reports are guaranteed to be tracked or their delivery acknowledged • Across DET, private schools, the DCCSDS and QPS there are a number of information systems used to track and manage child protection information.	• Email is not a reliable medium for delivery of sensitive information. In an application environment, email does not typically guarantee delivery or receipt of information unless accompanied by additional controls • As the recipients of the reports do not interact with the application in any way, any problem or intentional changes in behaviour of the underlying infrastructure (which might not be within DET's control) can potentially result in non-delivery of reports without any related alert being captured by DET • Due to the number of systems in use within the wider environment, a number of additional risks arise including: ○ The potential for inconsistency in approach to handling child protection cases across the multiple agencies ○ Lack of centrally updated, consistent and up-to-date information ○ Challenges in sharing consistent information across agencies may increase overall effort and quality of data.	**Tactical and Strategic Application Enhancement Options** There are a number of approaches available to DET in order to address the risks relating to the delivery and management of SPR information. In the sections below, a number of options are described that outline remediation approaches and steps that may be taken to tactically address priority risks in the short term in addition to a number of more strategic longer term enhancement approaches.

6.5.6 Application Enhancement Options

There are a number of solution enhancement options open to DET in order to address the identified risks relating to the SPM and the delivery and management of the SPR information, these have been divided as follows:

- **Tactical**: A number of fixes that can be applied relatively quickly in the short term in order to mitigate a number of key risks
- **Strategic:** More holistic long term solution options that, if implemented, could improve overall consistency and quality of end to end Student Protection Reporting across the Queensland government agencies.

It should be noted that the design and implementation of any enhancements could change depending on the results of the data security classification activities described above.

Tactical Enhancements

The SPR could be distributed to relevant agencies through the use of a single-use download URL, referred to as a “Onetime URL”, rather than as an email attachment. A one-time URL is a specially crafted address that is valid for one use only and must be used within a certain period of time before expiring. This approach will reduce the risk associated with the distribution of email attachments and adds the ability to acknowledge the download of reports by users until a more permanent solution is implemented.

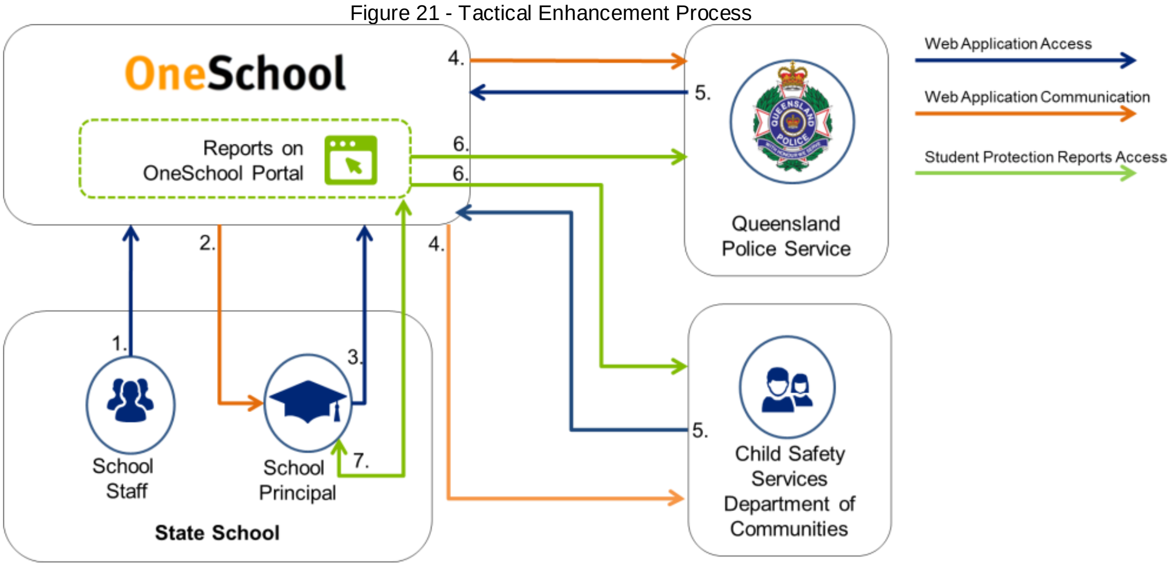
This short term enhancement involves the implementation of the following process to facilitate the agencies’ access to SPR’s:

1. Staff member submits a report
2. The Principal is notified that a report has been submitted
3. The Principal finalises the report to be submitted. Upon finalisation of the report by the Principal, a unique one-time URL is generated for each report recipient to provide a mechanism for securely downloading the report from the OneSchool website. A unique token is created and stored on the OneSchool system for each recipient.
4. A unique email containing the one-time URL is sent to each agency contact with a link this will pass the newly created token to the OneSchool report download web page.
5. On clicking the URL, verification checks are performed against the token sent to ensure that it is still valid. If the tokens are found to be invalid or expired, a suitable message will be displayed on screen and the file download will not occur. If the token is valid, a web page will present the user with input fields, as a baseline, requiring the user to enter the following:
    a. Name & Email Address
    b. Agency notifier ID.DET will need to work with agencies to determine if each branch receiving the reports has a unique identifier. These identifiers can then be mapped to the recipients in the OneSchool database. If these do not exist, new identifiers can be assigned and communicated to the end user. Note that removal of the ID does not impact functionality as this is used as an additional validation check. If DET can use federated access and single sign-on, this step will be redundant.
    c. On submission of the form, the agency notifier ID will be matched against pre-existing data. If a match cannot be found, verification fails and the report will not be downloaded.
        - This has the added benefit of reducing the risk of the scenario where an unauthorised user has obtained the original email but does not know the associated agency contact identifier.

6. The recipient can now download the report if their identifier matched and the token was valid.
7. The principal can access the report directly on the portal.

The process described above is depicted within the diagram below.

Figure 21 - Tactical Enhancement Process


OneSchool
Reports on OneSchool Portal
4.
5.
6.
6.
2.
4.
1.
3.
7.
School Staff
School Principal
State School
Queensland Police Service
5.
Child Safety Services Department of Communities
Web Application Access
Web Application Communication
Student Protection Reports Access

The following caveats apply to this process:

1. If the email is compromised before the one-time URL is used, it is possible that the report could be downloaded by a third party, compromising security. However the additional token expiry checks prior to download are likely to prevent such attempts from being successful in most cases. Furthermore, securing the download page for GovNet users only could further reduce the potential for unwarranted access to the reports.
2. This solution does not remove the risk of security breaches once the report has been downloaded by QPS and the DCCSDS.

In addition, it is recommended that tactical recommendations 1, 2, 3 and 4, outlined in Table 33 above, are implemented while the onetime URL solution is built and deployed. It should be noted that the recommendations may change depending on the results of the recommended security classification and risk assessment activities.

Strategic Enhancements

Three high level approaches that DET and the Queensland Government could be assessed in order to enhance the consistency and quality of end-to-end Student Protection Reporting across the Queensland Government agencies are outlined below.

Each of the three options described below incrementally increases the level of integration between DET, QPS and DCCSDS systems. This incremental increase in integration is expected to correlate to a corresponding increase in implementation cost and complexity.

A high level summarised view of the three options is provided below. It is noted that each option would require significant stakeholder consultation, comprehensive cost benefit and requirements analysis before more detailed architectural designs or implementation approaches can be documented.

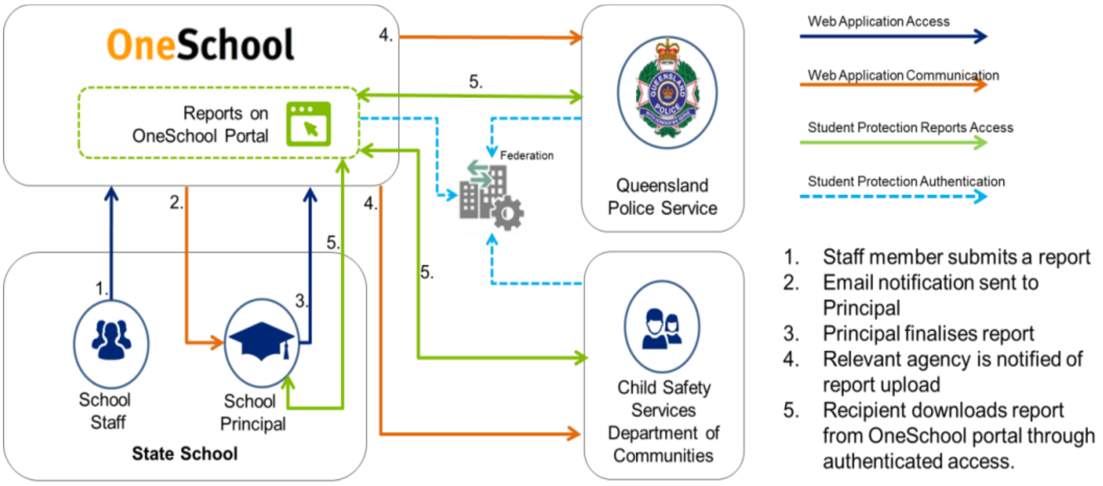
Strategic Enhancement Option 1

This option involves the provision of QPS and DCCSDS staff with direct access to the OneSchool portal through federated identity management and authentication. This allows for the following;

- A single portal for reporting, notification and recording of activities associated with student protection which can be used by DET, QPS and the DCCSDS.
- Managing access to the portal via federated identities should reduce the administration overhead of user account management. A federated identity would involve the linking of the identity and access management systems of QPS, DCCSDS and DET so that users from one organisation can access another organisation's systems (like OneSchool) using their own username/password. This could potentially also include 'single sign-on' capability.
- Centralised reporting on Student Protection information access and increased visibility of actions performed by the agencies.

The diagram below shows a simplified view of the changes to the Student Protection Reporting process that would result from the implementation of this option.

Figure 22 – Strategic Option 1: Student Reporting Process



OneSchool
Reports on OneSchool Portal
Federation
Queensland Police Service
Child Safety Services Department of Communities
School Staff
School Principal
State School
1.
2.
3.
4.
5.
Web Application Access
Web Application Communication
Student Protection Reports Access
Student Protection Authentication
1. Staff member submits a report
2. Email notification sent to Principal
3. Principal finalises report
4. Relevant agency is notified of report upload
5. Recipient downloads report from OneSchool portal through authenticated access.

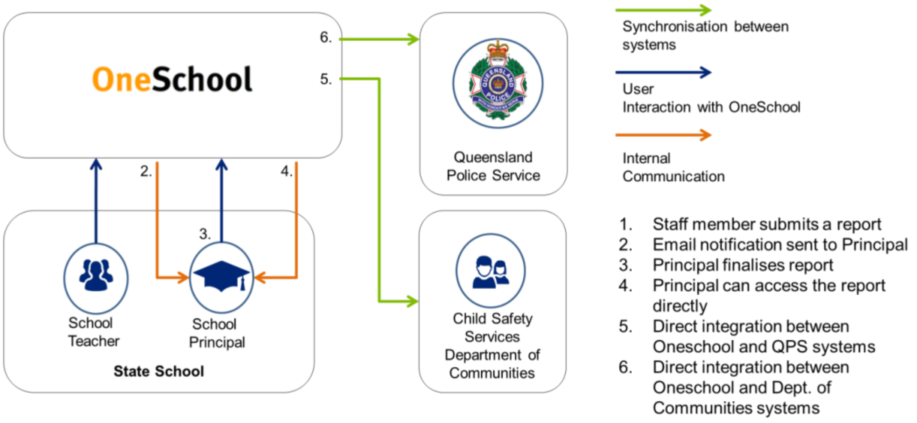
Strategic Enhancement Option 2

This option involves implementing technical system integration between OneSchool and the various systems in use within each of the relevant Queensland Government agencies.

By increasing the level of integration, it should be possible to increase the overall level data consistency and quality and realise a corresponding improvement in the reliability of Student Protection Reporting across the various agencies.

The following diagram below shows a simplified view of the changes to the Student Protection Reporting process that would result from the increased integration.

Figure 23 - Strategic Option 2: Student Reporting Process


OneSchool
6.
5.
2.
4.
3.
School Teacher
School Principal
State School
Queensland Police Service
Child Safety Services Department of Communities
Synchronisation between systems
User Interaction with OneSchool
Internal Communication
1. Staff member submits a report
2. Email notification sent to Principal
3. Principal finalises report
4. Principal can access the report directly
5. Direct integration between Oneschool and QPS systems
6. Direct integration between Oneschool and Dept. of Communities systems

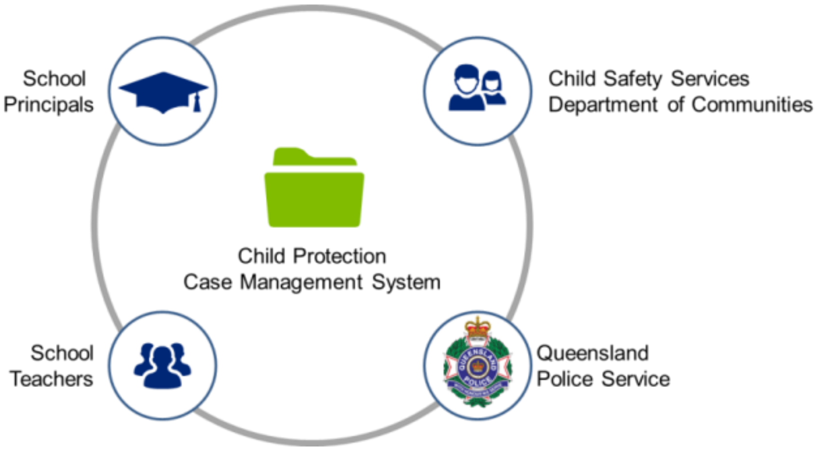
It is noted that Application Programming Interfaces (APIs) are the most likely mechanism that could be employed to implement increased integration. However no assumptions have been made as to whether the systems would be integrated directly to each other or via a common intermediary system or “Enterprise Service Bus”. Further analysis would be required in order to clarify the optimal architectural approach.

Strategic Enhancement Option 3

It has been noted that Student Protection information within Queensland is distributed across a number of systems within numerous government agencies and as a result, no single source of information exists.

The lack of consistent information is potentially compounded by the fact that individual agencies do not have full insight into the business processes and decision frameworks in use within the other agencies with regard to prioritisation and processing of Student protection cases. This means that there is no single integrated Student Protection process that covers DET, QPS and the DCCSDS.

Figure 24 - Strategic Option 3: Centralised Case Management System


School Principals
Child Safety Services Department of Communities
Child Protection Case Management System
School Teachers
Queensland Police Service

In order to address these challenges, Queensland Government could seek to implement a holistic end–to-end Child Protection process at a state level. This implementation would be expected to necessitate the deployment of a case management information system that is utilised by the relevant stakeholder groups, potentially also including the private school system. The integrated case management system would facilitate the following:

- Increased integration and quality of information across various stakeholder groups
- Increased information sharing across agencies and improved consistency of reporting
- Consistent business processes and end to end case management allowing for effective and timely handling of child protection concerns.

It is noted that the implementation of the systems and processes described above requires extensive engagement of the state-wide stakeholders groups across government.

7 Limitation of our work

This report has been prepared exclusively for the Department of Education & Training as per the purposes set out in the contract dated 17 August 2015. This report should be read in conjunction with the terms and conditions agreed in the Professional Services Panel Arrangement (QGCPO 878-13). This report is not intended to and should not be used or relied upon by anyone else and we accept no duty of care to any other person or entity.

Deloitte Forensic and Technology Advisory staff are not lawyers, and our report should not be relied upon as legal advice. Our work was not conducted in accordance with any auditing or assurance standards issued by the Audit and Assurance Standards Board, and consequently no opinions or conclusions were made under these standards. We will not provide any assurance or opinion on the matter including for example, whether you should proceed with any form of formal action against a third party.

This report is based on the information provided to us by Department of Education & Training, OneSchool and other stakeholders. Other than where specified, Deloitte does not assume responsibility for the validity and accuracy of the information obtained in this regard. For the purposes of preparing this report, reliance has been placed upon the material, representations, documentations, information and instructions obtained. We have not undertaken any audit, testing or verification of the information obtained as we assumed that this information is true, correct and complete and not misleading. If this is not the case or the information changes after we receive it, then our work may be incorrect or inappropriate for you.

Deloitte completed its field work on 9 October 2015 and has not updated its work since that date. The services will be limited by the agreed scope, information available, the accessibility of information sources and clarity or lack of clarity of your objectives. We reserve the right to revise any opinion or conclusion in our work if material information becomes known to us after the date our work is issued.

Appendix A. Operations Review Hypotheses and Suggested Initiatives

In forming the operational recommendations described within the earlier sections, a detailed analysis of the findings was performed and compared against industry good practices as described in section 5.1.3.

This analysis provided a number of hypotheses for potential improvements which would typically be validated, refined and amended (or rejected) with DET stakeholders throughout the duration of the project. As mentioned previously, there was no opportunity to perform this validation with DET due to the parallel incident investigation.

The detailed hypotheses and corresponding suggested improvement initiatives are included within this appendix for completeness. DET should validate any recommendations prior to implementation planning.

Reinforce control and quality of SPM with tactical improvements

Table 34 - Tactical Suggested Initiatives

Approach	Related Findings
Implement the following additional controls and quality assurance mechanisms for any change or issue impacting SPM alongside the current process followed to develop, operate and support OneSchool: 1. All changes to SPM module should have clear requirements documented following the DET standard template and signed off by the business 2. Any change to the architecture of the SPM should be reviewed and endorsed by the Technical Architecture Board 3. Peer code reviews should be performed for all changes/fixes 4. Test conditions should be reviewed and signed off by the business sponsor and test scripts should be peer reviewed within the Testing team prior to tests being conducted 5. System testing should always be completed by the Testing team and the results reviewed by the Education Business Support team 6. Scripted UAT should always be completed by the Business Sponsor with support from the Education Business Support team 7. Formal post implementation tests should be executed and formally signed off by the business 8. A Business Analyst should be appointed and involved in any change associated with SPM 9. The solution of any issue associated with SPM should be reviewed and approved by a senior OneSchool team member before the issue is considered resolved.	N/A

Review the OneSchool SDLC framework using a Risk Based Approach

Table 35 - SDLC Suggested Initiatives

Ref #	Description	Related Findings
I2.1	Create a OneSchool SDLC Handbook or update DET SDLC Handbook. This handbook should clearly define: 1. The process and procedures that need to be followed to develop and support OneSchool 2. Responsibilities for each key activity (i.e. RACI matrix) 3. The documents that need to be produced and the rules for review and approval 4. The standards that need to be followed (i.e. code standards).	F1.3, F2.2, F2.3, F2.4, F2.5
I2.2	Adopt a Risk Based Approach to drive the SDLC processes. A risk assessment should be completed for each change request at the beginning of the process, resulting in a risk profile rating. The rest of the process should take this rating into consideration to adjust the level of formality in key areas such as control, quality assurance and risk management (e.g. a higher risk requires more formal tests and a formal review of test scripts by the business users). The risk profile should be reviewed and approved by the OneSchool Application Board as specified by the board terms of reference. The risk profile should also be re-assessed as the change request progresses through the SDLC phases.	F3.1, F2.1
I2.3	Improve the testing practices by: 1. Adopting a risk based testing approach where high priority areas receive more testing attention. This should be aligned with the risk profile of each change and should also be considered for the specific test scenarios within each change request 2. Clearly define which team is responsible for each type of testing (i.e. integration testing, system testing). This should be confirmed within the test plan for each release, but ideally should be consistent for all change requests (i.e. developers always do integration testing, Test team always do system testing and regression testing) 3. Adopt the same approach and level of documentation for all system testing, and try to maximise the number of change requests that are tested by the independent Test team. If required, consider recruiting additional resources to make this possible 4. Consider peer review of the test scripts for change requests with a higher risk profiles 5. Consider collecting test evidence followed by an independent review after testing for change requests with a high risk profile has been performed 6. Ensure higher involvement of Business Units in testing, namely to help define and review test scripts and run structured UAT. Ensure that all change requests are formally accepted by the business unit 7. Consider making post-deployment scripted tests mandatory for change requests with a higher risk profile.	F3.9, F3.10, F3.11, F3.12, F3.13, F3.14, F3.15, F3.16
I2.4	Conduct formal peer review of software code for high risk change requests.	F3.8
I2.5	Improve requirements management and solution design by incorporating the following into the revised SDLC framework:	F2.4, F2.5, F2.6, F3.3,

	1. All change requests should have requirements documented in a standardised way and signed-off by the business. The complexity of the template should be adjusted to the size and risk profile of the change request. Additionally, the documentation should allow for traceability of requirements across the SDLC. 2. Changes to signed-off requirements need to follow a structured and properly governed change management process. This is especially critical for high risk changes. 3. Consider splitting the logical design document into two documents, functional design and technical design, for at least the high risk changes. If this is not feasible, consider structuring the logical design template in a way that the solution is initially described from a functional perspective to facilitate business review. 4. Define a simplified logical design template that should be completed and reviewed for small change requests.	F3.4, F3.5, F3.6, F3.7
I2.6	Update the DET Change Management process to enforce the review of individual change requests within the OneSchool release. If not feasible for all change requests, this should be at least mandatory for high risk changes.	F2.3, F3.17

Review the OneSchool Operating Model (i.e. Operations Plan) and appoint key outstanding roles

Table 36 - Operating Model Suggested Initiatives

Ref #	Description	Related Findings
I3.1	Update the OneSchool Operating Model to make it current and include the following improvements: 1. Clearly articulate the frameworks and methodologies that should be followed by OneSchool and when they should be used (i.e. ICT Project Management framework should be used for all change requests with a person day effort greater than x days) 2. Include references to clearly defined processes and procedures that should be followed by OneSchool teams (e.g. SDLC Framework) 3. Review the suggested Initiatives relating to Governance "*Implement stronger operational governance mechanisms"*	F1.3, F2.1, F2.2, F2.3, F2.4, F3.1, F3.6
I3.2	Review the organisational structure supporting OneSchool to: 1. Implement the split between application delivery and application support teams. This will allow for each to focus on their core activities 2. Have clear responsibilities associated with each role identified in the organisational structure.	F1.3, F3.3
I3.3	Appoint ICT technical project managers to lead the technical delivery of OneSchool change requests. Conduct an analysis of historical and forecasted change request demands to estimate the number of full time resources. Consider having a portion of these resources filled by internal resources to keep knowledge within DET.	F1.2, F3.22, F3.23
I3.4	Appoint a technical project manager to operationally manage and coordinate the end-to-end delivery of each OneSchool release under the oversight of the OneSchool leadership team and OneSchool Application Board.	F3.7, F3.9, F3.22
I3.5	Appoint business analysts to act as the bridge between Business Units and technical staff during the development of change requests. Key	F1.2, F3.4

	activities should include requirements gathering, functional design and testing. Conduct an analysis of historical and forecasted change request demands to estimate the number of full time resources required. Consider having a portion of these resources filled by internal resources to assist knowledge retention within DET.	
I3.6	Assign responsibility for maintaining the operational plan and other documentation to ensure currency. This role should also be responsible for ensuring that OneSchool teams understand the Operational Plan and their responsibilities. This could be helped by conducting periodic training sections.	F3.6
I3.7	Consider expanding the role of the Deployment team within the OneSchool Education Support System team to act as a Release & Deployment Manager they should be responsible for managing all aspects of the end-to-end release process including ensuring the correct sign-offs have been acquired for different phases in the process. Assess if the individual performing this role has the appropriate skills for the broader responsibilities. This role will rely on other roles to execute all the required activities to ensure that a release is correctly deployed within the Production Environment, this role will also be responsible for ensuring all the required activities and control mechanisms/sign-offs have been executed or provided.	F1.1, F3.1, F3.3, F3.7, F3.9, F3.22

Implement stronger operational governance mechanisms

Table 37 - Governance Suggested Initiatives

Ref #	Description	Related Findings
I4.1	Formalise the weekly change request meeting by defining clear Terms of Reference and agreeing documented outputs that should be shared with the Application Board. This meeting should include the following: 1. Assess, prioritise and approve delivery for small OneSchool change requests (as per current responsibilities) 2. Monitor progress of OneSchool release delivery and any associated risks, issues and dependencies. Provide steering and decision making capability and problem mitigation and resolution, with escalation to Application Board as appropriate. This component should be led by the technical project manager responsible for the delivery of the OneSchool release (see I3.5) 3. Review and approve/escalate to Application Board/Application Board scope changes to approved Change Requests. 4. Review testing and deployment documentation prior to submission to the Application Board for approval (see I4.3 for more detail)	F2.1, F2.2, F2.3, F3.2, F3.5
I4.2	Ensure the Application Board review and approve the test summary and UAT results prior to deployment as defined by the *"OneSchool Application Board - Operating Guidelines and Procedures"*	F3.9, F3.10, F3.11, F3.12, F3.13, F3.14, F3.15, F3.16
I4.3	Ensure the Application Board review and approve deployment of all releases as defined by the *"OneSchool Application Board - Operating*	F3.9, F3.10,

	Guidelines and Procedures".	F3.11, F3.12, F3.13, F3.14, F3.16, F3.18
I4.4	Establish the Solution Design Group to review the solution design of OneSchool change requests. If not feasible for all, make this mandatory for at least high risk changes.	F2.2, F3.6
I4.5	Implement independent audit reviews to the OneSchool procedures and practices to ensure the mandated frameworks, procedures and governance mechanisms are being followed.	F3.18, F3.24
I4.6	Review the risk management practices within OneSchool to ensure project and operational risks are identified and managed in a more consistent and structured manner. Work with the Governance, Strategy and Policy team to agree clear rules for escalation of OneSchool risks to the IT Branch level.	F1.1, F1.2, F2.3, F3.1

Refine the ICT Project Management framework (ICT PMF) and improve usage by OneSchool

Table 38 - ICT PMF Suggested Initiatives

Ref #	Description	Related Findings
I5.1	Ensure the ICT Project Management Framework is followed end-to-end by OneSchool for the overall release and the individual change requests that fit into the Project category.	F3.24
I5.2	Provide appropriate training to the business users on the usage of the ICT Project Management Framework and generic project management principles and practices (e.g. PRINCE 2).	F3.24
I5.3	Consider making the Technical Project Manager responsible for the outcomes of the technical activities and technical documentation (not necessarily delivering outputs, but accountable for driving the delivery).	F1.2, F3.9
I5.4	Consider refining the ICT Project Management Framework to ensure: • clear rules are included to assess which activities should be treated as Projects and consequently will need to follow the PMF • additional clarity is provided on what documents need to be produced at each phase and what sign-offs are required • Focus the methodology on the key co-ordination, management, reporting and governance activities that are required to deliver a project rather than technical steps and activities • Leverage other frameworks (such as an SDLC) to describe the technical steps and deliverables that need to followed and produced for ICT work streams within a project.	F1.2, F2.6

Develop better quality assurance, proactive monitoring and problem management procedures to support OneSchool Application

Table 39 - Quality Assurance Suggested Initiatives

Ref #	Description	Related Findings
I6.1	Implement additional quality assurance mechanisms in the OneSchool Support Model. If not feasible for all incidents, make this mandatory for high risk areas, such as the SPM. Examples of such mechanisms are illustrated below: • Mandatory independent review and approval of the solution to incidents associated with high risk areas. This should be supported by the service management tool (i.e. ServiceNow) by enforcing an additional step within the workflow. • Periodic reviews (i.e. weekly) of incidents to identify recurring incidents and triggers thorough analysis of the root-cause (i.e. Problem Management)	F3.20
I6.2	Implement a formal problem management process to focus on resolving the root cause of incidents, eliminating reoccurring incidents and proactively identify issues that can be solved before impacting end users.	F3.21, F3.23

I6.3	Document and clarify responsibilities for the procedures associated with monitoring the OneSchool application both from a technical and a functional perspective.	F3.19

Improve usage of tools across OneSchool SDLC

Table 40 - Improve Tool Suggested Initiatives

Ref #	Description	Related Findings
I7.1	Automate the regression tests to reduce the time taken and increase accuracy.	F3.16, F4.2
I7.2	Work with SDLC team to conduct an analysis to identify the right tools to support the SDLC process. Focus on identifying a tool that can support the end-to-end process. Specific attention needs to be paid to areas that are currently poorly supported such as requirements management, quality assurance and defect management. This analysis should take into consideration the capabilities of the current tool (i.e. TFS) and compare it with market alternatives. Implement the appropriate tool(s).	F4.1

Appendix B: Operations Review Document List

Category	Key Contents
Org Chart	DET-wide Organisation chart, IT Branch Organisation chart for roles underneath the Assistant Director-General Information Technology (CIO) and other Organisation charts for its subsidiary units.
Police Only change request	Communication, code, meeting minutes and logs relevant to the Police Only change request.
DET ICT Project Life Cycle	High level overview of the DET ICT Project Life Cycle indicating key areas of focus and activities for each phase, project management templates and planning tools.
DET and OneSchool Governance	Terms of Reference and Operating Guidelines for the Governance Boards across DET and within IT Branch related to the development, support and operation of OneSchool, detailing the objectives, scope, membership, roles and responsibilities and frequency of meetings for these boards.
EA Standards and Principles	Enterprise Architecture principles, ICT profiling standards and classification frameworks for the Queensland Government and DET.
Additional change requests	Additional information for Board approved changes, small changes and bug fixes including TFS logs, requirements, release instructions and test summaries.
SDLC Handbook	Description of the SDLC used across DET IT Branch for software development, operation and support, including graphics, reporting templates and detailed requirements and activities for each phase in the SDLC, as well as development methodologies and standards.
Change and Release Management Procedures	DET IT Branch change management process and classification details, OneSchool release schedule, production readiness certificate details, build procedures and test summaries.
Tools	A list and brief description of the tools used throughout the development, operation and support of OneSchool including project management, document management, service management, requirements gathering, development and testing.
Support	Incident management process and frameworks, support training documents, rosters, investigation and escalation details.
Role Descriptions	Description of the roles and responsibilities of the key positions involved in the development, support and operation of OneSchool, including: • Key Support Roles • IT Solutions and Operations • Education Business Systems ○ Test team ○ DBA and Reports

	• Platform Operations • Application Operations • Education Business Support • Education Business Improvement • Support Centre.
OneSchool Architecture	Solution architecture of the OneSchool application, descriptions of the email report generation process, high level description of OneSchool report delivery process and internal Ping Access Diagram, Office365 solution architecture, SPM logical design and information management framework.
OS Operating Model	Description and detail of the OneSchool Operational model, functions and Business Units, including descriptions of: • Financial model • Portfolio management • Application management • Application development and delivery • Business support • Platform operations • IT services and support • Business units
Risk Management	OneSchool risk register, risk management policies and methodologies used across DET IT Branch for project risk management, risk review documentation, and relevant meeting agenda and minutes.

Appendix C: Operations Review Meeting List

Interviewee	Job Title	Date
[redacted]	Test Analyst (UAT)	20/08/2015
[redacted]	Head of OneSchool Development	19/08/2015
[redacted]	L3 Functional Support for Child Protection Module	18/08/2015
[redacted]	Frontline Support	18/08/2015
[redacted]	L3 Functional Support for Child Protection Module	10/08/2015
[redacted]	Senior Test Manager	18/08/2015
[redacted]	Training Manager	24/08/2015
[redacted]	Executive Director OneSchool	13/08/2015
[redacted]	Manager Finance L3 Support	20/08/2015
[redacted]	Director Education Business Systems	13/08/2015
[redacted]	Director OneSchool Education Business Improvement	19/08/2015
[redacted]	Senior Advisor for Child Safety	11/08/2015
[redacted]	Acting Director of Child Safety Unit	11/08/2015
[redacted]	Senior Advisor for Child Safety	1/09/2015

Appendix D: Development and Testing Tools

Name	Usage
.NET Reflector	Debug Third-Party software
Axure RP Pro	Business Analysis
BeyondCompare	File Comparison and merging
BlueVerry Test Assistant	Testing
CodeSmith	Code Templates
Compuware Vantage	Implementation
FileLocator	Search Tool
HP Quick Test Pro	Testing
HP TRIM	Document capture/approval
IBM Rational DOORS	Requirements capture
IBM Rational System Architect	Architecture
Inflectra Spira Remote Launch	Testing
Inflectra Spira Team	Testing
KendoUI	UI Components
Microsoft Project	Project Management
Microsoft Project Server	Project Management
Microsoft Team Foundation Server 2008	Version Control/Work Management
Microsoft Team Foundation Server 2010	Development, Test
Microsoft Team Foundation Server Event Subscription Tool	Development
Microsoft Team Foundation Server MSSCCI Provider 2008	Development
Microsoft Team Foundation Server MSSCCI Provider 2010	Development
MSBuild 2008 RSS	Development
NetAdvantage	UI Controls

Notepad++	Text editing
PostSharp	C# Extensions/Libraries
QueueExplorer	Client/Server debugging
Resharper	Code analysis/best practice
Silverlight	Used for timetabling
Slickrun	Operating System shortcuts
SnagIt	Screen Capture
SQL Compare	Database comparing and merging
SQL Complete	SQL Code Formatting and Intellisense
SQL Pretty Printer	Formatting
SQL Server	Database development
SVNBridge	Development
Team Build Screen	Development
UltraMon	Debugging
VirtualCloneDrive	Software Installation/Viewing Files
Visio Pro 2007	Design document
Visual Studio 2008 Team Explorer	Development
Visual Studio 2010 Team Explorer	Development

Appendix E. Technical Review Document List

Category	Key Contents
Security	Information classification and handling guidelines, NTSAF and QGISCS guidelines
Solution Architecture	Logical Design and Solution architecture for the prototype and final solution of the Student Protection module
Risk Assessment	Risk assessment for secure email transmission of student protection forms and Risk management processes
Student Protection	Documentation for the Student protection module guide, initiation, report screens, benefits profile, benefits register, and concerns register
Technical Architecture	Email integration and flow, email report generation processes, Data Centre migration information, corporate exchange layout
Code	Code relevant to Student Protection module code review

Appendix F. Technical Review Interview List

Interviewee	Job Title	Date
[redacted]	Network SME	2/09/2015
[redacted]	Exchange SME	2/09/2015
[redacted]	Security SME	2/09/2015
[redacted]	Platform & Operations SME	2/09/2015
[redacted]	Manager Infrastructure	2/09/2015
[redacted]	Director, Platform Operations	25/08/2015
[redacted]	Senior Project Manager Office 365	1/09/2015
[redacted]	Executive Director, Web & Digital Delivery	1/09/2015
[redacted]	Acting Director, Child Safety	26/08/2015
[redacted]	Associate Director Child Safety	26/08/2015
[redacted]	Developer	20/08/2015

Appendix G. Detailed Code Review

This table below explains the detailed review of the software code for each business requirement, including a reference to the software code, additional comments and an indication of the ability of this code to implement the requirement.

Report Generation

Ref #	Code reference	Comments	Requirement Met
LR1.(a)	DETA.OSLP\Student\DataAccess\ConcernDA.cs, line 224	A "Created_User" GUID is associated with a new report when the report is created. The assumption is that this reference can be tied back to the actual name of the person creating the report.	YES
LR1.(b)	DETA.OSLP\Student\DataAccess\ConcernDA.cs, line 222	An "EQ_ID" (which is a unique identifier for the student in the OneSchool system) is associated with a new report when the report is created. The assumption is that this reference can be tied back to the student to obtain their name and sex	
LR1.(c)	DETA.OSLP.Web.Mvc\Areas\Student\Views\Concern\EditorTemplates\ConcernDetailViewModel.cshtml, lines 44-49	The field "Provide details of the alleged significant harm or risk of significant harm" on Step 2 of the concern report is assumed to be also used to collect information about the basis for raising the report	
LR1.(d)	DETA.OSLP.Web.Mvc\Areas\Student\Views\Concern\EditorTemplates\ConcernDetailViewModel.cshtml, lines 44-49	The field "Provide details of the alleged significant harm or risk of significant harm" on Step 2 of the concern report asks for details of the abuse	
LR1.(e)	DETA.OSLP.Web.Mvc\Areas\Student\Views\Concern_ModalEditSuspectedPerson.cshtml, lines 11-42 DETA.OSLP.Web.Mvc\Areas\Student\Views\Concern\EditorTemplates\ConcernDetailViewModel.cshtml, lines 108-117	i) The assumption is that the student's age can be obtained through the EQ_ID reference associated with the report ii) Details of the suspected person is gathered in Step 2 of the concern report iii) Details of any other persons who may have information is gathered in Step 2 of the concern report	

Ref #	Code reference(s)	Comments	Requirement Met
LR2.(a)	DETA.OSLP\Student\DataAccess\ConcernDA.cs, line 222	A "Created_User" GUID is associated with a new report when the report is created. The assumption is that this reference can be tied back to the actual name of the person creating the report.	YES
LR2.(b)	DETA.OSLP.Web.Mvc\Areas\Student\Views\Concern\EditorTemplates\ConcernDetailViewModel.cshtml, lines 44-49	An "EQ_ID" is associated with a new report when the report is created, which is a unique identifier for the student in the OneSchool system. The assumption is that this reference can be tied back	

		to the student to obtain their name and sex	
LR2.(**c**)	DETA.OSLP.Web.Mvc\Areas\Student\\Views\Concern_ModalEditSuspectedPerson.cshtml, lines 11-42 DETA.OSLP.Web.Mvc\Areas\Student\\Views\Concern\EditorTemplates\ConcernDetailViewModel.cshtml, lines 108-117	The field "Provide details of the alleged significant harm or risk of significant harm" on Step 2 of the concern report is assumed to be also used to collect information about the basis for raising the report	
LR2.(d)	DETA.OSLP\Student\DataAccess\ConcernDA.cs, line 222	i) The assumption is that the student's age can be obtained through the EQ_ID reference associated with the report ii) Details of the suspected person is gathered in Step 2 of the concern report iii) Details of any other persons who may have information is gathered in Step 2 of the concern report	

Ref #	Code reference(s)	Comments	Requirement Met
LR3.(a)	DETA.OSLP.Web.Mvc\Areas\Student\\Views\Concern\EditorTemplates\ConcernDetailViewModel.cshtml, lines 44-49	The field "Provide details of the alleged significant harm or risk of significant harm" on Step 2 of the concern report is assumed to be also used to collect information about the basis for raising the report	YES
LR3.(b)	See Req. 4	See Req. 4	

Ref #	Code reference(s)	Comments	Requirement Met
LR4.(a)	DETA.OSLP\Student\DataAccess\ConcernDA.cs, line 222	An "EQ_ID" is associated with a new report when the report is created, which is a unique identifier for the student in the OneSchool system. The assumption is that this reference can be tied back to the student to obtain their name/Sex.	YES
LR4.(b)	DETA.OSLP\Student\DataAccess\ConcernDA.cs, line 222	The assumption is that the student's age can be obtained through the EQ_ID reference associated with the report	
LR4.(c)	DETA.OSLP.Web.Mvc\Areas\Student\\Views\Concern\EditorTemplates\StudentDetailViewModel.cshtml, lines 35-53 DETA.OSLP\Student\DataAccess\ConcernDA.cs, line 221	The student's address is displayed on Step 1 of the concern report. The assumption is that this is obtained via the "EQ_ID" association attached to the report. A "Centre Code" is associated with a new report when the report is created, which is a unique identifier for the school in the OneSchool system. The assumption is that this reference can be tied back to the school to obtain name and address details.	
LR4.(d)	DETA.OSLP.Web.Mvc\Areas\Student\\Views\Concern\EditorTemplates\ConcernDetailViewModel.cshtml, lines 44-49	The field "Provide details of the alleged significant harm or risk of significant harm" on Step 2 of the concern report asks for details of the abuse	
LR4.(e)	DETA.OSLP.Web.Mvc\Areas\Student\\Views\Concern_ModalEditSuspectedPerson.cshtml, lines	Details of the suspected person is gathered in Step 2 of the concern report	

	11-42		
LR4.(f)	DETA.OSLP.Web.Mvc\Areas\Student\Views\Concern\EditorTemplates\ConcernDetailViewModel.cshtml, lines 108-117	Details of any other persons who may have information is gathered in Step 2 of the concern report	

Report Delivery

Ref #	Code reference(s)	Comments	Requirement Met
LR5.(a)	DETA.OSLP.Web.Mvc\Areas\Student\Views\Concern\Summary.cshtml, lines 433, 477-488 DETA.OSLP.Web.Mvc\Content\scripts\Areas\Student\oslp.student.concern.summary.js, lines 86-122, 139 DETA.OSLP.Web.Mvc\Areas\Student\Controllers\ConcernController.cs, line 294	If-else logic on lines 86-122 of oslp.student.concern.summary.js appears correct for response combination [Y, Y, N], which suggests that the else-statement will be executed thereby instructing the ConcernController to display the "Send student protection report" modal window as expected.	YES*
	DETA.OSLP.Web.Mvc\Areas\Student\Views\Concern_ModalFinaliseSexualAbuse.cshtml, lines 81-85, 101, 109	If-else logic on line 81 appears correct for response combination [Y, Y, N], which suggests that the if-statement will be executed and the "Police Contact" and "Child Safety Contact" fields will be displayed as expected.	
	DETA.OSLP.Web.Mvc\Areas\Student\Views\Concern_ModalFinaliseSexualAbuse.cshtml, lines 120, 173-176 DETA.OSLP.Web.Mvc\Content\scripts\Areas\Student\oslp.student.concern.summary.js, lines 52-57, 144 DETA.OSLP.Web.Mvc\Areas\Student\Controllers\ConcernController.cs, line 314 DETA.OSLP\Student\Business\Concern.cs, lines 610, 653-740	If-else logic on lines 662-675 of "Concern.cs" appears correct when both police and child safety email addresses have been supplied, which suggests that the report will be correctly emailed to both Police and Child Safety.	
LR5.(b)	DETA.OSLP.Web.Mvc\Areas\Student\Views\Concern\Summary.cshtml, lines 433, 477-488 DETA.OSLP.Web.Mvc\Content\scripts\Areas\Student\oslp.student.concern.summary.js, lines 86-122, 139 DETA.OSLP.Web.Mvc\Areas\Student\Controllers\ConcernController.cs, line 294	If-else logic on lines 86-122 of oslp.student.concern.summary.js appears correct for response combinations [Y, Y, Y], [Y, N, Y] and [Y, N, N], which suggests that the else-statement will be executed thereby instructing the ConcernController to display the "Send student protection report" modal window as expected.	YES*
	DETA.OSLP.Web.Mvc\Areas\Student\Views\Concern_ModalFinaliseSexualAbuse.cshtml, lines 77-92, 101, 109	If-else logic on lines 81 and 87 appears correct for response combinations [Y, Y, Y], [Y, N, Y] and [Y, N, N], which suggests that neither if-statement will be executed therefore ensuring only the "Police Contact" field is displayed.	

	DETA.OSLP.Web.Mvc\Areas\Student\Views\Concern_ModalFinaliseSexualAbuse.cshtml, lines 120, 173-176 DETA.OSLP.Web.Mvc\Content\scripts\Areas\Student\oslp.student.concern.summary.js, lines 52-57, 144 DETA.OSLP.Web.Mvc\Areas\Student\Controllers\ConcernController.cs, line 314 DETA.OSLP\Student\Business\Concern.cs, lines 610, 653-740	If-else logic on lines 662-675 of Concern.cs appears correct when only a police email address has been supplied, which suggests that the report will be correctly emailed to only Police	
LR5.(c)	DETA.OSLP.Web.Mvc\Areas\Student\Views\Concern\Summary.cshtml, lines 433, 477-488 DETA.OSLP.Web.Mvc\Content\scripts\Areas\Student\oslp.student.concern.summary.js, lines 86-122, 139 DETA.OSLP.Web.Mvc\Areas\Student\Controllers\ConcernController.cs, line 294	If-else logic on lines 86-122 of oslp.student.concern.summary.js appears correct for response combination [N, Y, N], which suggests that the else-statement will be executed thereby instructing the ConcernController to display the "Send student protection report" modal window as expected.	YES*
	DETA.OSLP.Web.Mvc\Areas\Student\Views\Concern_ModalFinaliseSexualAbuse.cshtml, lines 77-92, 101, 109	If-else logic on line 87 appears correct for response combination [N, Y, N], which suggests that the if-statement will be executed therefore ensuring only the "Child Safety Contact" field is displayed.	
	DETA.OSLP.Web.Mvc\Areas\Student\Views\Concern_ModalFinaliseSexualAbuse.cshtml, lines 120, 173-176 DETA.OSLP.Web.Mvc\Content\scripts\Areas\Student\oslp.student.concern.summary.js, lines 52-57, 144 DETA.OSLP.Web.Mvc\Areas\Student\Controllers\ConcernController.cs, line 314 DETA.OSLP\Student\Business\Concern.cs, lines 610, 653-740	If-else logic on lines 662-675 of Concern.cs appears correct when only a child safety email address has been supplied, which suggests that the report will be correctly emailed to only Child Safety	
LR5.(d)	DETA.OSLP.Web.Mvc\Areas\Student\Views\Concern\Summary.cshtml, lines 433, 477-488 DETA.OSLP.Web.Mvc\Content\scripts\Areas\Student\oslp.student.concern.summary.js, lines 86-122, 139 DETA.OSLP.Web.Mvc\Areas\Student\Controllers\ConcernController.cs, line 294	If-else logic on lines 86-122 of oslp.student.concern.summary.js appears correct for response combinations [N, Y, Y], [N, N, N] and [N, N, Y], which suggests that the if-statement will be executed thereby instructing the ConcernController to display the "Monitor student protection report at a school level" modal window as expected.	YES
	DETA.OSLP.Web.Mvc\Areas\Student\Views\Concern_ModalFinalise.cshtml, lines 75, 84-92 DETA.OSLP.Web.Mvc\Content\scripts\Areas\Student\oslp.student.concern.summary.js, lines 52-57, 144 DETA.OSLP.Web.Mvc\Areas\Student\Controllers\ConcernController.cs, line 314 DETA.OSLP\Student\Business\Concern.cs, line 615 DETA.OSLP\Student\DataAccess\ConcernDA.cs, line 769	Code path from view through to data access class appears valid and suggests that the report details would successfully be saved to the database on click of "Save and finalise"	

The application code satisfies the requirements LR5.(a-c). However if certain conditions are met there is a likelihood of failure. Two potential defect scenarios have been identified and are explained below:

Scenario 1: Potential defect LR5.(a-c)

A potential scenario may exist where reports are finalised yet not delivered to QPS/Child Safety.

During report finalisation, the following code is executed to send the report email to QPS/Child Safety and update the report as being finalised in the database:

```
// generate report and send email
SendEmail(dtoConcern);

if (Messages.HasErrors) return;
using (var scope = DataHelper.GetTransactionScope())
{
    ConcernDA.Finalise(dtoConcern);
    Messages.Add(Constants.TransactionMode.Update);
    scope.Complete();
}
```

Figure 1: DETA.OSLP\Student\Business\Concern.cs, FinaliseNonSecure(), lines 609-618

Based on the code above, the database update command - `ConcernDA.Finalise(dtoConcern);` - would not be performed under the following scenarios:

a) Should `if (Messages.HasErrors)` return false: this will occur if an error is raised when either sending the report email to QPS/Child Safety, or when sending a notification email to the report creator, as shown in the following code snippets:

```
//Send the email to the seleted agencies + cc the principal
try
{
    EmailUtil.SendEmail(
        Common.Configuration.ConcernFromEmailAddress,
        concernToEmailAddress,
        ResourceText.ProtectionConcernEmailSubject,
        body.ToString(),
        "OneSchool",
        attachmentCollection,
        principalDetails.Email,
        null, true,
        MailPriority.Normal, false);
}
catch (Exception)
{
    //TODO: move message into resource, and with correct wording.
    Messages.Add("Email send failed!", Constants.MessageCategory.Error);
}
```

Figure 2: DETA.OSLP\Student\Business\Concern.cs, SendEmail(), lines 720-738

```
try
{

    EmailUtil.SendEmail(
        Common.Configuration.ConcernFromEmailAddress,
        createdUserEmail,
        ResourceText.ProtectionConcernAdviceEmailSubject,
        emailBody.ToString(),
        "OneSchool",
        null,
        null,
        null, true,
        MailPriority.Normal, false);
}
catch (Exception)
{
    //TODO: move message into resource, and with correct wording.
    Messages.Add("Email to notifiers send failed!", Constants.MessageCategory.Error);
}
```

Figure 3: DETA.OSLP\Student\Business\Concern.cs, SendEmail(), lines 781-799

b) If an unhandled error is raised from SendEmail()

c) It appears that an additional situation has not been considered which could also prevent the database update from occurring. If the following conditions return false, then the send email function will not be triggered and the “Messages” collection will not be updated, therefore allowing the database update to proceed:

```
//send the email to the selected agencies
if (!string.IsNullOrEmpty(concernToEmailAddress))
{
    if (principalDetails != null)
    {
        <send email performed here>
    }
}
```

Figure 4: DETA.OSLP\Student\Business\Concern.cs, SendEmail(), lines 681-685

If this scenario were to be possible, then the above code should be revised to either raise an exception or update the “Messages” collection with an error, so that the database update will not be triggered.

Scenario 2: Potential defect LR5.(a-c).

The report file generated via SSRS is not error checked before being sent as an attachment in the email sent to QPS/Child Safety. The following code is executed prior to sending the email:

```
byte[] reportContent;
string contentType, fileExtension, fileName;

var reportParameters = new Dictionary<string, string>();
reportParameters.Add(BaseConcernDTO.PROP_CONCERN_ID, dtoConcern.ConcernId.ToString());
reportParameters.Add(PRINCIPAL_QUESTION_1,
dtoConcern.PrincipalResponseAnswers[0].ToString());
reportParameters.Add(PRINCIPAL_QUESTION_2,
dtoConcern.PrincipalResponseAnswers[1].ToString());
reportParameters.Add(PRINCIPAL_QUESTION_3,
dtoConcern.PrincipalResponseAnswers[2].ToString());

OneSchool.Framework.Web.Reporting.Utilities.RunReportAndReturnContent(
    REPORT_CODE,
    reportParameters,
    Messages,
    out reportContent,
    out contentType,
    out fileExtension,
    out fileName);

var memoryStream = new MemoryStream(reportContent);

var report = new Attachment(memoryStream, "StudentProtectionReport.doc",
MediaTypeNames.Text.Xml);
var attachmentCollection = new Collection<Attachment>();
attachmentCollection.Add(report);
```

Figure 5: DETA.OSLP\Student\Business\Concern.cs, SendEmail(), lines 696-718

If there is the possibility for the report not to be correctly generated with no exceptions raised, then the above code will continue through to email submission, and invalid file attachments may be sent to QPS/Child Safety.

From performing assembly reflection on the `OneSchool.Framework.Web.Reporting.Utilities.RunReportAndReturnContent()` method, it appears that the “Messages” collection is used to collect error details. As such, it may be judicious to raise an error after the above code should `if (Messages.HasErrors)` return true, so that the email submission will be prevented from occurring.

Core Requirements – Detailed Code Review

Ref #	Code reference(s)	Comments	Requirement Met
CR1.(a)	Procs.sql, Stored Procedure: "up_BatchJob_Protection_Incomplete_Notification_Insert", lines 2911-2920	Query against the "Protection.Concern" table returns all reports with a status of 'I' (indicating incomplete) and includes a join against a "Users_Vw" view for obtaining the email address of the report creator. Results are stored in a cursor for subsequent looping over for email submission.	YES
	Procs.sql, Stored Procedure: "up_BatchJob_Protection_Incomplete_Notification_Insert", lines 2923-2955	While loop is performed over the results cursor to obtain each email address to submit to and procedure/function "up_Send_DBEmail" is executed with the email address supplied.	
CR1(b)	Procs.sql, Stored Procedure: "up_BatchJob_Protection_Unfinalised_Notification_Insert", lines 3082-3096 Procs.sql, Stored Procedure: "up_Student_Protection_Approver_List", lines 4743-4782 Procs.sql, Stored Procedure: "up_BatchJob_Protection_Unfinalised_Notification_Insert", lines 3199-3208	Temp table "#FR_Principal" is created and populated by procedures "up_FR_Principal_List" and "up_Student_Protection_Approver_List". Query against the "Protection.Concern" table returns all reports with a status of 'S' (indicating submitted) and includes a join against the temp table "#FR_Principals" for obtaining the email addresses of the principal and student protection approvers. Results are stored in a cursor for subsequent looping over for email submission.	YES
	Procs.sql, Stored Procedure: "up_BatchJob_Protection_Unfinalised_Notification_Insert", lines 3211-3243	While loop is performed over the results cursor to obtain each email address to submit to and procedure/function "up_Send_DBEmail" is executed with the email address supplied.	
CR1(c)	DETA.OSLP\Student\Business\Concern.cs, lines 743-801	A notification email is sent to the report originator once the emails to QPS/Child Safety (if required) has been performed.	YES

Appendix H. Additional Suggestions for Code Structure Enhancement

ID	Area	Finding	Suggestions
1.4	Report Delivery	The code structure could be improve for additional modulatory and clarity to facilitate maintainability. Examples of improvement opportunities are outlined below.	Consider adopting the suggested improvements to increase maintainability.
1.4.1	Report Generation	There are instances where business logic is being performed at the View level (e.g. lines 77-92 of "_ModalFinaliseSexualAbuse.cshtml").	Ideally, this should be moved out into the business layer to achieve better decoupling from the presentation layer, thereby increasing the testability and maintainability of the code.
1.4.2	Report Generation	The business logic associated with where the report is to be sent is split across multiple files (i.e. "_ModalFinaliseSexualAbuse.cshtml" and "oslp.student.concern.summary.js")	It would be better to have this logic maintained in one location so that it can be more easily verified and maintained.
1.4.3	Report Generation	The use of both ViewModels and ViewBags together is not ideal (e.g. InitConcernViewModel() in "ConcernController.cs"). Both constructs serve a similar purpose and are generally not used together	All data pertaining to the View should be moved to the ViewModel where possible. Stronly-typed views make the code cleaner and easier to maintain and would also prevent the need to perform explicit casting and manipulation (e.g. lines 11-58 of "_ModalFinaliseSexualAbuse.cshtml")

Appendix I: Glossary of terms

ADG	Assistant Director-General
API	Application Programming Interfaces
BAU	Business As Usual
BVT	Build Verification Testing
CAB	Change Advisory Board
Call centre	DET Application Support Centre
Carmody Report	July 2012 Queensland Child Protection Commission of Inquiry report titled ‘*Taking Responsibility: A Roadmap for Queensland Child Protection*’
CIO	Chief Information Officer
CPIU	Child Protection Investigation Units
CR	Change request
DBA	Database Administration
DCCSDS	Department of Communities, Child Safety & Disability Services
DDG	Deputy Director-General
DET	Department of Education and Training
Director General	Director General of Department of Education and Training
FTS	Failure-To-Send notifications
FTS	Failure-To-Send notification(s)
ICT PMF	ICT Project Management Framework
IISC	Innovation & Information Steering Committee
IT Branch	IT Branch team
KBA	Knowledge Based Article
Logs	Email logs
Third Party Company 1	Details Redacted
NDR	Non-Delivery-Reports
NTSAF	Queensland Government Network Transmission Security Assurance Framework
OneSchool	The ‘OneSchool’ system used by DET
OneSchool ASC	OneSchool Application Support Centre
QA	Quality Assurance
QGCIO	Queensland Government Chief Information Office
QGISCF	Queensland Government Information Security Classification Framework
QGISCF	Queensland Government information security classification framework
QPS	Queensland Police Service
SDLC	Software Development Lifecycle
SME	Subject Matter Experts
SMG	Semantic Messaging Gateway
SPM	Student Protection Module
SPR	Student Protection Report
TFS	Team Foundation Server
The incident	Collectively the failure of the OneSchool SPM to send ‘QPS only’ reports to intended recipients.
The matrix	OneSchool SPM decision matrix
TRIM	Total Records and Information Management
UAT	User Acceptance Testing