Access 4 Learning Community

Powered by: SIF

Simple. Secure. Scalable. Standard.

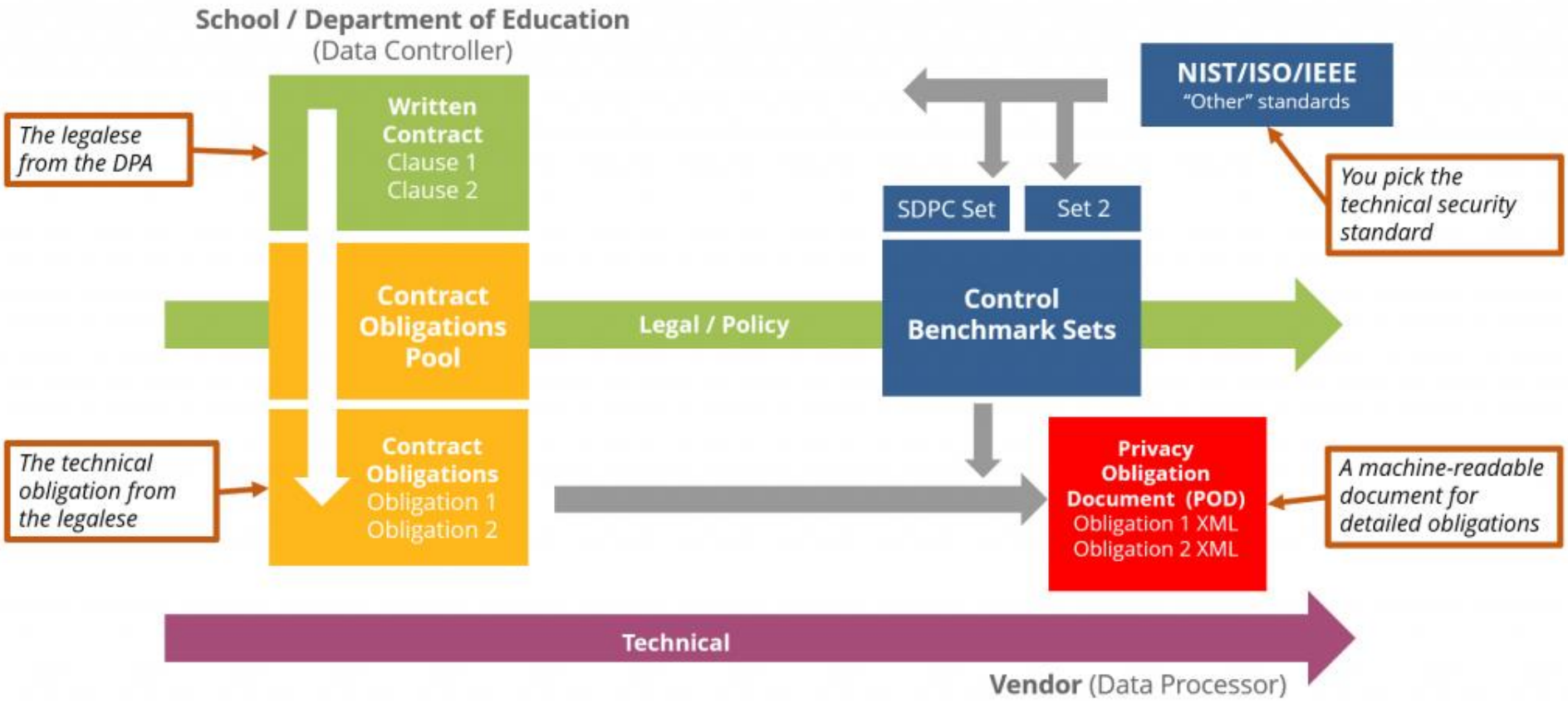
Student Data Privacy Consortium

December 2021 webinar

Access 4 Learning Community

Powered by: SIF

Simple. Secure. Scalable. Standard.



Safer Technologies 4 Schools

Safer Technologies 4 Schools (ST4S)

st4s.edu.au

Anthony Yaremenko, NSIP Program Manager

Access 4 Learning Community

Powered by: SIF

Simple. Secure. Scalable. Standard.

National Schools Interoperability Program NSIP

Acknowledgement of Country

I wish to acknowledge the Kulin Nation, Traditional Custodians of the land on which ESA's offices are located, and pay my respects to Elders past, present and emerging.

I also acknowledge the Traditional Owners of the lands across Australia, their Elders, Ancestors, cultures and heritage.

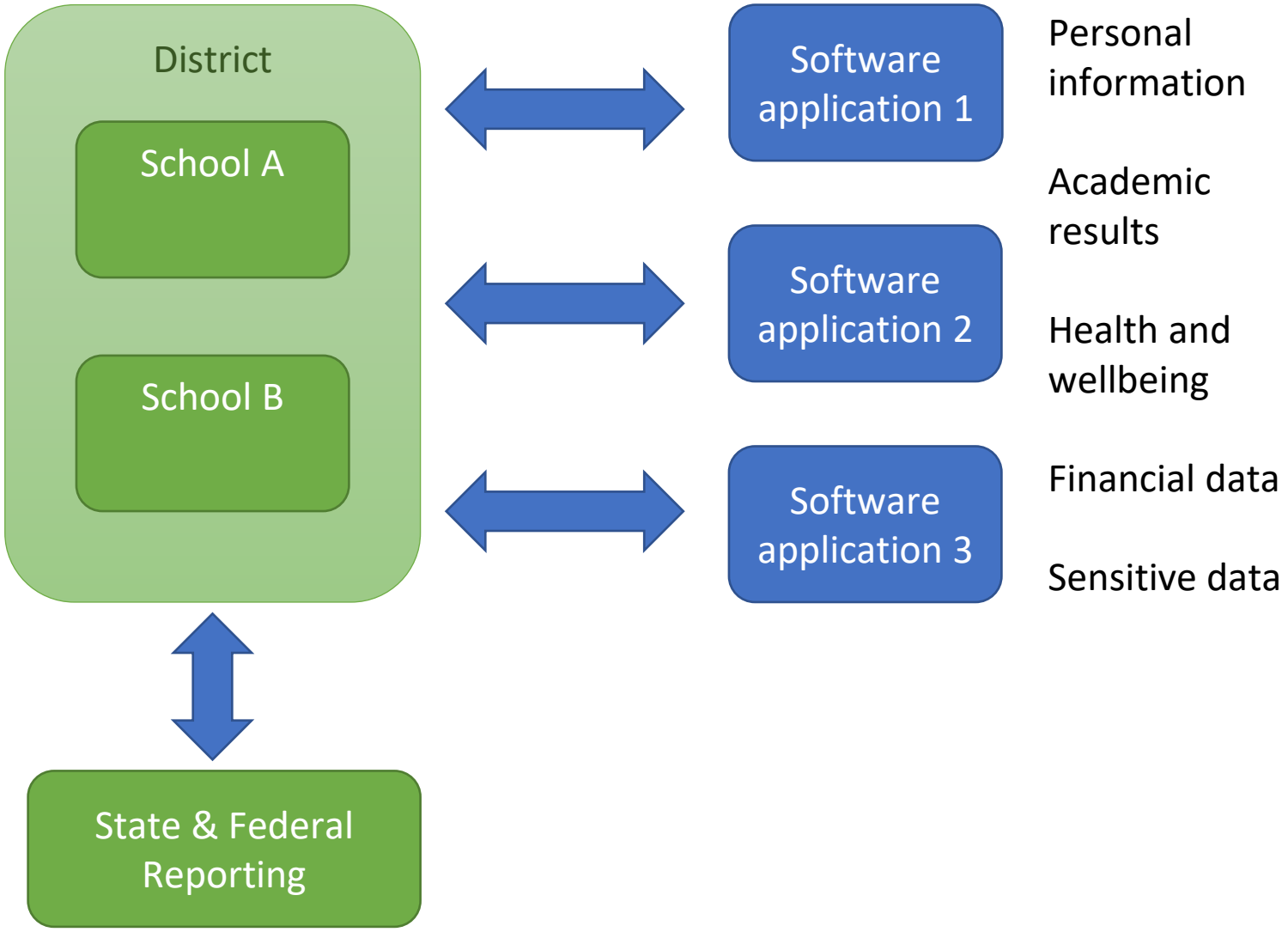
NSIP

- Safer Technologies for Schools (ST4S) is coordinated by the NSIP team at ESA
- NSIP long-term members of A4L / SDPC
- NSIP board: CIOs from all States and Territories, Catholic, Independents and Federal Government
- NSIP - business unit of Education Services Australia (www.esa.edu.au)
- ESA - national not-for-profit company owned by the state, territory and Australian Government education ministers
- ESA - established by education ministers in 2010 to advance key nationally agreed education initiatives, programs and projects

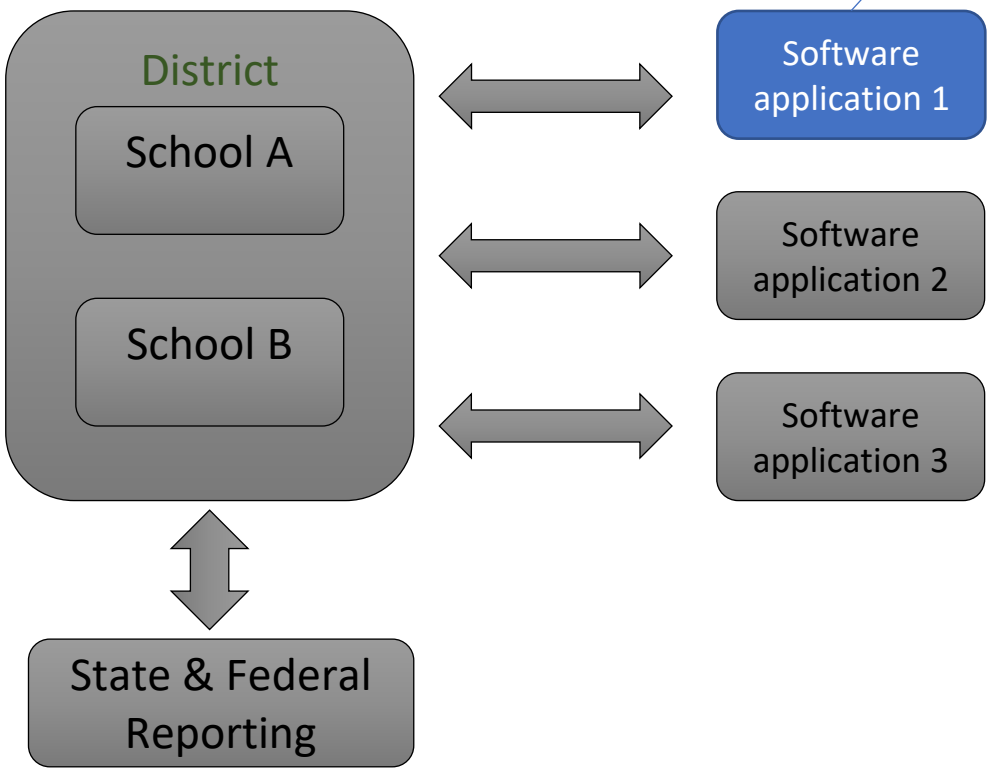

AUSTRALIA
MAJOR TOURIST DESTINATIONS
Arafura Sea
Coral Sea
INDIAN OCEAN
Kakadu National Park
Cape Tribulation
Great Barrier Reef
SOUTH PACIFIC OCEAN
NORTHERN TERRITORY
Magnetic Island
Whitsunday Islands
The Kimberleys
Glen Helen Gorge
QUEENSLAND
Uluru (Ayers Rock)
WESTERN AUSTRALIA
Fraser Island
SOUTH AUSTRALIA
Gold Coast
Kings Park
Swan Bells tower
Flinders Ranges
NEW SOUTH WALES
Opera house
Darling harbour
Sydney olympic park
Bondi Beach
Manly Beach
Perth
Barossa Valley
Blue Mountains
INDIAN OCEAN
Great Australian Bight
CANBERRA
Sydney
VICTORIA
Philip Island penguin parade
Mornington Peninsula
Melbourne
Great Ocean Road
Bass Strait
Tasman Sea
TASMANIA
0
500 Kilometers
0
250
500 International Miles
Copyright © 2011-12 www.mapsofworld.com

Over 4,000 different applications in use at schools

Education Supply Chain



Education Supply Chain



Can we trust Software application 1?

With what level of data?
Just email addresses?
What about health data?
What about financial data?
Who is liable / responsible if/when things go wrong?

Education Supply Chain

People also ask

Which is an example of a supply chain attack?

A supply chain attack is a cyber-attack that seeks to damage an organization by targeting less-secure elements in the supply chain. ... **The Target security breach, Eastern European ATM malware, as well as the Stuxnet computer worm** are examples of supply chain attacks.

https://en.wikipedia.org › wiki › Supply_chain_attack

Supply chain attack - Wikipedia

Verizon 2021 Breach Report

https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf

- "**Ransomware is really taking hold of Education vertical incidents**, and has been responsible for 80% of the Malware-related incidents, up from 48% last year"

- "…Educational Services have the longest number of days in a year—28—where they had credential dumps run against them. The global median here is eight days. The overall number of credentials attempted is also **one of the highest of all industries we analyzed** for this year's report…"

Ransomware payments

- https://www.nbcnews.com/tech/security/parents-end-chain-ransomware-hit-rcna646
- https://www.cbsnews.com/news/schools-popular-ransomware-targets/
- https://abcnews.go.com/US/wireStory/large-florida-school-district-hit-ransomware-attack-76818911

Search jobs | Sign in | Search

The Guardian
For 200 years

Australian edition

Hackers target NSW school online accounts in phishing campaign

Scam email tries to exploit Microsoft platform used by schools in bid coinciding with prime minister's warning of wider cyber-attack

Catholic school in Australia falls victim to Cyber Attack

December 20, 2019 By iZOOlogic In Financial Malware, Phishing, Compromised Data

Private school's lessons crashed by Zoom 'bongers'

Two teens managed to access the Zoom

news.com.au

National | World | Lifestyle | Travel | Entertainment | Technology | Finance | Sport

technology online > hacking

Hacker group threatens Newcomb Secondary College in Victoria

A high school has been hit by a cyber attack, with the criminals threatening to release information if the school doesn't 'co-operate' within a week.

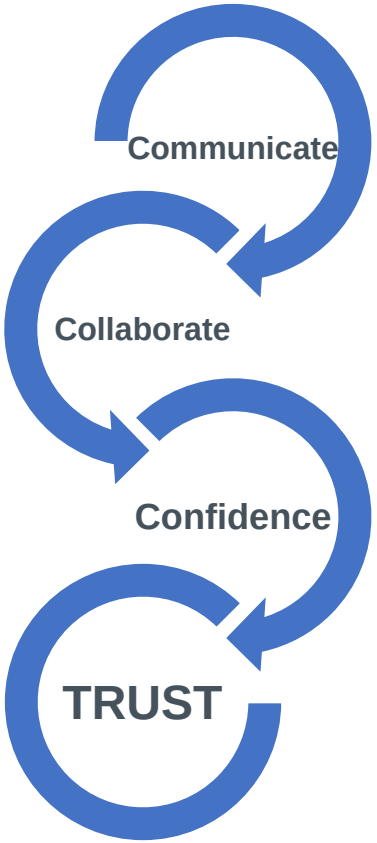
Anton Nilsson NCA NewsWire APRIL 28, 2021 5:41PM

What is ST4S?

An Australian framework for online education services to assess:

- Security
- Privacy
- Online Safety
- Interoperability

Provides a nationally consistent baseline for assessments across Australia



Key Outcomes for Vendors & Sector

- To increase awareness and raise the profile of security & privacy controls
- Clear guidance on what is expected of vendors and for classrooms regarding safer usage
- National baseline requirements that allow vendors to self-assess
- Feedback and support to vendors on areas requiring improvement
- Reduced administrative burden for vendors & education sector

- All contributing to **improved student and school safety**

Concepts

- **Working Group:** Security and privacy experts from across the country. Meet monthly. Suggest framework updates.
- **Assessment framework:** Set of control questions with response options.

  *Eg What are the minimum encryption algorithms applied to protect all data **in transit** over networks, including encryption of data that is communicated between the user, web applications and system components (e.g. database systems)?*
- **Assessment tiers:** Not all products are equal. Data & functionality require higher/lower levels of controls. Tier 1/2/3. eg encrypting basic class details vs encrypting mental health records or financial information
- **Non-compliant responses:** Important controls are required to be met and if not generate a ‘non-compliant’ (fail) result

Assessment Framework

Security

- Where is the live solution hosted?
- Is multifactor authentication used?
- How often are audit logs reviewed?

Privacy

- How can users request a copy of their data?
- Does the privacy policy comply with the Federal privacy laws?
- Are photos and contact details associated with a user?

Functionality & Education controls (10 +/- 20)

- What functionality is available (surveys, online meetings, remote access, screen share, chat, forums, commenting, file download/upload)
- In relation to <x> functionality, tell us about your controls (eg chat logs etc)

Interoperability

- What APIs are available to exchange data?
- What standards (incl. SIF, IMS) are supported?

All available in the ST4S Vendor Guide on www.st4s.edu.au

How does it work?

1. Vendors answer a set of control questions and are asked to upload evidence to support their response (eg privacy policy, security policy, incident response plan, etc)

2. Assessment team work with vendor to resolve any queries. Assessment team develop an understanding of the product, vendor develops an understanding of the assessment

3. Draft report is developed and iterated

4. Final report is signed-off and distributed to our CIOs and ST4S Working Group

Safer Technologies for Schools Assessment

Prepared by NSIP, a business unit of Education Services Australia for the Safer Technologies for Schools Working Group
For limited distribution only (jurisdiction chief technology officers, relevant schools and the service provider whose service is the subject of this report).

Sample product/service (Sample vendor)

Assessment outcome: Medium risk

The overall risk level is the highest risk level remaining after all available treatments have been applied.

Service summary

Version:	Paid – Latest	**Review date:**	18/05/2020
Tags:	Library management; Administrative support services; Booking systems.	**Assessment Tier:**	Tier 2
URL:	http://www.sampleproduct.com.au	**Audience:**	Staff and Students

Purpose of use: Sample product is a library management system. Modules include cataloguing, circulation, search, overdue notices, borrowers, reports and stocktake.

Information assets and hosting

Data hosting:

Service components (live solution, backup):	Onshore (in Australia)
Service provider staff location (support staff):	Onshore (in Australia)
Account holder data:	Onshore (in Australia)

Data classification:
- ☒ Non-personally identifiable information
- ☒ Personally identifiable information
- ☐ Sensitive information

Legal jurisdiction: Victoria, Australia

Parent/carer consent: Parent/carer consent is required as:
- ☐ Student personal information is disclosed to register an account
- ☒ Student personal information is collected, used or disclosed through use of the service
- ☒ Student images, video, work and/or results are uploaded and published to the service

Actionable risks and risk treatments

After conducting a comprehensive review, the following risks and associated treatments have been identified. The risk treatments listed are designed to reduce risk exposure. Users must adhere to all stated risk treatments when using this service. The risk level is that which remains after the listed treatments have been applied.

#	**Account management** *Account management standards assess theTerms of Service for the service provider and user, including the data disclosed during account registration, consent requirements, and the policies and processes that apply to account termination, administrator control of accounts and generation of user profiles.*		
	Risk	**Risk treatment**	**Risk level**
PR3 PR5	Account registration is required, and the following information must be disclosed: ○ **First name (staff)** ○ **Surname (staff)** ○ **Email address (staff)** ○ **Country and/or state/province (staff)**	• Complete only mandatory fields. • Use anonymous and/or organisational details to replace personal information wherever possible. • Do not use organisational passwords. • Gain consent as per the Parent/carer consent section of this report. • This service does not require users to enter complete and accurate information when registering accounts. Users should create accounts using anonymous and/or organisational details wherever possible.	**Low**
PR8	When registering accounts for this service, mandatory data fields are not identified to the user. This may result in users providing more information than is necessary through optional fields. Over-collection of information increases risks for the security of personal information which may be vulnerable to data loss or identity theft if a data security breach occurs.	• When registering accounts, ensure users only enter the information specified in the **Account Management** section of this report.	**Medium**
#	**Usage conditions** *Usage conditions vary based on the functionality available within the service. These conditions aim to reduce the risks associated with student safety, reputational damage, loss of intellectual property rights, and unauthorised or over-disclosure of personal, sensitive or organisational information.*		
	Risk	**Risk treatment**	**Risk level**

Journey so far… 2019-2021

Queensland Government

VICTORIA State Government

NSW GOVERNMENT

Department of Education
GOVERNMENT OF WESTERN AUSTRALIA

INDEPENDENT SCHOOLS AUSTRALIA

NORTHERN TERRITORY GOVERNMENT

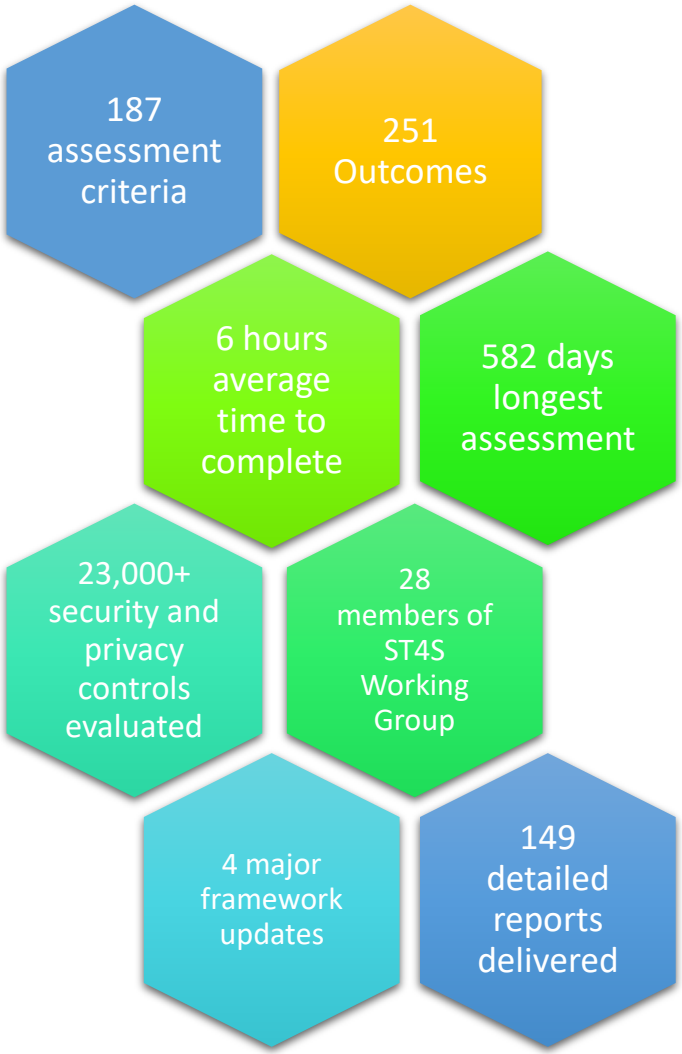
Government of South Australia
Department for Education

Tasmanian Government

ACT Government
Education

NATIONAL CATHOLIC EDUCATION COMMISSION

Statistics


187 assessment criteria
251 Outcomes
6 hours average time to complete
582 days longest assessment
23,000+ security and privacy controls evaluated
28 members of ST4S Working Group
4 major framework updates
149 detailed reports delivered

Wide Range of Vendors

Findings

Encryption on the wire - TLS/SSL (S1, S3)

- TLS version & SSL Cipher Suites
- BaaS – Google Firebase, AWS Amplify, move to ‘serverless’
- Cipher suites configured on the server
- As SSL/TLS is configured ‘server side’ BaaS basically hides away server settings
- Challenging for vendors to adjust SSL ciphers and sometimes the TLS versions
- Looking at working with security teams and possible revisions to assessment criteria (ie set of known and supported BaaS’s)

Data Segregation – S4

- Evolving space: physical tin, logical segregation, cloud
- Focus more on vendor APIs and communication with database
- Are well developed frameworks in use (Nest.JS, Laravel, LoopBack etc) or using serverless eg AWS API Gateway, Authy etc.
- Expect this space to develop

Findings

Increase in Artificial Intelligence and Insights

- Increase in apps offering data insights/analytics (Billy didn't do so well in maths and is below the 5% of his cohort)
- Data handling and data ethics
- Consider https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-ethics-framework/australias-ai-ethics-principles

Increase in Health and Wellbeing Apps/Services

- Increase in health and wellbeing type apps coming through (especially with covid).
- 'Duty of care' issues emerging eg if a student is repeatedly hitting the 'sad face' and not the 'happy face' for 3 months on a health check-in mobile app, does that establish an actionable concern? What should the school do? What should the product do in terms of alerts etc?

Learnings

Non-participating vendors

- Vendors who were invited to participate but did not respond
- Vendors who did not want to participate
- Developed non-participating reports
- Created trouble ☹

Large vendor companies

- Separate sales, security, privacy, legal, sales/marketing silos
- Teams distributed across the globe
- Applications that require underlying platform
- Responses shift based on last area to review
- Process may halt at 99% completion
- Complex +++

Small-Medium vendor companies

- Keen to please
- Time & resource sensitive
- May over-commit

Readiness Check Launched

www.st4s.edu.au/readiness-check

- Now the first step for all vendors
- Critical subset of full assessment criteria (~40 criteria)
- Provides instant feedback to vendor
- Vendors can complete over multiple sessions and take multiple attempts
- Submit when ready
- Working Group then prioritise for full assessment

Safer Technologies 4 Schools

Readiness Check

ST4S Readiness Check Results

Ready Status: **Not Ready for ST4S Assessment**
Tier: Tier 1

Detailed Results:

Item	Question	Response	Minimum Required	Status
S1	What are the minimum encryption algorithms applied to protect all data in transit over networks, including encryption of data that is communicated between the user, web applications and system components (e.g. database systems)?	Encryption: DES, RC4; Hashing: Message Digest (MD to MD6), RIPEMD-128 or above, SHA-0, SHA-1; Digital Signatures: DSA (1024) or RSA (1024); Key Exchange: DH (1024) or RSA (1024); Protocol: TLS1.1 or below	The response provided does not meet the minimum requirements. The minimum requirement for a Ready outcome is: 'Encryption: AES 128 or above only (AES 256 recommended); Hashing: SHA-256 or above only (SHA-384 recommended); Digital Signatures: DSA (2048+) ECDSA (256) or RSA (2048+); Key Exchange: DH (3072+), ECDH (P-256) and/or RSA (2048+); Protocol: TLS1.2 or above only (TLS 1.3 recommended). (T1)'	Not Ready
S3	If customer data is uploaded to the service using a mechanism such as encrypted USB, SFTP, Secure API, etc., what are the minimum encryption methodologies applied?	Encryption: AES 128 GCM/CCM, CHACHA20 POLY 1305 or above only (AES 256 GCM/CCM recommended); Hashing: SHA-256 or above only (SHA-384 recommended); Digital Signatures: DSA (2048+) ECDSA (256) or RSA (2048+); Key Exchange: DH (2048+), ECDH (P-256) and/or RSA (2048); Protocol: TLS 1.2 or above only (TLS 1.3 recommended) (T1)		Ready

But……

… we would all benefit from an international approach…

Apache Log4j2 library vulnerability (CVE-2021-44228) and Conti ransomware incidents

NCSA- 3 ALERT: A cyber threat that requires immediate monitoring, analysis and strategic coordination….

ST4S Controls:

T1 - Does your organisation have an implemented continuous monitoring plan …
T2 - Does your organisation use a centrally managed approach to patch or update applications…
T3 - Are security vulnerabilities in operating systems, applications, drivers and hardware devices assessed as extreme risk patched or mitigated within 48 hours of being identified?
T7 - When a data breach occurs, are affected customers and/or organisations notified as soon as possible after a data breach is discovered and given all relevant details?

ST4S – Standards

S1: What are the minimum encryption algorithms applied to protect all data in transit over networks, including encryption of data that is communicated between the user, web applications and system components (e.g. database systems)?

ST4S Control	AU ISM	NIST 800-53 rev4	ISO 27002
S1	1139	SC-8 Protect the confidentiality /integrity of transmitted information.	10.1.1 13.2.3 14.1.2 14.1.3

NIST Cybersecurity Framework

NIST Cybersecurity Framework

- Flexible framework that can be applied to any organization
- References NIST 800-53, COBIT, ISO 27001:2013
  - https://www.nist.gov/cyberframework

NIST Cybersecurity Framework

5 keys functions

- Identify
- Protect
- Detect
- Respond
- Recover

NIST Cybersecurity Framework

- Identify critical enterprise processes and assets
- Document information flows
- Maintain software and hardware inventory
- Establish cyber policies including roles and responsibilities
- Identify threats, vulnerabilities, and risks to assets

What should an education CSF look like?

- Work needed to determine scope of controls suitable for education context
- What is in scope?
- What is out of scope?
- Are there additional considerations?
  - Adults & children
  - Consent
  - Functionality: Information exposure Functionality: Communication
  - What is reasonable for education vendors?

CSF: Identify – Asset Management

ID.AM-1: Physical devices and systems within the organization are inventoried

Q6. Does the vendor have a documented and implemented IT Asset management process including:

- An ICT equipment and media register that is maintained and regularly audited;
- A directive that ICT equipment and media are secured when not in use;
- The secure disposal of ICT equipment and media (including sanitising/removal of any data or secure destruction/shredding)?

A Way Forward:

1. Agree we have a shared problem worth solving
2. Establish an international Project Team (A4L SDPC)
3. Identify a suitable, recognised control set
4. Work through the control set (relevancy, develop control questions and responses)
5. Develop a standardised assessment approach
6. Develop standardised assessment reporting
7. Develop a results sharing process
8. Maintain the framework

Thank You & Questions

Access 4 Learning Community

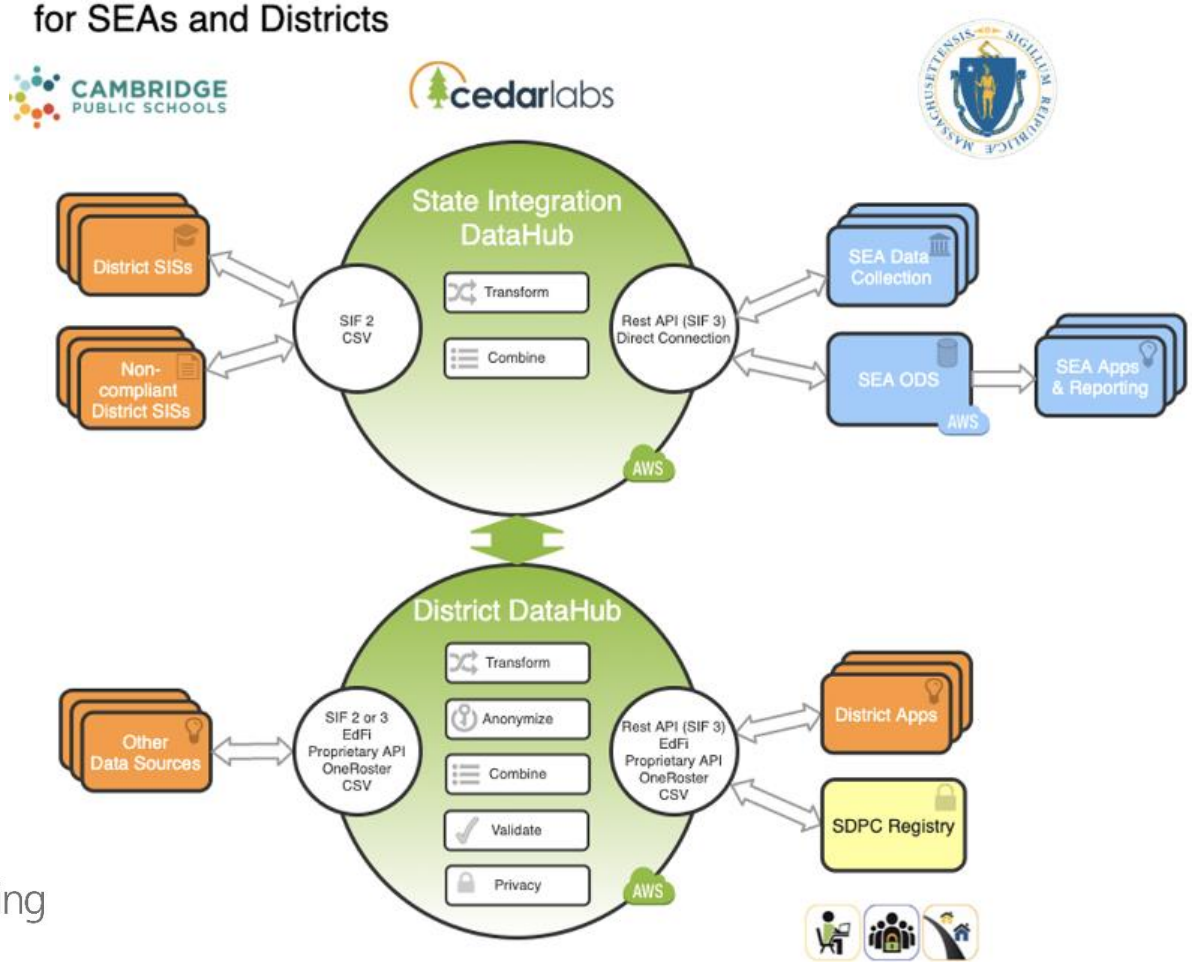
Powered by: SIF

Simple. Secure. Scalable. Standard.

National Schools Interoperability Program NSIP

DataHubs

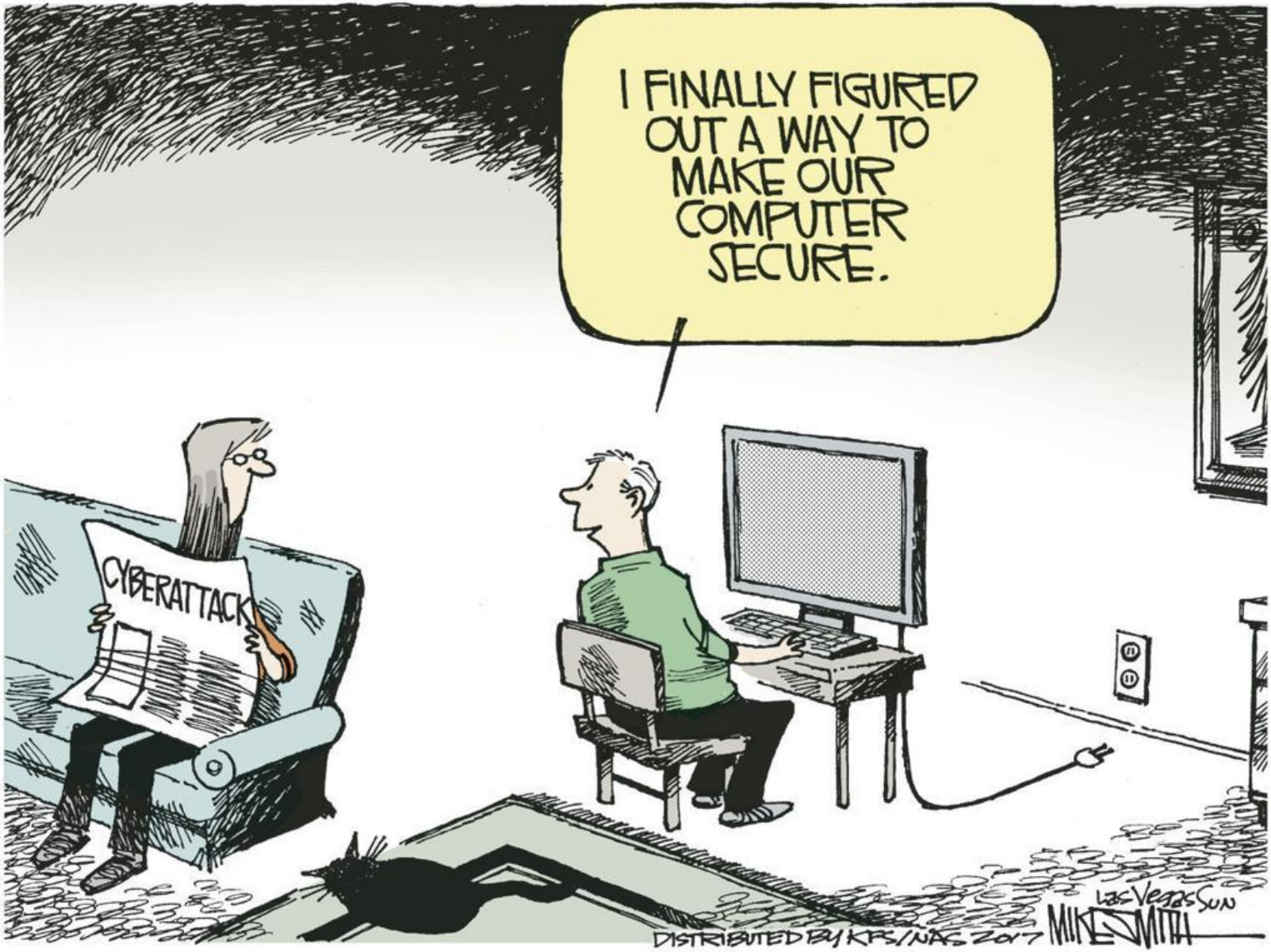
The MA DataHub:
Real-time statewide data integration and privacy management for SEAs and Districts



Access 4 Learning Community

Powered by: SIF

Simple. Secure. Scalable. Standard.


I FINALLY FIGURED OUT A WAY TO MAKE OUR COMPUTER SECURE.
CYBERATTACK
DISTRIBUTED BY KFS/NAS 2017
LAS VEGAS SUN
MIKE SMITH