Greenville County Schools

Education Technology Services

"Interfacing the mind with the technology of the future!"

Inspired | Supported | Prepared

2022 | Our Journey to ISO 27001:2013 | Noel Adams

Education Technology Services

LinkedIn
https://linkedin.com/in/noeladams

Professional Biography

Noel Adams is the Cyber Security (guy) of Education Technology Services at Greenville County Schools and has served with the district for 20 years. Greenville County Schools is the 44th largest district in the nation with over 76,951 students and 10,095 employees and is the largest school district in South Carolina

Mr. Adams holds the following certifications:

- CyberSec First Responder
- Certified Vulnerability Assessor
- GIAC GCFE (Computer Forensics)
- Cisco CCNA Cyber Ops
- CICP (Core Impact Certified Professional)
- MCITP, MCSE, A+
- AccessData Certified Investigator
- Plus a lot more but there's only so much room.

Mr. Adams also volunteers his time:

- Warrant Officer in the South Carolina State Guard - G2 Cyber Security & Intel
- Google CIO Client Advisory Board for K12
- Defcon 864 Board Member
- FBI Infragard National Cyber Camp Board Member
- US Air Force Association Cyberpatriot program Technical Advisor
- SLED Cyber Liaison Officer
  - SC Critical Infrastructure Cybersecurity (SC CIC) Program

CYBER·SC

February 16th 2023 | Columbia, SC, USA

Education Technology Services

Our Mission

The mission of Education Technology Services (ETS) is to create, support, assess, and maintain an optimal technology environment for student education and administrative support in the School District of Greenville County.

February 16th 2023 | Columbia, SC, USA

CYBER·SC

Agenda

Some background about GCS

- District background
- Information Security Responsibilities
- Why ISO 27001 Certification?
- What did we do to achieve ISO?
- The next steps
- What can you take away from this?

CYBER·SC

Greenville County Schools: Devices

13,948
iPad Tablets

113,650
Chromebooks

38,384
Laptops/Desktops

4,200
Radios

7,890
Printers

28,510
Other Technology
(Servers, Faxes, Switching, Routers, Phones, Wi-Fi)

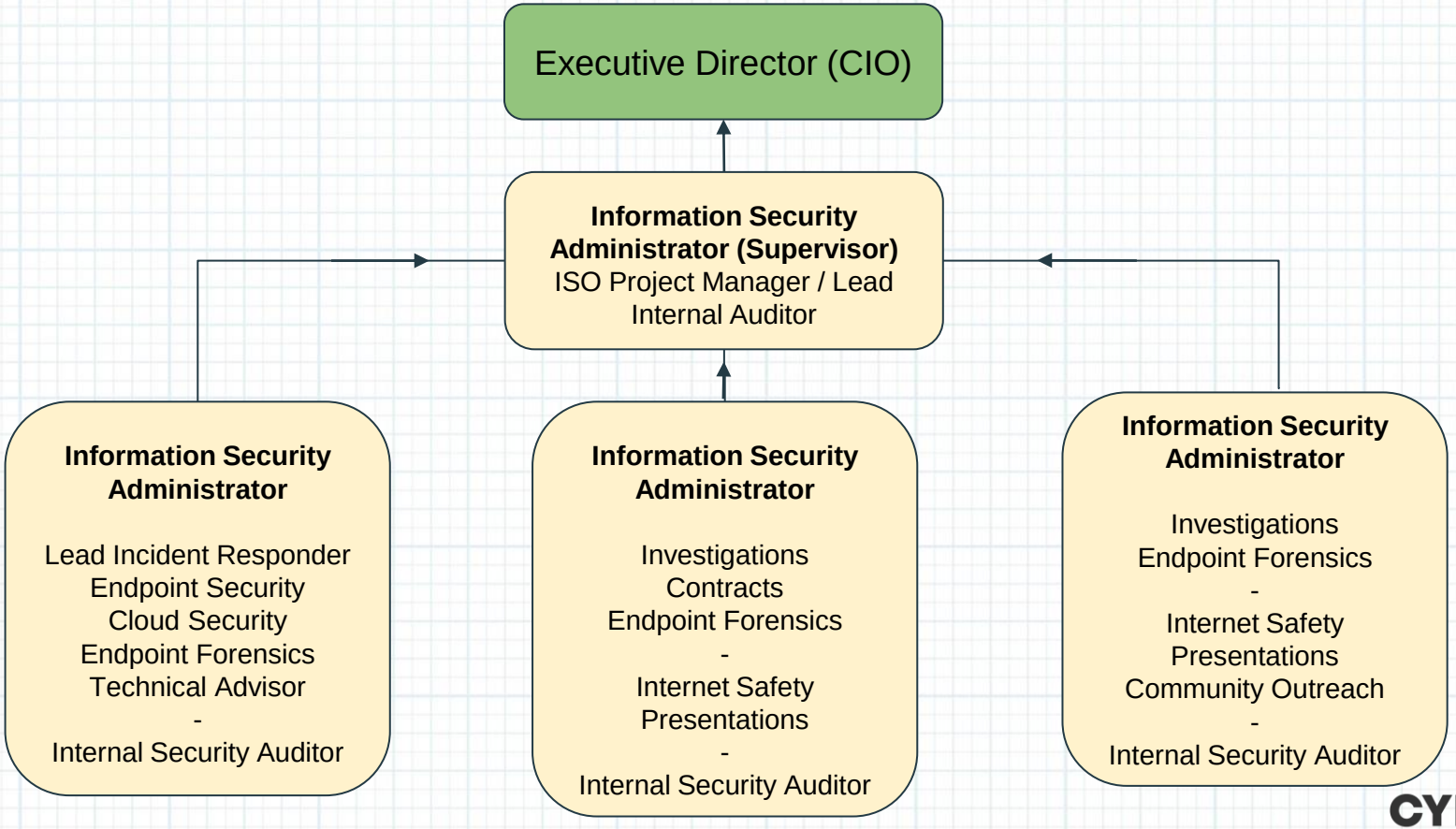
CYBER·SC

February 16th 2023 | Columbia, SC, USA

It’s not often you have a security administrator who has 80% of his user base actively trying to circumvent security restrictions. It was a challenge every day.

~Noel Adams

ETS: Information Security Staff



Information Security (The Job)

What we do:

- *Serve as expert advisors to senior management*
- *Incident Response*
- *Endpoint / Network Forensic*
- *Internal / External Penetration Testing*
- *Web Application Security Testing*
- *New Technology Evaluations for Security Compliance*
- *Disaster Recovery Planning*
- *District Security Standards and Procedures Creation*
- *Risk Assessments*
- *Internal Auditors (Security)*
- *Breach Investigations*
- *Data Sharing Agreements to Control 3rd Party Access*
- *And Much Much More….*

CYBER·SC

Incidents

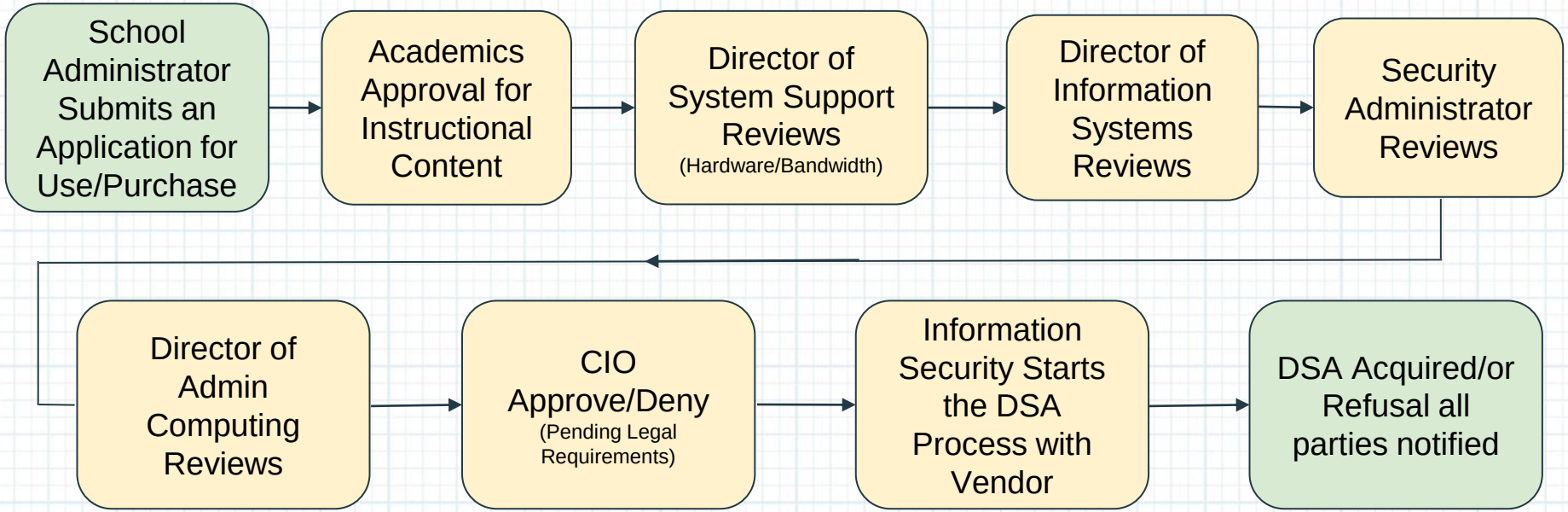
Computer security incident response has become an important component of information technology (IT) programs. Security-related threats have become not only more numerous and diverse but also more damaging and disruptive.

–NIST Special Publication 800-61, U.S. Dept. of Commerce

Data Security (Application(s) Approval)

Our department worked with legal council to create a policy and procedure that any vendor that needs to access student PII must adhere to. All data share agreements (DSA) are limited to only what is needed and have a term-limited by default. By creating this process we comply with COPPA, FERPA, CIPA. and ISO 27001.

Data Security (Application Approval Cont)



Access Management System

Information Security worked with our in-house development department to automatically provision users with least privilege. Then we looked are 3rd parties for an access management system but in the end they didn't do what we needed so we created our own.

AMS is utilized with 3rd party contractors, teachers, etc so that they can be granted least privilege access after the access forms are completed and approved. AMS by default expires all contractors after a set time. Access can be granted/extended via a supervisor and all actions are logged.

Access Management System (Cont)

AMS was designed for the principal, supervisor to control access to their locations:

- *Data*
- *All staff distribution*
- *Network devices like printers*
- *Software permissions*
- **Allows for the creation of accounts for Contractors and Student Teachers*
    - *Always require secondary approval by student information assurance and information security or HR.*

Vulnerability Assessments

Information Security performs internal and external penetration/vulnerability testing of district assets utilizing open source and industry standard tools.

CYBER·SC

Continued….

Some information security assessments have been:

- *Physical Access Controls Systems*
- *Surveillance Systems*
- *HVAC Systems*
- *Fuel Systems*
- *New Hardware Assessments*
- *Web Application Testing*
- *Network Systems (everything)*
- *& much more….*

Always remember to check your 3rd parties when they install equipment.

Web Application Testing

Information security works closely with the director of information systems to test any in-house created applications for security vulnerabilities and recommend remediation methods

We have in the past also performed this testing on some 3rd parties upon notification in writing.

We normally utilize professional (paid) toolsets to perform testing but also trained in Open Source tools like Burp, Nikto, OWASP Zap

Forensics

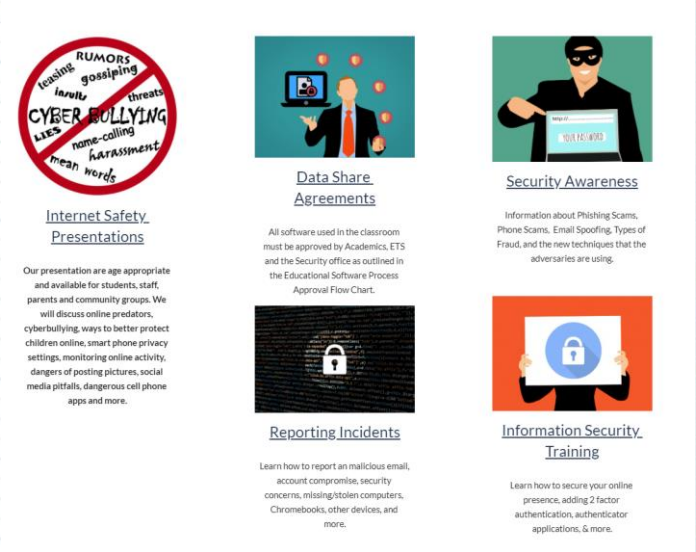
All Security Administrators trained in computer forensic either from being former law enforcement or specialized training. We currently have staff who hold industry certifications for computer forensic.

We are the only school district in the state which has in-house forensic analysts.

Security Awareness Training

- *Created an easy to following security awareness training portal.*
- *Yearly review of security awareness training*
- *Starting a Security Awareness Training program has helped reduce phishing by 35% within the first year.*

There are plenty of free resources you can use to help in building a successful program.



CYBER·SC

Internet Safety

One of our Security Administrators (Rick Floyd) goes out to schools to present to students/parents how to stay safe online. He keeps up to date on all the latest apps the kids are using, and these presentations are for grades 3 - 12. He has presented to church groups, community events and has been on the local and national news.

https://sites.google.com/a/greenvilleschools.us/rlfloyd

Internet Safety Presentations

Our presentation are age appropriate and available for students, staff, parents and community groups. We will discuss online predators, cyberbullying, ways to better protect children online, smart phone privacy settings, monitoring online activity, dangers of posting pictures, social media pitfalls, dangerous cell phone apps and more.

CYBER·SC

What is ISO 27001

ISO/IEC 27001 is widely known, providing requirements for an information security management system (ISMS), though there are more than a dozen standards in the ISO/IEC 27000 family. Using them enables organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.

Now Why Go After an ISO 27001 Certification?

In 2016 , The State of South Carolina introduced Proviso 93.25 and creates a mandate for ISO 27001 or NIST 800 Certification

~Proviso 93.25 of the 2016–2017 South Carolina Appropriations Act and any successive statutes, these standards are to be implemented by State agencies, including institutions, departments, divisions, boards, commissions and authorities.

CYBER·SC

ISO 27001 Training

Lead Auditor Trained and Certified 27001 Auditor
Security Administrators then were trained in all areas of the ISMS (Information Security Management System) standard for ISO 27001:2013

Training consisted of:

- *Basics and details of auditing*
- *Key principles of ISMS and Auditing of ISMS*
- *Evaluate the Implementation and effectiveness of ISMS*
- *Evaluate compliance against the requirements*
- *Assess performance against objects and key performance indicators*
- *Identify areas of potential improvement and ensure continual improvement.*
- *Collecting data, objective evidence and then generate findings (Major, Minor, and opportunity for improvement)*

CYBER·SC

Audited Areas

- **The Statement of Applicability:** The Statement of Applicability (SoA) forms a fundamental part of your information security management system (ISMS). The SoA is one of the most important documents you'll need to develop for ISO 27001:2013 certification.
- **Management Review Process**:This system gives senior staff the opportunity to evaluate the effectiveness of their organization's ISMS and make any changes that could boost its ability to protect sensitive information. Audit review covers effectiveness of management meetings and scrutinization of minutes generated during Management Review Committee.
- **Continual Improvement**: Audits the system of continual improvement implemented by Greenville County Schools' ISMS. Organizations that take improvement seriously will be assessing, testing, reviewing and measuring the performance of the ISMS as part of the broader business led strategy, going beyond a 'tick box' regime. This is certainly the case with Greenville County Schools' ISMS.

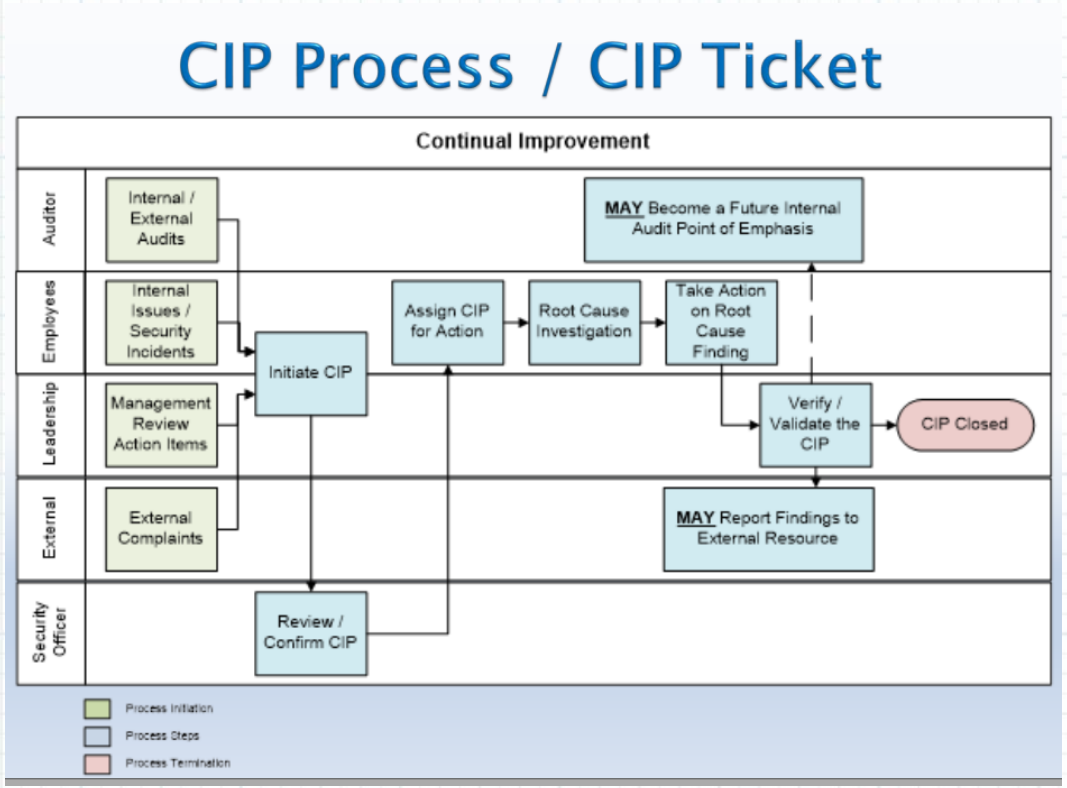
CYBER•SC

Areas Audited (Cont)

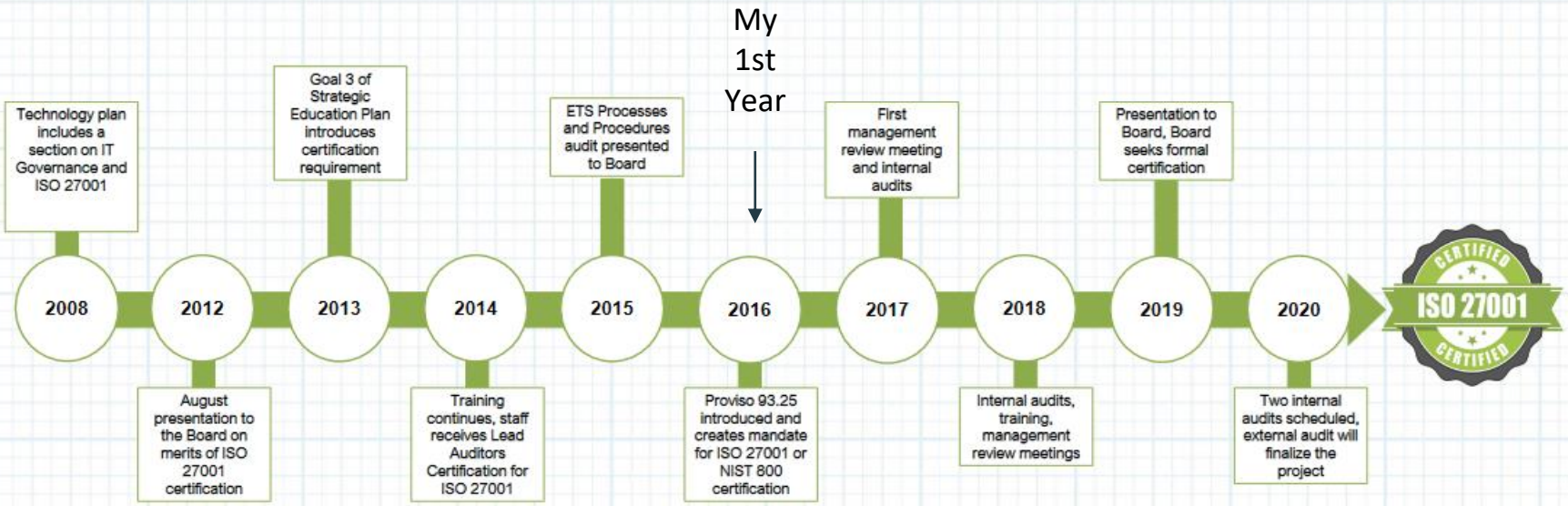
- **Internal Auditing Program**: The Internal Audit program is reviewed to insure qualified personnel are conducting audits in line with the ISO 27001 standard. Stage 1 Review also focuses on the effectiveness of those internal audits.
- **Risk Management Program:** Information security risk management (ISRM) is the process of identifying, evaluating, and treating risks around the Greenville County Schools' valuable information. It addresses uncertainties around those assets to ensure the desired business outcomes are achieved.
- **ISMS Scope and Policy**: ISO 27001 standard involves setting the scope of your Information Security Management System. This is a crucial part of the ISMS as it will tell stakeholders, including senior management, customers, auditors and staff, what areas of your business are covered by your ISMS. During audit, we should able to quickly and simply describe or show our scope to an auditor and describe your key interested parties.
- **Document Control:** The purpose of this procedure is to ensure control over creation, approval, distribution, usage and updates of documents and records used in the Information Security Management System (ISMS).

ISO 27001 Training (Continual Improvement Process) CIP

Example of a CIP Process:



ISO 27001 Certification Timeline



Timeline of the ISO 27001

2012 - August Presentation to the Board on merits of ISO 27001 Certification
2013 - Goal 3 of the Strategic Education Plan introduces certification requirement
2014 - Training continues, staff receives Lead Auditor Certifications for ISO 27001
2015 - ETS Processes and Procedures audit presented to the Board
2016 - SC State Introduced Proviso 93.25
2017 - First Management Review meeting and Internal Audits
2018 - Internal Audits, Training, Management review meetings
2019 - Presentation to Board, Board seeks formal certification
2020 - Internal audits completed, passed external audit. (ISO 27001:2013 obtained)
2021 - External surveillance audit complete.
2022 - External surveillance audit complete.
2023 - Recertification audit scheduled for this summer.

CYBER·SC

Regulatory Requirements

COPPA
Children's Online Privacy Protection Act

DEPARTMENT OF EDUCATION · UNITED STATES OF AMERICA
FERPA 2012 compliant
Student Education Records 2012 new record keeping requirements

- Relieve pressure of regulatory and certifying agencies individual requirements
- ISO 27001 reduces the time and resources required for a third-party audits
- Establish change control and save valuable resources by reducing complexity in operations district wide

FEDERAL COMMUNICATIONS COMMISSION · FCC · USA
CIPA 2012
Student Internet Protection

HIPAA

CYBER·SC

Certification Progress

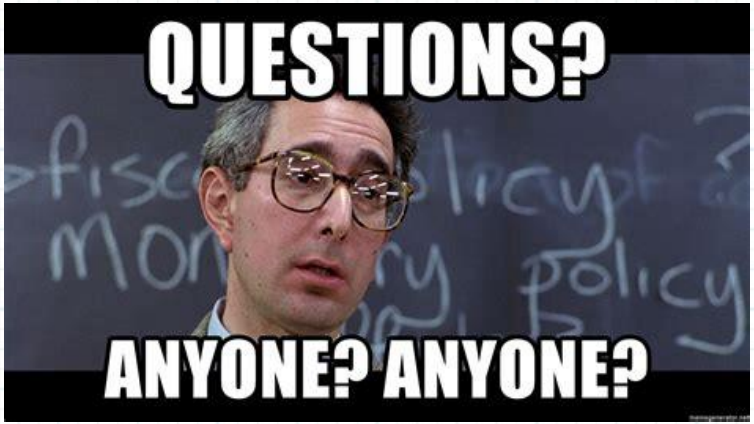
- A lot of work had to be completed, including:
- High-level policy
  - Incident response plan
  - Information Security in contracts and procurement
- Software / Data Approval Policies
- Information Security Policies
- Disaster recovery plan
- Content Management System
- Access Management System

Lessons Learned

- *Consider implementing an Information Security Management System, pick a standard with top-down management support*
- *Encrypt everything; laptops, flash drives, portable storage, cell phones, mobile devices, tablets, data-in-transit, etc.*
- *Change passwords frequently and use complex passwords.*
- *USE MFA!!!!! (Implemented 2022)*
- *Hire a technical writer*
- *Awareness, Awareness, Awareness!!!*

Next Steps…

- *International Standards Organization (ISO) publishes the new ISO 27001:2022 standard in October 2022*
- *While allowed to recertify in ISO 27001:2013 we are moving forward and will be certifying in ISO 27001:2022.*
- *Internal Audits are in progress*
- *External audit scheduled for summer.*



Contact info:
Email: nadams@greenville.k12.sc.us
Linkedin: linkedin.com/in/noeladams