Queensland Audit Office

Managing child safety information

Report 17: 2014–15

Queensland Audit Office

Location Level 14, 53 Albert Street, Brisbane Qld 4000

PO Box 15396, City East Qld 4002

Telephone (07) 3149 6000

Email qao@qao.qld.gov.au

Online www.qao.qld.gov.au

Front cover image is an edited photograph of Queensland Parliament, taken by QAO.

ISSN 1834-1128

Your ref:
Our ref: 10785

Queensland Audit Office

May 2015

The Honourable P Wellington MP
Speaker of the Legislative Assembly
Parliament House
BRISBANE QLD 4000

Dear Mr Speaker

Report to Parliament

This report is prepared under Part 3 Division 3 of the *Auditor-General Act 2009*, and is titled *Managing child safety information.*

In accordance with s.67 of the Act, would you please arrange for the report to be tabled in the Legislative Assembly.

Yours sincerely

Andrew Greaves
Auditor-General

Queensland Audit Office
Level 14, 53 Albert Street, Brisbane Qld 4000
PO Box 15396, City East Qld 4002

Phone 07 3149 6000
Email qao@qao.qld.gov.au
Web www.qao.qld.gov.au

Contents

Summary **1**

Conclusion 1
Availability of information 2
Security of information 2
Reform roadmap and investment plan 3
Recommendations 4
Reference to comments 5

1 Context **7**

1.1 Child safety services 7
1.2 Organisational roles and responsibilities 11
1.3 Key information systems 14
1.4 Information security classification 15
1.5 Standards and good practice 16
1.6 The Child Protection Commission of Inquiry 16
1.7 Audit objective, method and cost 17
1.8 Report structure 17

2 Availability of child safety information **19**

2.1 Background 20
2.2 Conclusion 20
2.3 Planning information needs 20
2.4 Information system 21
2.5 Information management 22
2.6 Recommendations 28

3 Information security **29**

3.1 Background 30
3.2 Conclusions 30
3.3 Security management 30
3.4 Responding to security breaches 33
3.5 Recommendations 33

Appendix A— Comments **37**

Appendix B—Audit details **45**

Summary

One of the roles of the Department of Communities, Child Safety and Disability Services (the department) is to protect children and young people who have been harmed or are at risk of harm.

For the year ending 30 June 2014, the department provided about $1.65 billion in grant funding to approximately 2 700 government and non-government organisations. Of this funding, 32 per cent, or around $522 million, was for child safety services.

When providing services to vulnerable children and young people, organisations—both government and non-government need to collaborate, and to do so quickly and easily. Sharing relevant information at the right time is critical to the safety and well-being of a child or young person. This was a clear finding in a 2014 coroner's inquest into the death of a child.

It is also important to maintain confidentiality of information. Appropriate physical and computerised security arrangements have to be put in place to safeguard data from unauthorised access and disclosure—either accidental or deliberate.

Achieving this balance between making information accessible when it is needed and secure at all times is a challenge for the department and the organisations with which it works.

In this audit, we assess whether the department has been able to make sure that the right information is made available only to the right people at the right time and in the right format.

Conclusion

The department has yet to get the balance right between security and availability of child safety data. This problem, involving parties inside and outside government, is made more complex because of the highly sensitive nature of the data involved. When young lives are at risk, priority must be given to accessibility and availability; while always remembering that inappropriate access to this data could increase the risk of harm.

Ready access to the information needed to deliver child safety services remains problematic—primarily for service providers. To date, the department has focused on making its information secure and accessible internally. Its information systems are not designed to share information easily and securely between organisations. To do its job, however, the department needs to share information with other government departments and non-government organisations (NGOs).

As it stands, the department cannot provide sufficient assurance that child safety information is secure and kept confidential. This is mainly because entities along the service chain, including NGOs, use emails to send and receive information. In addition, staff are currently extracting information from the secure departmental system and storing it in spreadsheets and databases, and downloading it onto mobile and memory devices. This means the information is being stored in a number of different places and in different ways and different systems.

Over the last ten years, $85 million has been spent building the integrated client management system. Part of this involved building in appropriate layers of security. Because of the system's limitations, this security is, at times, being circumvented, resulting in inefficient and poor information management practices.

Apart from the duplication of effort and resources that this causes, it leads to problems with data integrity. It also results in an inability to easily collect all of the information needed to report on service outcomes. Most importantly, it hampers effective coordination of services for 'at risk' children or young people.

Availability of information

The department does not have a clear and workable model for information flow throughout the service chain. This restricts information sharing across entities.

It also limits the department's ability to apply a more strategic approach to child safety services, because it cannot easily collect and analyse all of the necessary information. In addition, inconsistent information management practices across regions mean that important information about the outcomes of performance is not being recorded and reported.

Information systems and sharing is not integrated and this creates significant duplication of effort. Service providers re-create subsets of the same information in electronic and physical forms. The department and service providers along the service chain rely heavily on manual methods of sharing information. The result is that service providers do not always receive important information about children on time.

Similarly, it is not easy for the department to get information about the children's wellbeing and progress from service providers. The number of disparate systems has led to inconsistent information being held across various aspects of the service chain. This causes difficulty in identifying accurate information.

As a result, the department cannot easily produce reports on outcomes for the children in care such as:

- whether they have completed school
- whether they are suspended from school
- whether they have been reunited with their parents and then found themselves back in the system.

This is because it is very time consuming to match data held within different organisations to confirm accuracy. It is also difficult to aggregate individual case-based information to report on service outcomes. In fact, information is recorded and reported in a complex way and there is a need to analyse data and report at strategic, tactical and operational levels. Therefore, two separate teams within the department are needed to generate and monitor performance reports.

Security of information

Information security within the department

The department has adequately secured its child safety information within its key systems, with the significant exception that it does not always remove staff access when they no longer need the access.

Staff routinely take information out of the system to work with it in easier formats like spreadsheets. Staff who do not have authorised access to key systems can then access the information that has been extracted from those systems. The department has not compensated for these weaknesses by building in data checks and other controls to detect unauthorised access to information outside of the key systems.

Information is also being exchanged through internet email. This brings with it risks of unintentional disclosure to third parties if it is sent to the wrong email address.

The department also allows information to be downloaded onto removable media, such as USB memory devices. This increases the risk of unauthorised information disclosure.

Practices such as these defeat the reason behind having a purpose-built system for securing sensitive data.

Information security at non-government service providers

The NGOs we audited have acted within the intent of their service agreements to protect sensitive information, but they need to improve the security of their computer systems.

The situation is exacerbated by the fact that the department does not set minimum information security standards for its service providers on how they are to protect child safety information in electronic form. Nor does it guide them on how to manage security risks when using outsourced or cloud service providers. Lack of clear expectations in this regard in service agreements is a governance failing.

As a result, each organisation applies its own risk management and security practices. Security controls vary depending on management's knowledge of information technology. One organisation depended solely on its outsourced service provider to advise it on how to secure its information technology environment.

Reform roadmap and investment plan

In response to the Queensland Commission of Inquiry into Child Protection, the department and other service providers have commenced implementing a 10 year reform roadmap and investment plan. This is to improve support for families and the protection of children. The department has indicated that the findings and recommendations of this audit should be addressed as part of and in support of that reform program.

Recommendations

We recommend the department:

1. **develops and implements a co-ordinated model that includes a holistic approach for information management and sharing across the entire child safety service chain.**
2. **implements contemporary information systems that:**
   - **integrate the information that is held across all parts of child safety services**
   - **automate information exchange with authorised persons**
   - **are flexible and adaptable to changes in business processes**
   - **provide relevant functionality and reporting**
   - **enable the collection of relevant information and promote outcomes-based reporting**
   - **make it easier to manage multiple records on the same client within different media and in different formats.**
3. **uses information available across organisational boundaries within the service chain to gain insights and improve service outcomes. For example, to:**
   - **verify whether children not recorded as attending schools are really not attending schools and implement plans for their educational support**
   - **implement effective measures to address school attendance, suspension, exclusions, absences and abscondments to evaluate the success of its partnership with Department of Education and Training**
   - **monitor all aspects of child safety services including those where the responsibility is devolved to other government departments**
   - **establish regular monitoring processes for education support plans, health passports and transition plans**
   - **implement mandatory recording of reference keys for the Integrated Client Management System and OneSchool to ensure that information on the same child is being recorded correctly and consistently in the two systems**
   - **implement measures to improve and monitor the completion and timeliness of information about transition arrangements within the case plans and transition from care plans.**
4. **specifies the efficient and secure exchange of information as a key business requirement when selecting new systems or revising the existing system**
5. **improves security within the existing environment by:**
   - **extending secure email services in the current system to encrypt information exchange with all service providers**
   - **identifying where sensitive child safety information is stored in the file system and ensuring access controls are authorised by business owners**
   - **reviewing and updating user access levels regularly for key child safety systems**
   - **preventing transfer of sensitive child safety data from the departmental network to unencrypted, removable media (such as USB memory sticks).**
6. **develops security standards for service providers. These standards should be included in service agreements.**

Reference to comments

In accordance with s.64 of the *Auditor-General Act 2009,* a copy of this report was provided to the Department of Communities, Child Safety and Disability Services with a request for comments.

Their views have been considered in reaching our audit conclusions and are represented to the extent relevant and warranted in preparing this report.

The comments received are included in Appendix A of this report.

1 Context

The Department of Communities, Child Safety and Disability Services (the department) provides care and coordinates a number of child safety services from government and non-government organisations (NGOs). These organisations include the Department of Education and Training; schools, Hospital and Health Services; Department of Health; and 156 NGOs.

The department and child safety service providers collect, record, maintain and exchange a range of personal and sensitive information to support child safety functions. A significant amount of front line services are provided by other agencies and NGOs outside of the department. The efficient flow of information through the service chain is crucial in the safety and wellbeing of children.

1.1 Child safety services

Due to the sensitive nature of the information, all entities in the child safety service chain must keep the information confidential and secure. The department's challenge is securing this information while ensuring it is accessible to those providing care to the children and young people.

The department's response to child safety is organised into three broad phases:

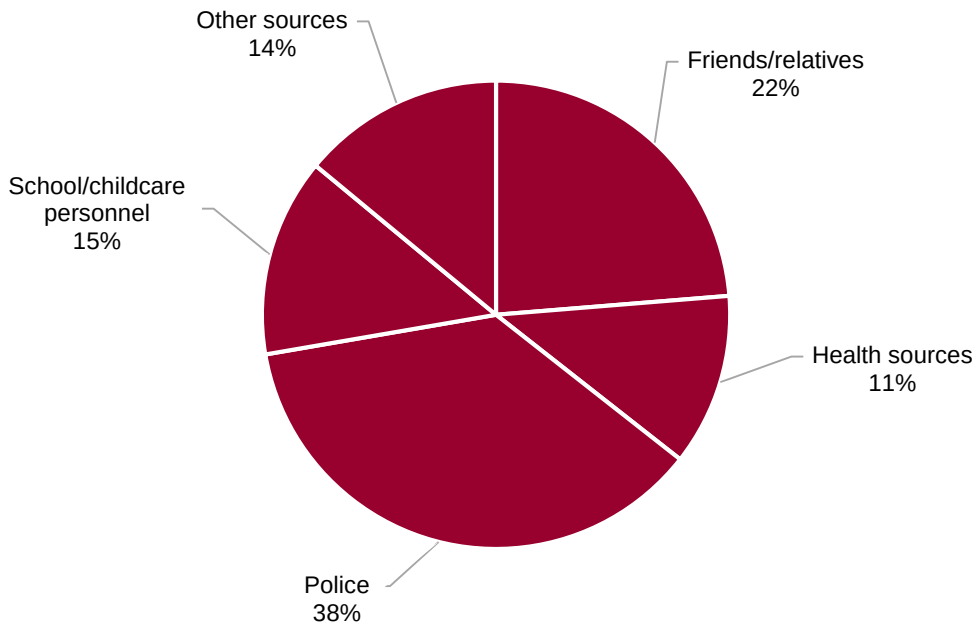
- intake
- investigation and assessment
- ongoing intervention.

Intake phase

This is the initial decision making point at which the department responds to reports about harm or risk of harm to a child. Reports about child safety concern come from a number of sources, as illustrated in Figure 1A.

During this phase, departmental officers use professional judgement and screening criteria to determine whether the child needs protection.

Figure 1A
Proportion of intakes by primary source 2013–14



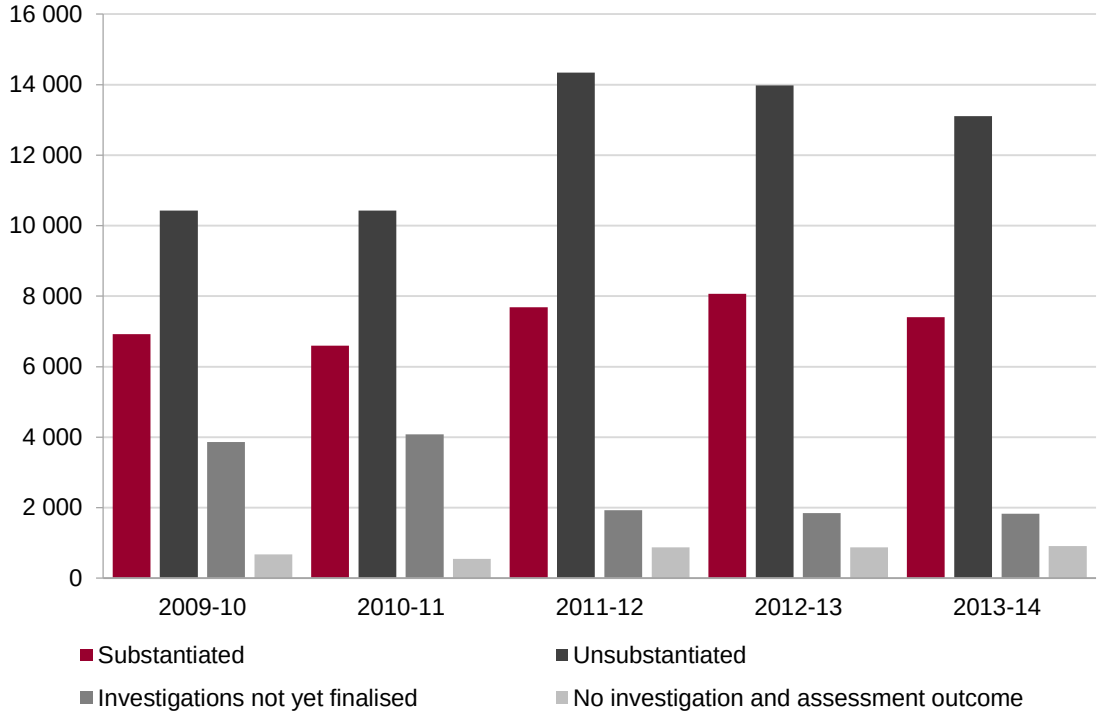
Source: Department of Communities, *Child Safety and Disability Services*

Investigation and assessment phase

In this phase, the department investigates to decide whether the child needs the department's protection or whether other agencies and NGOs can support the child and the family. Figure 1B shows the results of investigations in this phase.

Most cases are found to be unsubstantiated, which means that the child is not assessed to be in need of protection and the family can be referred to other support services where required. When the cases are substantiated and a child is found to be in need of protection, the department provides ongoing intervention for the family.

Figure 1B
Reports about harm or risk of harm to a child requiring investigation, by outcome



Source: Department of Communities, Child Safety and Disability Services

Ongoing intervention phase

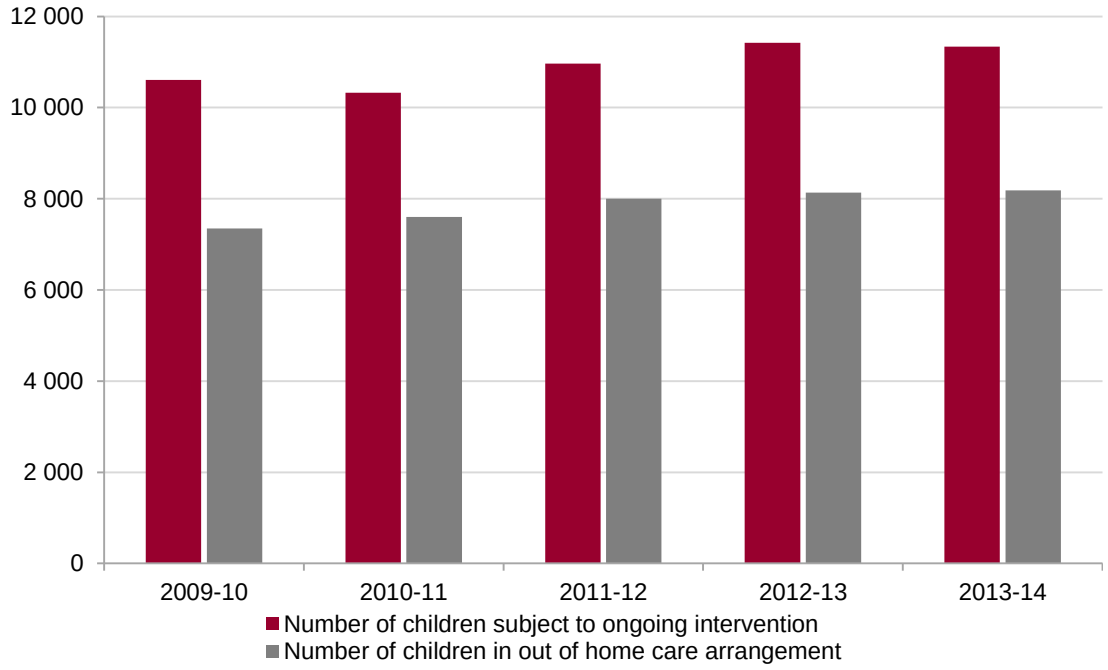
This phase is the main focus of our audit. It begins when the department has determined that the child needs protection, or assesses that the child is not in need of protection but the level of risk in the family for child safety is high. The department may need to remove a child from their home to ensure their safety.

In this case, the department uses placement services including foster carers, family members, residential care placements and safe houses. These services are coordinated through NGOs who support home-based carers or maintain residential care facilities.

As at June 2014, 11 334 children are subject to ongoing intervention. Of these, 8 185 live in out-of-home care arrangements. In this report, these children are referred to as children in care.

Figure 1C shows the number of children who progress to the ongoing intervention phase.

Figure 1C
Children subject to ongoing intervention and/or living in out-of-home care



Source: Department of Communities, *Child Safety and Disability Services*

Information associated with the children subject to ongoing intervention is managed by the department and NGOs involved in the service delivery chain. The department establishes information management practices associated with the care of these children.

1.2 Organisational roles and responsibilities

Figure 1D outlines the roles of the main entities involved in providing child safety services.

Figure 1D
Child safety service providers

Entity	Role
Department of Communities, Child Safety and Disability Services (DCCSDS)	Responsible for the protection of children and young people who have been harmed or at risk of harm. Coordinates child safety services with other service providers.
Department of Education and Training (DET)	Develops education support plans to identify education strategies for children who are: • of compulsory school age, and/or • enrolled in a school, and • subject to finalised child protection order with guardianship of DCCSDS, and • residing in out-of-home care arrangements. Participates in teams dealing with suspected child abuse and neglect when a co-ordinated multi-agency response and statutory intervention is required. Participates in multi-agency collaboration programs to support children in out-of-home care with severe and complex issues.
Non-government organisations (NGOs)	Provide placement services (out-of-home care) for children in care. Provide support services for children and families (for example, counselling and intervention services, and providing referral for active intervention and outreach support).
Hospital and health services (HHS)	Participate in teams dealing with suspected child abuse and neglect where a co-ordinated multi-agency response and statutory intervention is required. Participate in multi-agency collaboration programs to support children in care with severe and complex issues.
Queensland Police Service (QPS)	Investigates and assesses whether a child is at immediate risk of harm and investigates cases where the alleged harm may involve a criminal offence to the child. In these situations, QPS works with authorised officers from DCCSDS. Participates in teams dealing with suspected child abuse and neglect where a co-ordinated multi-agency response and statutory intervention is required.
Justice and Attorney General	Collaborates with DCCSDS when a child or young person subject to child protection intervention is also subject to youth justice services.

Source: Queensland Audit Office

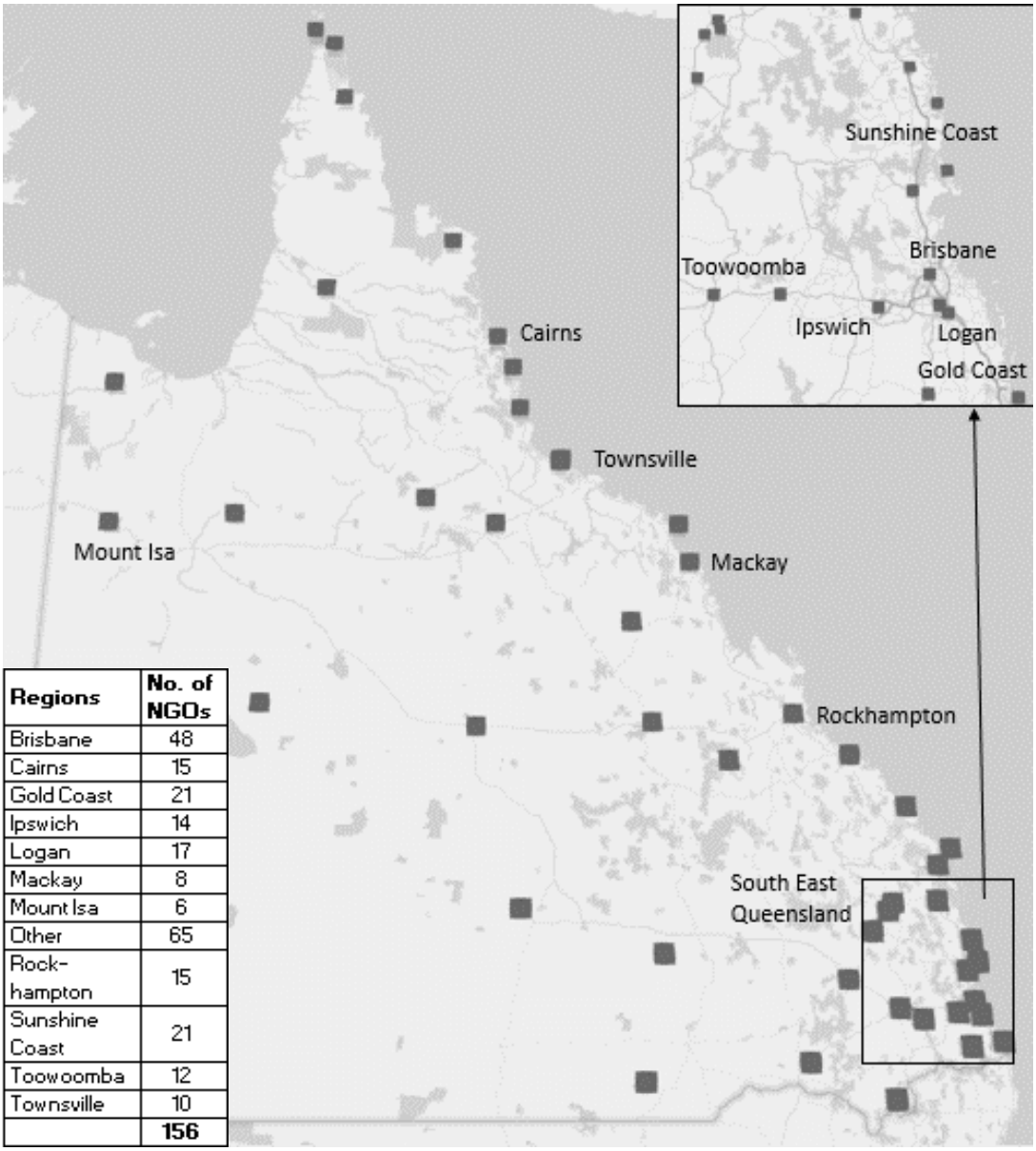
The department delivers child protection services through 55 child safety service centres across seven regions:

- Far North Queensland Region
- North Queensland Region
- Central Queensland Region
- North Coast Region
- Brisbane Region
- South West Region
- South East Region.

Figure 1E illustrates the distribution of NGOs providing child safety services across Queensland. These organisations are located in highly populated areas in Brisbane, Gold Coast and the Sunshine Coast and also extend to remote areas in Far North and Central Queensland.

The widely dispersed nature of these services brings challenges and complexities in managing information. As mentioned, some of the service centres are remotely located and information cannot always be exchanged electronically.

Figure 1E
Distribution of NGOs providing child safety services across Queensland



Regions	No. of NGOs
Brisbane	48
Cairns	15
Gold Coast	21
Ipswich	14
Logan	17
Mackay	8
Mount Isa	6
Other	65
Rock-hampton	15
Sunshine Coast	21
Toowoomba	12
Townsville	10
	156

Source: Queensland Audit Office

1.3 Key information systems

The key information systems used to record and store child safety information are described in Figure1F.

Figure 1F
Key information systems for child safety information

Entity	Systems	Description
DCCSDS	Integrated Client Management System (ICMS)	This records detailed assessment and casework information on those children, young people and families who have contact with the child protection system.
	ICMS corporate data warehouse	This is a repository of ICMS data designed to make corporate reporting and analysis easier.
	Community Sector Information System (CSIS) —previously known as the Referral for Active Intervention (RAI) System	This is a web-based referral system for early intervention services for children, young people and their families to prevent entry or re-entry into the statutory child protection system. The system is currently being used only for services provided by the NGOs in the area of referral for active intervention and family support services.
	Suspected Child Abuse and Neglect System	This is a record and repository tool for suspected child abuse and neglect meetings.
	End user computing in Excel Spreadsheets and Access databases	This is a suite of Excel spreadsheets and Access databases set up outside the core system to meet user and/or reporting requirements.
DET and Schools	OneSchool System	This systems manages information on curriculum and learning information for students attending state schools.
	Various student management systems	This is the student management systems used by Independent and Catholic schools.
Department of Health and HHS	Hospital Based Corporate Administration System	This is the patient administration system used to record all patients' (including children's) health visits.
NGOs	Various NGO case management systems/electronic records	These are the systems the NGOs use for managing child safety services.
All entities	Email systems	These are information exchange and communication systems for all entities.

Source: Queensland Audit Office

1.4 Information security classification

Information assets typically fall into two broad categories: information for public use (unclassified information); and information which requires appropriate controls to protect its confidentiality.

The department has evaluated its child safety related information assets within its systems in accordance with the Queensland Government information security classification framework. This framework sets guidelines for appropriate security grouping for information assets (see Figure 1G below).

The department has applied this classification scheme at the system level rather than to individual pieces of information and or data.

Figure 1G illustrates the government information security classification levels:

Figure 1G
Queensland Government information security classification

Information security classification	Description
Highly protected	Information assets that require a substantial degree of protection as compromise could cause serious damage to the state, the government, commercial entities or members of the public. Very little belongs in the highly protected category and this security classification level should be used sparingly.
Protected and Cabinet-in-Confidence	Information assets whose compromise could cause damage to the state, the government, commercial entities or members of the public. This level of classification also includes Cabinet-in-Confidence. As a principle, most non-national security information assets would be adequately protected by the procedures given to X-in-confidence or protected classifications.
X-in-confidence	Information assets whose compromise could cause limited damage to the state, the government, commercial entities or members of the public. X-in-confidence does not include Cabinet-in-Confidence, and all Cabinet-in-Confidence material should be treated as protected.
Unclassified	Information assets that have been assessed for security classification and do not require one of the classification levels. It may be helpful to mark information assets with this classification level so that it is known that the assessment has been made. Information which has not been assessed is best marked not-yet-security-assessed or with some similar identification and should be treated as Unclassified.

Source: Queensland Government Chief Information Office

1.5 Standards and good practice

The *Child Protection Act 1999* and *Queensland Information Privacy Act 1999* make it clear what the expectations are with regard to the protection of child safety and personal information. This legislation requires that agencies managing child safety and personal information keep that information confidential.

The agencies must also take reasonable steps to protect the information against loss, unauthorised access, use, modification, disclosure or any other misuse. These requirements extend to service providers contracted by the agencies who receive and send personal information as part of their service provision.

The *Child Protection Act 1999* stipulates that, to meet a child or young person's needs, the information must be shared in a timely and effective way. This Act states that because a child's safety, wellbeing and interest are paramount, their protection and care will take precedence over the protection of individual privacy. However, these need to be balanced with the privacy requirements contained within the *Information Privacy Act 1999*.

While Queensland legislation does not define standards for compliance with security of systems, a number of international standards exist that outline good practices for securing any system of business value. These include:

- ISO 31000:2013, *Risk management — Principles and guidelines*
- ISO/IEC 27001:2006, *Information technology — Security techniques — Information security management systems — Requirements*
- ISO/IEC 27002:2006, *Information technology — Security techniques — Code of practice for information security management*
- ISO/IEC 27005:2012, *Information technology — Security techniques — Information security risk management*
- ISACA.org, *COBIT 5: A business framework for the governance and management of Enterprise IT*

1.6 The Child Protection Commission of Inquiry

On 1 July 2012, the state government established the Queensland Child Protection Commission of Inquiry to review the entire child protection system. On 1 July 2013, the Commissioner handed down the Carmody Report on *'Taking responsibility: A Roadmap for Queensland Child Protection*'. This included 121 recommendations.

One of the recommendations was to implement a community-based intake model as one means of reducing the high volume of matters referred to the department. New community-based services, known as Family and Child Connect, are being introduced across Queensland to support families at risk of entering or re-entering the child protection system.

Family and Child Connect will lead a local alliance of government and non-government services within the community. These services will be established in 20 locations across Queensland, with the first seven operating from January 2015. The remaining sites will be rolled out in two phases from July 2015 and January 2016.

As the department implements this and the rest of the 120 Carmody recommendations, it is likely that the number of NGOs providing child safety services will increase.

Implementation of Carmody recommendations will require better information exchange processes between the department, NGOs and other agencies. Therefore, it is increasingly important for the department to clearly explain its strategy for sharing information along the service chain.

As part of its response to Carmody recommendations, the government has allocated $52.865 million over the next five years for investment in information and communication technology. It is essential that the suite of new systems promotes collaboration between all involved in the service chain, no matter how complex the relationships are.

1.7 Audit objective, method and cost

The objective of the audit is to assess whether child safety information is secure, yet available to authorised personnel who provide child safety services.

The entities subject to the audit were:

- Department of Communities, Child Safety and Disability Services
- three NGOs.

In this audit, we focused on information management for child safety services provided during the ongoing intervention phase. We did not include information provided to and from foster and kinship carers.

While other departments involved in providing child safety services were not included in the scope of this audit, we have used data from the Department of Education and Training to determine consistency and availability of information across departments.

The cost of the audit was $310,000.

1.8 Report structure

The remainder of the report is structured as follows:

- Chapter 2—Availability of child safety information.
- Chapter 3—Security of child safety information.
- Appendix A contains responses received.
- Appendix B outlines our audit approach.

2 Availability of child safety information

In brief

Background

The Department of Communities, Child Safety and Disability Services' is responsible for protecting children and young people who have been harmed or are at risk of harm. They do this through the delivery of child safety services via government and non-government entities.

The involvement of several entities in child safety services means that relevant information must be readily available to all authorised parties.

Conclusion

The right information is not always available at the right time to the department's service providers. As a result, all parties within the service chain rely on information being exchanged manually and maintain duplicate data sets.

In addition, the department cannot easily aggregate the data from all sources to analyse trends and the results of service outcomes. This makes it difficult for them to evaluate the success of child safety programs.

Key findings

- The department has invested significant resources in implementing information models for its internal use, but has been slow to address the information requirements of its service providers. We did not see evidence of continual assessment of new technology to support changing business needs.
- There is significant duplication of effort within the child safety service chain. There are more than 156 service provider recreating subsets of the same information in multiple electronic and physical forms. This is because the case management system is not designed to share information across multiple service providers.
- The lack of integrated systems also means that:
  - information from the service providers about the wellbeing of children is not easily accessible to the department
  - it is difficult to determine which system has the correct information
  - analysing information to monitor overall trends in service outcomes is a time-consuming exercise.
- Departmental officers and service providers tend to be cautious when sharing information. The disinclination to share information is compounded by technology limitations and different interpretations of child safety practices across regional areas. This results in critical information not being available when needed.
- Due to the complex way in which information is recorded and reported, significant resources and two separate teams are required within the department to generate and monitor the department's performance reporting.

Summary of recommendations

We recommend that the department:

1. **develops and implements a co-ordinated model that includes a holistic approach for information management and sharing across the entire child safety service chain**
2. **implements contemporary information systems that integrate the information held across child safety services, automates information exchange and provides relevant functionality and reporting needs**
3. **uses information available across organisational boundaries within the service chain to gain insights and to improve service outcomes.**

2.1 Background

To allow effective collaboration in the interests of children's safety, the department needs to be able to make the right information available to authorised people at the right time through the right channels.

This chapter examines whether relevant information is available to those providing services to improve the safety and wellbeing of children and young people.

2.2 Conclusion

The right information is not always available at the right time to the department's service providers. Because of varied information management practices, there is inconsistent information and service provision (under or over servicing) for children and young people in care across regional areas. The department is not providing timely information, even when service providers make repeated requests.

The main reason for the current situation is that the systems are not designed for collaboration and sharing of information. People currently need to exchange information outside the system, using emails and printing the documents for physical files. The lack of comprehensive knowledge of laws and regulations has also resulted in reluctance by organisations to exchange information because of doubts about whether or not it is lawful.

The department has not made full use of technology to aggregate individual case-based information. This would provide insights into the overall results of the child safety service. At present, inter-departmental data matching and performance reporting is time consuming and laborious. This restricts the department's ability to easily obtain simple insights into the outcomes of services.

2.3 Planning information needs

The department has not planned for the evolving information requirements of the entire child safety service chain. It implemented the Integrated Client Management System (ICMS) in response to the recommendations resulting from the 2004 Crime and Misconduct Commission Inquiry into foster care practices. One of the recommendations of the inquiry was to enable state-wide access to case notes and the department has achieved this through ICMS. Since 2004, the department has allocated funds to the ICMS project to record information relating to each case.

However, ICMS functionalities have not kept up with changes in information requirements as child safety services changed over time. Staff in regional centres have adapted by using spreadsheets and other manual methods.

In addition, the department has not analysed available information to assess service outcomes. As a result, it cannot analyse data to gain insights into the outcomes of services to children and young people in care.

For example, it is not easy to report on children and young people in care who:

- completed Year 10 and Year 12 education
- enrolled in a vocational course or employment skills development program
- gained employment and stayed employed while in care
- reunited with their families but subsequently returned to the child protection system.

Planning for information requirements is imperative as the department implements new community-based services in response to the recommendations from the Carmody Report. This is even more important as seven new services (for Family and Child Connect) have gone live and the department is selecting an appropriate vendor for a technology solution that has been targeted for go-live in July 2015.

We have not seen evidence of detailed assessment and collaborative planning to clearly specify the information requirements of the child safety service chain.

We acknowledge that the department is implementing a framework for outcome-based reporting in response to Carmody recommendations. However, the current plan does not include a holistic approach to the information requirements of all of those involved in the service chain.

2.4 Information system

The department has coordinated an investment of $85 million over the last ten years in its ICMS for child safety services. The department contributed approximately $49 million and Youth Justice Services contributed approximately $36 million.

Today, changes to the system are time consuming, due to its complex infrastructure and ageing technology. Consequently, ICMS' ability to meet changing business requirements is limited.

In particular, this limitation causes problems relating to access to information. This leads to people managing information outside of key systems (for example, through spreadsheets and databases), relying on physical records and using disparate systems.

2.4.1 Access to information

Organisations commonly use collaboration technology that allows them to build information systems for workgroups across various regions. However, the department's ICMS is not based on this type of technology. It does not allow information to be recorded once and then shared across multiple service providers.

For example, the department records information in ICMS, but then cannot share it with service providers. So they re-create a subset of the same information in their own systems. This leads to significant duplication of effort, with more than 156 service providers for placement and child support services.

While some service providers have implemented their own case management systems, these investments will not remove duplication of effort. Each service provider is implementing its own separate system with no current plans for integration with departmental systems.

Also, the department's systems do not enable officers to record events as they happen or to access information on an anywhere/anytime basis. As a result, recording and sharing information have become additional tasks to the existing workload of these officers. They have to copy information from the system into emails and print emails to keep in physical files.

2.4.2 Information outside key systems

As ICMS cannot be used by the entire child safety service chain, staff in regional offices manage information outside the key systems by creating spreadsheets and databases.

While the service agreements require service providers to report their performance accurately, the department does not have tools to verify the information they provide. This type of information cannot be generated from its Integrated Client Management System. Regional officers manage this type of information outside key systems through spreadsheets.

Part of the information is available and accessible only to the team who records the information—and not to the department itself. This increases reliance on the availability and knowledge of key staff and promotes practice variation across regional offices.

Examples of information outside of key systems include spreadsheets to record and monitor:

- referrals for out-of-home care and other services for children and young people
- funded, actual and available placement capacity for out-of-home care services
- services for children and young people with disabilities, psychological and behavioural issues provided by hospital and health services, Disability Services (another area within the department) and the Department of Education and Training.

2.4.3 Reliance on physical (hard copy) documents

The department has not adopted contemporary practice in information management by keeping electronic information in its digital form only. It relies heavily on physical documents and duplication of effort, as both the department and service providers print and store all electronic records, emails and manual information in physical files.

Although the department requires the service providers to return physical files at the end of the service to a child or young person, it has not made clear the procedures for these returns. One of the three service providers audited has never returned their files to the department and has only recently started investigating file return procedures.

Heavy reliance on physical files also increases the risk of the department and service providers being unable to recover the information in the event of a disaster that destroys the physical files.

2.4.4 Disparate systems

The lack of integrated systems to record and share information with service providers also means that the service providers' information is not readily available and transparent to the department. The service providers regularly report the progress and wellbeing of the children. This information, however, is not always recorded in the ICMS. Therefore, the department cannot use this information centrally to assess service outcomes.

Having disparate systems and physical files has resulted in duplication, inconsistency and out-of-date information in some systems. This raises the question of which system contains the correct information.

For example, there is no assurance that the department has an accurate record of school information for children in care. As at November 2014, there were 1 009 school-age children (around 18.5 per cent of the total) whose school records in the department's system (ICMS) were different from those recorded in the Department of Education and Training system (OneSchool).

In addition, there is a significant number (1 628—around 30 per cent of the total) of children in care whose residential addresses are not consistent between ICMS and OneSchool.

2.5 Information management

The nature and type of information made available to service providers depends on how well the department's staff understand child safety practices and legislation. The department provides a practice manual but this is interpreted and applied differently across different regional areas. As a result, some of the significant elements of child safety information are not recorded or exchanged with service providers.

The inconsistent recording of information has affected front line child safety services including education and transition from care.

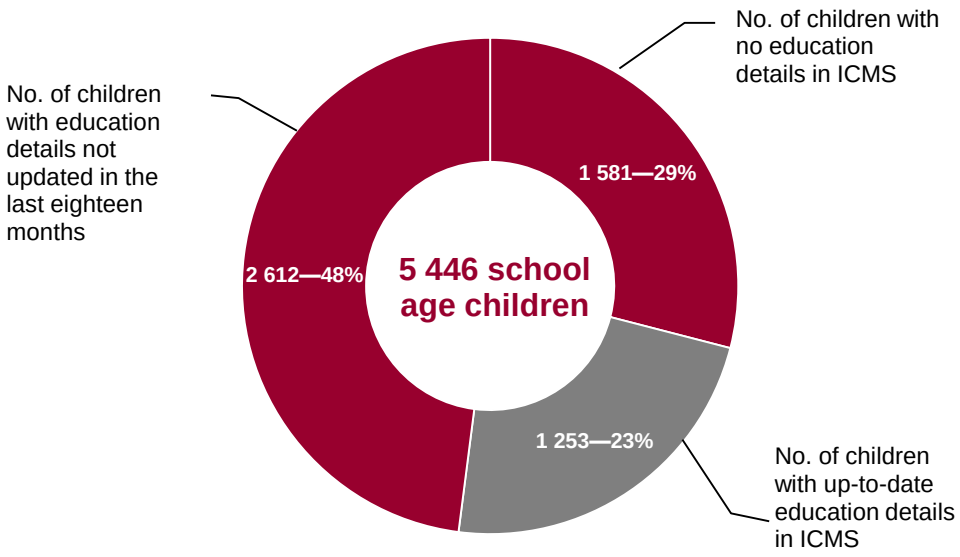
2.5.1 Children and young people's education

There is no way for the department to easily monitor the overall trend of children and young people's school attendance, for example their suspensions and exclusions from school and their record of abscondment from school. This limits the department's ability to formulate targeted strategies to improve the overall education outcome for children in care and to assess how well the department is discharging its legal obligation to ensure children are attending school.

The department's case officers review the education needs of children and young people through individual case plans and education support plans. However, they do not always record education details in ICMS or keep them updated. Figure 2A shows that as at November 2014, 29 per cent of school age children in care did not have education details in ICMS and 48 per cent had education details which had not been updated in the last eighteen months.

The Department of Education and Training systems did not have enrolment records for 1 430 school age children in care. Without examining each of the 1 430 children's individual records, it is difficult for the department to know whether these children are attending school.

Figure 2A
Currency of education details of school age children



Source: Queensland Audit Office from data obtained from the Department of Communities, Child Safety and Disability Services

The Department of Communities, Child Safety and Disability Services and the Department of Education and Training also provide education support funding for children who are eligible for an education support plan. To find out which of the eligible children and young people are receiving this support, the department conducts data matching with the Department of Education and Training system (OneSchool).

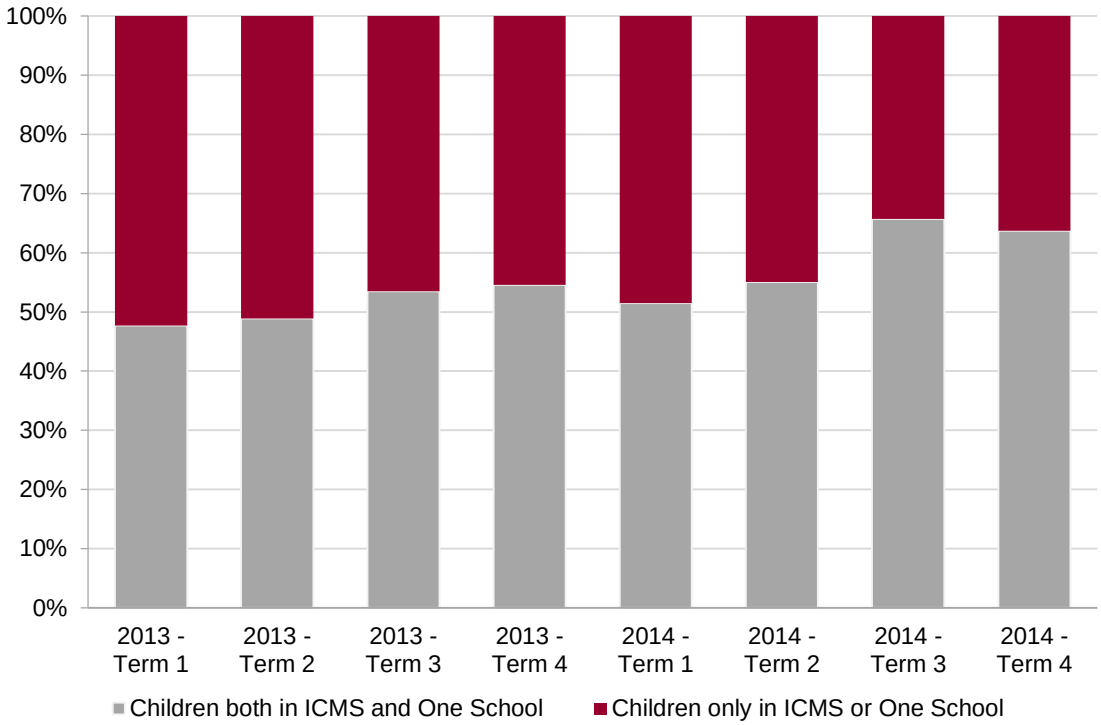
This process is manual, inefficient and so time consuming that by the time it is completed, the data in the report is out of date. This has led to under and over provision of child safety educational support. Children eligible for education support plans do not always receive assistance at school while some who are not eligible obtain assistance.

Figure 2B shows the inconsistencies in information recorded in the department's system when compared with the Department of Education and Training systems.

As at 31 October 2014, there were 1 401 children identified in ICMS as requiring education support plans but not identified as receiving education support plans in the Department of Education and Training's system.

Similarly, there were 519 children identified as receiving education support plans in the Department of Education and Training system who were not eligible for education support plans according to ICMS.

Figure 2B
Education support plan data matching



Source: Queensland Audit Office from data obtained from the Department of Communities, Child Safety and Disability Services

The main causes for the difference between the two systems include:

- Officers from both departments do not always understand the eligibility criteria for education support plans.
- The department does not always provide schools with timely advice of changes affecting eligibility for education support plans.
- The department's systems do not have alerts set up to report on new children requiring an education support plan.
- Reference keys that identify children in ICMS and OneSchool are not consistently used in either system.
- The Department of Education and Training uses manual processes to compile information about students enrolled at Independent and Catholic schools and cannot provide full details for matching data. This impacts on the accuracy of the results.

While both departments have spent significant funding on their respective systems, neither has prioritised automated data matching for children and young people in care.

In addition, the department has not addressed the main causes that contribute to such discrepancies. Until the main causes are addressed, inconsistent records in ICMS and OneSchool will continue to exist and the data matching process will not achieve its intended purpose of ensuring that children who are eligible for education support plans are receiving them.

2.5.2 Transition from care

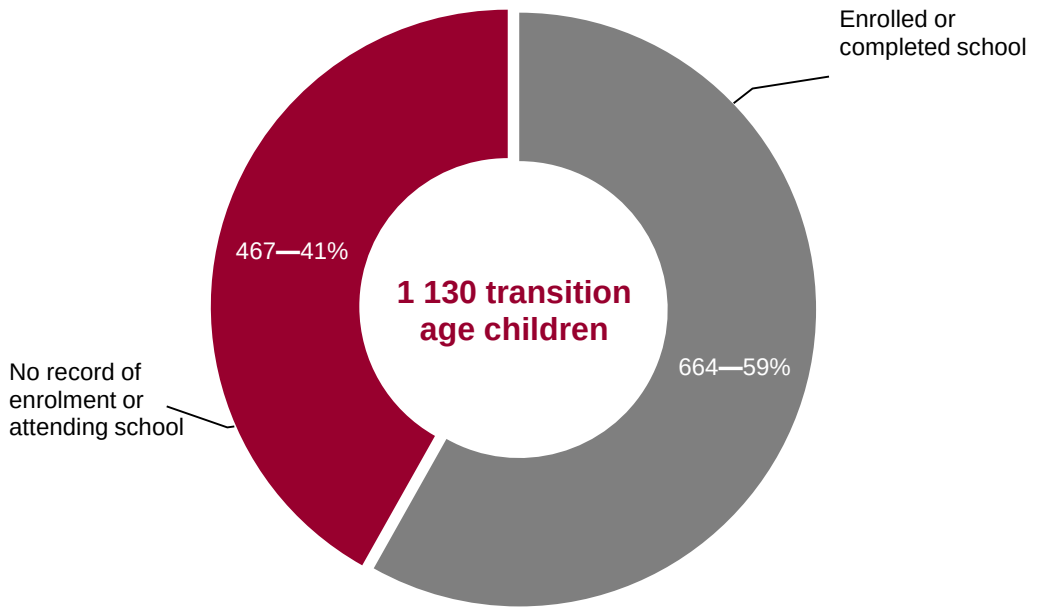
Transition from care happens at the age of 18, when a young person in care becomes an independent adult within the general community. Planning for transition from care begins as part of the ongoing case management when a young person turns 15.

The service providers advised us that, overall, the case plans are not detailed enough to support young people in transitioning from being a child in care to becoming an independent adult within the general community.

The ICMS includes features to record whether transition planning has occurred. As at October 2014, about 1 130 children and young people in the custody or guardianship of the department were in the transition age group (15–17 years old). In ICMS, about 420 of these young people did not have a transition plan incorporated into their case plan.

In addition, the department does not use this information to find out whether these young people are still in school. This is critical information to help decide how well the young person will transition into an independent adult. The Department of Education and Training data shows that 41 per cent of young people at transition age are not recorded as attending school. This is depicted in Figure 2C.

Figure 2C
Transition from care—education details



Source: Queensland Audit Office from data obtained from the Department of Communities, Child Safety and Disability Services and Department of Education and Training

2.5.3 Information sharing

All of the parties within the child safety service chain that we audited understand the importance of keeping information confidential, but departmental officers and service providers have different levels of understanding about the importance of sharing relevant information. This results in a disinclination to share information, which is compounded by technology limitations.

Organisations providing safe houses and residential care facilities do not always receive critical documents on time when children or young people are placed in an out-of-home care arrangement with them. These documents include the authority to care, which provides the basis for the carer to legally care for the child, and the case plan, which provides relevant information about the child's needs and goals while in care.

As a result, the provision of this information depends on the knowledge and diligence of child safety officers and child safety service centres.

While departmental policies outline the range of information to be provided to carers, the onus is on service providers to request essential information. The department is aware, from the audits it conducted, that service providers often do not receive relevant information. In one of the cases that we sampled, the service provider repeatedly requested a case plan and the department advised that the child did not need a case plan. The department's audit on the service provider subsequently raised an exception for not having the case plan.

Service providers have not always received critical information such as:

- The education support plan that identifies educational goals and targets and strategies for the child. None of the service providers we audited received education support plans.
- The health passport that contains the information the carer requires to meet the health needs of the child. None of the children or young people in residential care and safe houses that we audited had a health passport, even though the health passport must move with the child whenever the child moves to a new placement.
- Detailed information about transition arrangements as part of the case plan to support the gradual transition of children returning to the care of their parents.

The department's technological limitations on recording and sharing information often gives the people working in the child safety chain the perception that information management is just another administrative requirement. They have difficulty seeing how it contributes to services to children and young people, so they do not always record data in the appropriate format.

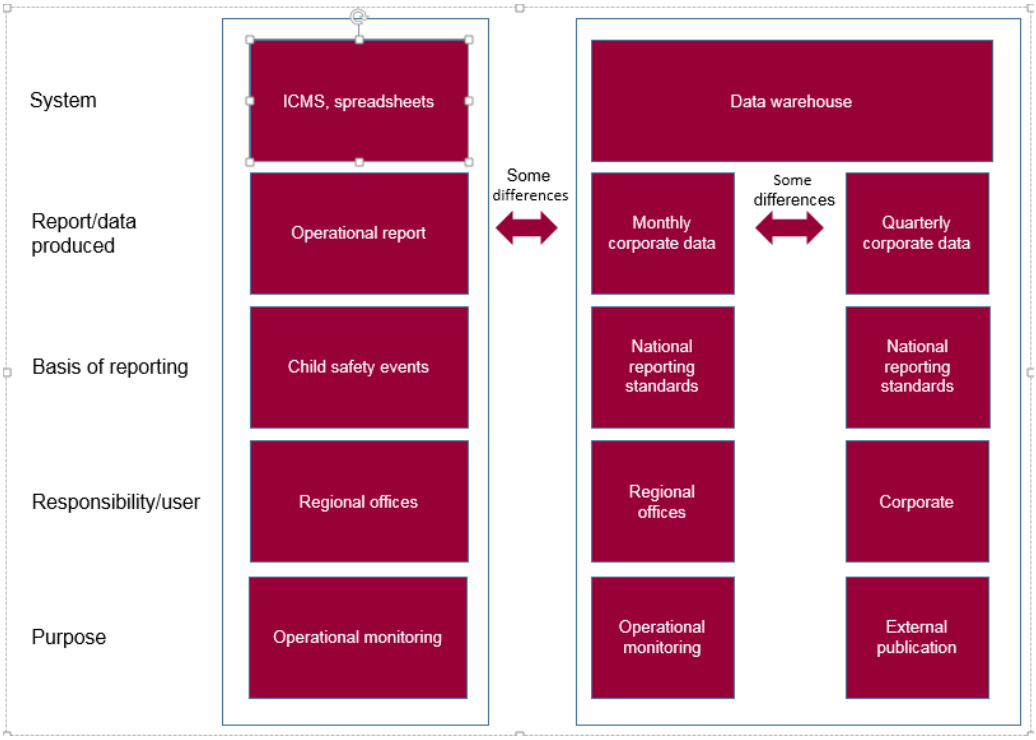
Being careful not to impose an additional burden on child safety officers, the department does not address data issues when data is recorded. Rather, the department employs extra administrative staff or incorporates system-based rules to 'fix' data quality issues in the system. While this approach provides a temporary solution, it creates inefficiencies in the long term.

In contrast, one of the service providers implemented a built-in application control whereby case notes are automatically finalised within seven days of creation. This encourages timely completion of case notes and momentum for completion. The application also includes processes to review the quality of recorded data.

2.5.4 Performance reporting

The department's performance reporting is complex, time consuming and requires significant resources. Corporate performance reports are produced in accordance with national reporting standards, which are different from internal reporting rules. As a result, the figures in the published reports are not the same as those in the departmental reports, as illustrated in Figure 2D.

Figure 2D
Comparison of department's operational and corporate reporting



Source: Queensland Audit Office.

Separate teams within corporate (head) office and the regions generate various performance reports for the department. The Planning and Performance Unit uses significant resources within corporate office to generate:

- monthly corporate data for each regional office. This is used to monitor operational performance reporting
- quarterly corporate data. This is quality assessed per national reporting standards for on-line publication.

Each regional office monitors and reports its monthly performance using:

- monthly corporate data by region, provided by the Planning and Performance Unit
- a combination of standard operational reports and local spreadsheets and databases. The regional offices each have their own 'data guru' to assist in creating and manipulating spreadsheets and databases to meet their reporting needs.

The difference between corporate and regional reports is mainly due to different rules being applied to data sets and delays in data entry for up to two months after the end of the reporting period. It takes the department at least three months to report and publish quarterly results.

As at the end of December 2014, the September quarterly results were not published or available for audit. As a result, we are only able to verify information based on June 2014 data, even though our analysis of ICMS data is as at 30 October 2014.

2.6 Recommendations

We recommend that the department:

1. **develops and implements a co-ordinated model that includes a holistic approach for information management and sharing across the entire child safety service chain**
2. **implements contemporary information systems that:**
   - **integrate the information that is held across all parts of child safety services**
   - **automate information exchange with authorised persons**
   - **are flexible and adaptable to changes in business processes**
   - **provide relevant functionality and reporting**
   - **enable the collection of relevant information and promote outcomes-based reporting**
   - **make it easier to manage multiple records on the same client within different media and in different formats**
3. **uses information available across organisational boundaries within the service chain to gain insights and improve service outcomes. For example, to:**
   - **verify whether children not recorded as attending schools are really not attending schools and implement plans for their educational support**
   - **implement effective measures to address school attendance, suspension, exclusions, absences and abscondments to evaluate the success of its partnership with Department of Education and Training**
   - **monitor all aspects of child safety services including those where the responsibility is devolved to other government departments**
   - **establish regular monitoring processes for education support plans, health passports and transition plans**
   - **implement mandatory recording of reference keys for the Integrated Client Management System and OneSchool to ensure that information on the same child is being recorded correctly and consistently in the two systems**
   - **implement measures to improve and monitor the completion and timeliness of information about transition arrangements within the case plans and transition from care plans**

3 Information security

In brief

Background

All organisations that share sensitive information in delivering child safety services are required to keep this information confidential. Consequently, these organisations need to take reasonable steps to keep personal information secure.

Conclusion

The Department of Communities, Child Safety and Disability Services cannot be certain that child safety information is kept confidential. Although it has secured the key systems, information extracted from the main systems is not always securely transferred and it is accessible to unauthorised staff.

The non-government organisations have acted within the intent of their service agreements to protect sensitive information. However, they need to improve the security of their information technology environments.

Key findings

- All entities subject to this audit have risk management practices in place, with senior management oversight and monitoring of information technology risks.
- The department has implemented good controls to secure the key information systems used to manage child safety information. However, due to system limitations, information is often extracted from key systems and put into spreadsheets. These can be accessed by people who do not have access to the key systems. In addition, information is also being exchanged through internet email with the attendant risks of unintentional disclosure to third parties if sent to the wrong email address.
- Staff retain access to child safety information when they no longer need it because the department does not reliably amend information systems access.
- All of the entities audited carry a risk of data disclosure because they allow the use of removable media and mobile technology.
- The department does not set minimum information security standards on how to protect child safety information that exists in electronic form for its service providers. Nor does it guide them on how to manage security risks when using outsourced or cloud service providers.

Summary of recommendations

We recommend that the department:

4. **specifies the efficient and secure exchange of information as a key business requirement when selecting new systems or revising the existing system**
5. **improves security within the existing environment by extending secure internet email services, ensuring access to sensitive information is authorised, performing regular user access reviews and preventing transfer of sensitive data via removable media**
6. **develops security standards for service providers. These standards should be included in service agreements**

3.1 Background

Unauthorised access to or disclosure of child safety information can pose grave risks to the safety and best interest of a child. All entities delivering child safety services are required to keep personal information confidential.

In assessing the security of child safety information, we have examined the control environments used to store and exchange child safety information within the department and within three non-government organisations (NGOs).

The key areas we examined are whether:

- there is effective oversight and monitoring of information technology risks
- information technology controls are maintained to prevent unauthorised access or modification
- there is an effective response when security breaches are detected.

3.2 Conclusions

The Department of Communities, Child Safety and Disability Services (the department) has formal risk management processes for the child safety information it stores. Information technology security risks are identified, reported and monitored by appropriate levels of senior management. However, risks relating to information exchanged with and stored by its service providers requires stronger departmental oversight.

The department has secured its information technology environment to protect child safety information stored within key systems. However, staff frequently extract information from the key systems and put it into more useable formats such as spreadsheets. Once information is extracted, it is not secure and the department cannot hold staff accountable for any unauthorised access to or disclosure of sensitive information. Information exchanged with service providers via email is not a safe approach for sensitive information.

All of the NGOs we audited have acted within the intent of their service agreements to protect sensitive information relating to child safety services. However, they need to improve the security of their information technology environments to be in line with industry standards. The department has formally communicated its expectations that service providers are to comply with legislation, but it has not set minimum standards for them on how to protect this information, nor on how to manage security risks when using outsourced or cloud service providers.

Risk management processes within each of the NGOs we visited differ, depending on their size and beliefs on how risks are to be managed. Two of the NGOs have risk management processes appropriate for the size of the organisations. In these organisations, senior management monitors information technology risks. One of the NGOs audited has identified and recorded information risks, but has not finalised plans to address several risks identified, the target risk levels or timeframes for remedial actions.

3.3 Security management

Security management means designing, implementing and monitoring the controls necessary to mitigate information security risks to an acceptable level and cost. It includes a broad range of information technology and procedural controls. Security management starts with classifying information assets in terms of the level of protection they require.

3.3.1 Information security classification

The department uses five main information systems for child safety and has used the Queensland Government information security classification framework to classify the systems. The sensitivity of the information and systems classification has guided the design and operation of the control environment.

The department did not include a requirement to classify government information in the service level agreements with external service providers. Consequently, the NGOs did not expressly classify their systems and information according to the government's classification scheme.

Two of the organisations we audited protected the information records in line with their sensitivity. One of the organisations deployed access restrictions and relied on outsourced information technology service providers to maintain security controls.

3.3.2 Information technology security controls

Overall, the department has security controls to protect information technology systems, their infrastructure and mobile devices in line with good practice guidelines. This includes identifying security weaknesses and having a prioritised program of corrective activities to address the weaknesses.

The department has documented security controls in policies, procedures, system architectures and system design documents. A security awareness program is also in place to ensure staff members are aware of their role in protecting information and the secure use of information technology.

The use of information technology differs among the NGOs we audited, so the level and nature of risk exposures were different for each organisation.

All of the NGOs we audited have implemented good practice information technology controls. However, some key controls are not enabled. The nature and extent of control deficiency varies across the organisations.

At one of the organisations, we identified a risk of unauthorised access by hackers. To address this risk, the organisation undertook, during the audit, to review their internal network design and user access and password policies. The organisation also needs to tighten controls relating to information technology administrator accounts and virus management.

The other two organisations need to improve their user passwords and access controls. They also need to tighten internet security controls.

3.3.3 Information exchange

Due to the limitations in the department's key child safety systems on making information available to other service providers, emails are used extensively to exchange information.

The department has acted to protect emails being sent through the internet. Email messages between the organisations we audited and the department are encrypted to prevent unauthorised disclosure to internet hackers. However, the scheme does not protect against disclosure of sensitive information if emails are accidentally addressed to an incorrect addressee.

The department has trialled a newer 'secure email' service in one of its business units but this is not used for exchanging information with service providers.

3.3.4 User access management

Each of the five information systems we assessed has well-designed controls to restrict access to only authorised persons. Two of the key systems have the ability to restrict access to individual cases. Each user has a unique identifier and the systems record user activities so that individual users can be held accountable for access and use of electronic information. While child safety information is within these key systems, it is well protected.

However, in two regional offices, sensitive data has been extracted from key information systems and stored in spreadsheets and Access data bases. Staff who did not have access to the key systems could access the extracted information.

For example, only nine staff members from one regional office had access to data within the key system but 184 users had access to the same data extracted into a spreadsheet. The department did not record access to the extracted files. Consequently, users accessing sensitive data in spreadsheets could not be held accountable for their actions.

User access is not reliably amended when staff no longer require access. In one system, 80 per cent of the user accounts corresponded to current employees who no longer require access. The department detected and corrected this for two information systems. The large proportion of unnecessary access, however, indicates that user reviews are not done in time to detect and correct unnecessary information system access.

All of the NGOs we audited restricted access to authorised individuals only and maintained records of authorisation decisions. However, access to some electronic information records was not recorded, so it was not possible to hold staff accountable for accessing sensitive information. One of the organisations began logging access to information during the audit.

3.3.5 Use of removable media

All of the entities we audited carry risks of data loss via removable media or use of mobile technology. The department allows removal of data via removable media such as USB memory sticks. When sensitive data is transferred onto removable media it should be encrypted to protect it from disclosure if accidentally left in a public place, lost or stolen.

The NGOs did not store files on mobile devices such as phones or laptops, but copies of emails are stored on phones and laptops. Phones and laptop computers have screen locks and passwords, but data encryption is not used to prevent unauthorised disclosure if a mobile device is stolen. Data on a stolen or lost laptop computer can also be read on any other computer by simply transferring the hard drive.

3.3.6 Security guidance

The department does not guide its service providers on how to comply with information security standards required for departmental information. Nor does it provide guidance on the types of assurances the NGOs should be seeking from their service providers. There are about 156 NGOs for child safety services and they are increasingly using cloud computing and outsourcing. This adds complexity and increases information security risks.

Each of the NGOs we audited uses an outsourced service provider for part or all of its information technology. These NGOs have not obtained formal assurances from their service provider that the required levels of security controls have been implemented.

Two of the NGOs use cloud services from Telstra and Microsoft. Their service agreements do not guarantee that personal information will not be accessed, transmitted or stored overseas.

3.3.7 Records retention

Service providers do not have clear policies outlining requirements for data retention. The current process is to retain electronic records indefinitely for two of the three NGOs we audited. While this is a good short term strategy, there is an increased risk of unauthorised disclosure of information as the data builds up over time. Also, it includes information about children and young people who may no longer be using the services of that organisation.

3.4 Responding to security breaches

The department has a policy and technical procedures for responding to real or suspected security breaches. Staff are familiar with their roles and responsibilities outlined in these documents. The Information Security Branch assesses and reports on incident trends to a management committee. Of the known and recorded incidents, there was no evidence of systematic failures requiring management intervention.

The NGOs have informal response plans to suspected security breaches. While their current Information technology staff are technically knowledgeable, there is a risk that a technical response to a security breach may not meet the expectations of the department.

3.5 Recommendations

We recommend that the department:

4. **specifies the efficient and secure exchange of information as a key business requirement when selecting new systems or revising the existing system**
5. **improves security within the existing environment by:**
    - **extending secure email services in the current system to encrypt information exchange with all service providers**
    - **identifying where sensitive child safety information is stored in the file system and ensuring access controls are authorised by business owners**
    - **reviewing and updating user access levels regularly for key child safety systems**
    - **preventing transfer of sensitive child safety data from the departmental network to unencrypted removable media (such as USB memory sticks)**
6. **develops security standards for service providers. These standards should be included in service agreements.**

Appendices

Appendix A— Comments **37**

Comments received from Director-General, Department of Communities, Child Safety and Disability Services 38

Appendix B—Audit details **45**

Appendix A—Comments

In accordance with s.64 of the *Auditor-General Act 2009*, a copy of this report was provided to the Department of Communities, Child Safety and Disability Services with a request for comment. Their response has been included in full.

We also sent extracts of the report to the Department of Education and Training and to the Minister for Education, Tourism, Major Events, Small Business and the Commonwealth Games, where the Department of Education is referred to.

The Department of Education (DET) was concerned whether the report provided adequate explanation relating to the limitations of the data and what is being measured. Specifically whether the 41% of young people in transition age group not recorded as attending school included:

- those attending an alternative education program
- attending Catholic or Independent school
- in part-time or full-time employment
- undertaking a course at TAFE or another registered training provider; or
- in apprenticeships or traineeships.

We advised DET that information about whether the 41% of young people in the transition age group were in any of the above categories was not available. In addition, we informed DET that the context in the report is that DCCSDS does not use this type of information to find out whether these young people are in school.

DET commented that the report highlights the challenges faced by DCCSDS in providing accurate and timely information and outlines the issues that DET experiences in trying to obtain accurate data from Child Safety Officers in DCCSDS, in order to provide education support plans for students who are eligible for support.

DET also commented that it has invested significant time and resources into improving the accuracy of the data in the OneSchool system, but maintaining accurate data has proved challenging due to the complexity of this cohort of students and the frequent changes to the living arrangements experienced by some of these students. Officers from DET and DCCSDS are continuing to work towards resolving the issues around the accuracy of the data in both systems, and to find solutions that are practical and are not administratively burdensome for schools or DCCSDS.

A copy of the full report was provided also to the Minister for Child Safety, and the Premier, for their information.

Comments received from Director-General, Department of Communities, Child Safety and Disability Services

Queensland Government

Office of the
Director-General

Department of
Communities, Child Safety and Disability Services

Your reference: 2015-P9124
Our reference: COM 02832-2015

14 MAY 2015

Mr Andrew Greaves
Auditor-General
Queensland Audit Office
PO Box 15396
CITY EAST QLD 4002

Dear Mr Greaves

Thank you for your letter providing a copy of the proposed final report of the performance audit on managing child safety information. I appreciate the opportunity to respond to the recommendations made by the Queensland Audit Office (QAO).

The Department of Communities, Child Safety and Disability Services (DCCSDS) is aware of the important and complex balance between information sharing, information privacy and information security in the area of child safety service provision. Departmental staff work in a framework where the best interests of children and young people are paramount. Child protection involves complex decisions on when, and the extent to which, sensitive information should be shared with other government or non-government agencies.

In response to the Queensland Child Protection Commission of Inquiry, the department and other service providers have commenced implementation of a 10-year reform roadmap and investment plan to improve support for families and the protection of children, and to improve the operation of child safety services. The findings and recommendations of this audit will be addressed as part and in support of the reform agenda, and the department will work with relevant partners to co-design and co-deliver appropriate strategies.

The department has reviewed the QAO report in detail and accepts the need to continue to improve our practices and systems to better manage child safety information. DCCSDS agrees with all of the report's recommendations. Work is already underway that will contribute to implementation in relation to four of the six recommendations. Work will commence in the near future on the other two recommendations, as indicated in the enclosed response.

The department has developed a Digital Strategy and commenced work on a key component, a Data Governance initiative, to ensure data is managed as an enterprise asset, including the classification and documentation of data flows across our service streams.

13th Floor 111 George Street
Brisbane Queensland 4000
GPO Box 806 Brisbane
Queensland 4001 Australia
General Enquiries
Telephone +61 7 3235 4312
Facsimile +61 7 3235 4327
Email dgoffice@communities.qld.gov.au
Website www.communities.qld.gov.au

Comments received from Director-General, Department of Communities, Child Safety and Disability Services

This initiative will include an Information Management model for child safety, and a child safety Information Management practice framework with appropriate tools and training, developed and delivered in conjunction with other agencies and the non-government sector.

Some other initiatives already being undertaken by the department include:

- New business processes, in line with the Child and Family Reforms, which improve secure information access and exchange between non-government organisations and the department, department to department and NGO to NGO.
- National data sharing projects including School Enrolment and Attendance, Child Health Outcomes, Homelessness vulnerability, Intergenerational vulnerability and Service System mapping being progressed under the National Framework for Protecting Australia's Children; as well as the E-health records project for children in out-of-home care, in conjunction with the National Health Information Regulatory Framework Working Group.
- Partnership with National ICT Australia to assist with design of a new information sharing paradigm between DCCSDS and the Department of Education and Training, including a personal identification and matching process.
- Continued expansion of a number of secure information exchange solutions such as the Cisco Registered Envelope Service to allow the secure exchange of information via email and the Axway solution to allow the secure exchange of documents.
- Regular reviews of system access and progress towards the introduction of a new access procedure to remind users of their responsibility for indicating their need to be removed from the service when they cease employment in that service area.

A high-level action plan has been developed in accord with the enclosed responses to recommendations made by the QAO. Implementation will be dependent on the availability of resources and the suitability of solutions available in the market to deliver desired functionality. A senior departmental officer will lead and facilitate development of a joint detailed implementation plan with relevant agencies and the non-government sector. Departmental staff will continue to work with officers from QAO to report on the status of implementation.

If you require any further information or assistance in relation to this matter, please do not hesitate to contact Mr Matthew Lupi, Executive Director, Child and Family Services, Department of Communities, Child Safety and Disability Services on 3224 2423.

Thank you for the opportunity to respond to this report.

Yours sincerely

Michael Hogan
Director-General

Enc (1)

Responses to recommendations

Responses to recommendations

Responses to recommendations provided by the Director-General, Department of Communities, Child Safety and Disability Services.

Responses to recommendations

No	Recommendation	Agree/ Disagree	Timeframe for Implementation	Additional Comments
1.	Develops and implements a co-ordinated model that includes a holistic approach for information management and sharing across the entire child safety service chain.	Agree	Commence July 2015. Review progress June 2016.	DCCSDS will lead the development of a coordinated model and joint implementation plan with other agencies and NGOs. Additionally, a child safety Information Management practice framework will be developed and appropriate tools and training delivered. As a component of the data governance initiative, DCCSDS, in conjunction with other government agencies and NGOs, is developing a system-wide performance management framework to define the roles and responsibilities of key stakeholders in the management of service delivery across all child protection sectors. Procurement of a new information system for major components of the secondary sector is under consideration. Progress on this and following recommendations and responses will be dependent on availability of resources and the suitability of solutions available in the market to deliver desired functionality.
2.	Implements contemporary information systems that: • integrate the information that is held across all parts of child safety services • automate information exchange with authorised persons • are flexible and adaptable to changes in business processes • provide relevant functionality and reporting • enable the collection of relevant information and promote outcomes-based reporting • make it easier to manage multiple records on the same client within different media and in different formats	Agree	Commence May 2015. Review progress June 2016.	DCCSDS supports this recommendation and will ensure future information systems requirements reflect the recommendations in this section of the report.

Responses to recommendations

3.	Uses information available across organisational boundaries within the service chain to gain insights and improve service outcomes. For example, to:	Agree		
	• verify whether children not recorded as attending schools are really not attending schools and implement plans for their educational support.	Agree	Commence June 2015. Review progress December 2015.	DCCSDS and DET are currently working together to improve information exchange related to school attendances, as outlined in this recommendation. The MOU will be reviewed in 2015. This review will explore strategies to improve the reporting and evaluation of educational outcomes for children and young people in care.
	• implement effective measures to address school attendance, suspension, exclusions, absences and abscondments to evaluate the success of its partnership with Department of Education and Training	Agree	Commence July 2015. Review progress December 2015.	
	• monitor all aspects of child safety services including those where the responsibility is devolved to other government departments	Agree	Commence July 2015. Review progress December 2015.	Existing governance arrangements monitor all aspects of child safety services. DCCSDS will identify gaps and improve practices.
	• establish regular monitoring processes for education support plans, health passports and transition plans	Agree	Commence July 2015. Review progress December 2015.	
	• implement mandatory recording of reference keys for the Integrated Client Management System and OneSchool to ensure that information on the same child is being recorded correctly and consistently in the two systems	Agree	Commence May 2015. Review progress June 2016.	DCCSDS will work with EQ to consider the best approach to implement this recommendation. It is noted that not all children will have an EQ ID (i.e. not all children are in state schools) therefore mandatory reference key may not be in itself able to deliver a complete solution. DCCSDS will consult with DET and other school sectors on the range of measures required to improve data matching across all sectors.
	• implement measures to improve and monitor the completion and timeliness of information about transition arrangements within the case plans and transition from care plans	Agree	Commence July 2015. Review progress December 2015.	

Responses to recommendations

No	Recommendation	Agree/ Disagree	Timeframe for Implementation	Additional Comments
4.	Specifies the efficient and secure exchange of information as a key business requirement when selecting new systems or revising the existing system	Agree	Commence May 2015. Review progress June 2016.	DCCSDS will ensure future information systems requirements reflect a need for the efficient and secure exchange of information.
5.	Improves security within the existing environment by:			
	• extending secure email services in the current system to encrypt information exchange with all service providers	Agree	Commence May 2015. Review progress January 2016.	DCCSDS currently has a secure email service available to staff (Cisco Registered Envelope Service) and will commence extending the usage and marketing of this product, particularly to Child Safety Services. DCCSDS will work with NGOs to build their capability to send secure emails.
	• identifying where sensitive child safety information is stored in the file system and ensuring access controls are authorised by business owners	Agree	Commence May 2015. Review Progress December 2015.	DCCSDS will work towards migrating sensitive child safety information into an Electronic Document Records Management System (eDRMS) and explore expanding current access controls to self-service access controls by business owners.
	• reviewing and updating user access levels regularly for key child safety systems	Agree	Commence May 2015. Review progress December 2015.	Regular user access reviews of sensitive information systems have commenced in the 2014–2015 financial year.
	• preventing transfer of sensitive child safety data from the departmental network to unencrypted, removable media (such as USB memory sticks)	Agree	Commence May 2015. Review progress January 2016.	DCCSDS requires the use of an encrypted USB and is implementing an event notification pop-up window to inform users of their responsibility when transferring sensitive or confidential information.

Responses to recommendations

No	Recommendation	Agree/ Disagree	Timeframe for Implementation	Additional Comments
6.	Develops security standards for service providers. These standards should be included in service agreements.	Agree	Commence June 2015. Review progress January 2017.	DCCSDS is amending its "Basic Recordkeeping Guide" to ensure it is expanded to cover Information Security (ISO27000 series) and Recordkeeping (IS40) and contemporised for recent information technology developments such as cloud-based storage of data. The department will incorporate compliance with the revised Guide into the DCCSDS Investment Specifications and funding agreements, and will monitor compliance through the Human Service Quality Framework. The Basic Recordkeeping Guide is available at http://www.communities.qld.gov.au/resources/childsafety/partners/funding/documents/ngo-recordkeeping-guide.pdf

Appendix B—Audit details

Audit objective

The objective of this audit was to assess whether child safety information is secure, yet available to authorised personnel who provide child safety services.

The objective of the audit was addressed through the sub-objectives and lines of inquiry as shown in Figure B1.

Figure B1
Audit Scope

Sub-objectives		Lines of inquiry
Controls to prevent, detect and respond to security breaches are effective.	1.1	There is effective risk management, oversight and monitoring of the security of child safety information.
	1.2	The network architecture, physical and technical controls are designed, implemented, and maintained to protect child safety information from unauthorised access.
	1.3	There is effective response when security breaches are detected.
Information relevant for the provision of services is reliable and available when needed.	2.1	There is effective information management for the provision of child safety services.
	2.2	Authorised personnel can efficiently access relevant information to provide child safety services.

Source: Queensland Audit Office

Reason for the audit

The nature of services to vulnerable children and young people calls for swift collaboration among government and non-government organisations. In addition, implementing recommendations from the recent Carmody report will result in an increase in the scope of work for NGOs and will likely lead to an increase in the number of NGOs involved in delivering child safety services. It is, therefore, timely to assess the management of child safety information practices in preparation for this change.

These organisations also need to keep the information secure and confidential as unauthorised access and disclosure—either accidental or deliberate could impact the safety of a child or young person.

Auditor-General Reports to Parliament

Reports tabled in 2014–15

Number	Title	Date tabled in Legislative Assembly
1.	Results of audit: Internal control systems 2013–14	11 July 2014
2.	Hospital infrastructure projects	October 2014
3.	Emergency department performance reporting	October 2014
4.	Results of audit: State public sector entities for 2013–14	November 2014
5.	Results of audit: Hospital and Health Service entities 2013–14	November 2014
6.	Results of audit: Public non-financial corporations	November 2014
7.	Results of audit: Queensland state government financial statements 2013–14	December 2014
8.	Traveltrain renewal: Sunlander 14	December 2014
9.	2018 Commonwealth Games progress	December 2014
10.	Bushfire prevention and preparedness	December 2014
11.	Maintenance of public schools	March 2015
12.	Oversight of recurrent grants to non-state schools	March 2015
13.	Procurement of youth boot camps	April 2015
14.	Follow up audit: Tourism industry growth and development	May 2015
15.	Results of audit: Education entities 2014	May 2015
16.	Results of audit: Local government entities 2013–14	May 2015
17.	Managing child safety information	May 2015