ATS Adventist Technology Summit

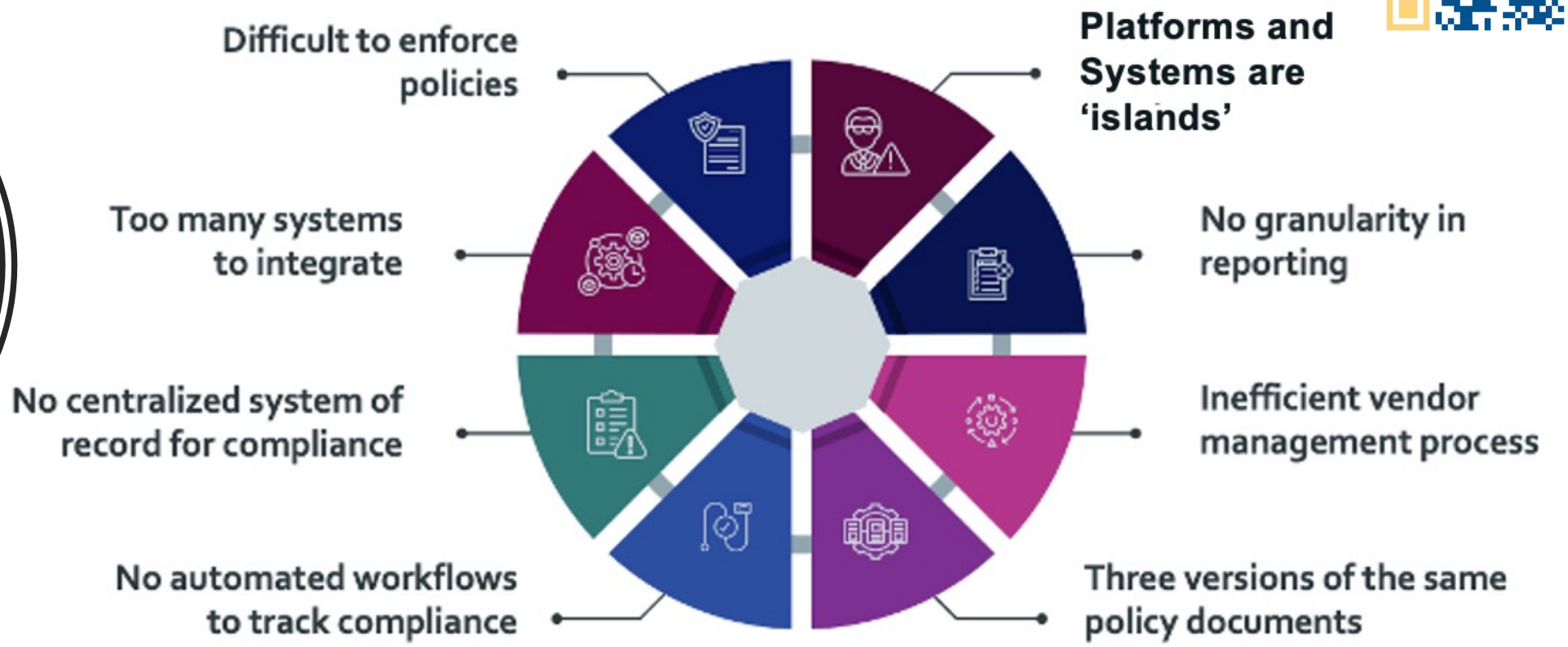
Data Security

Compliance, Policies, and Standards

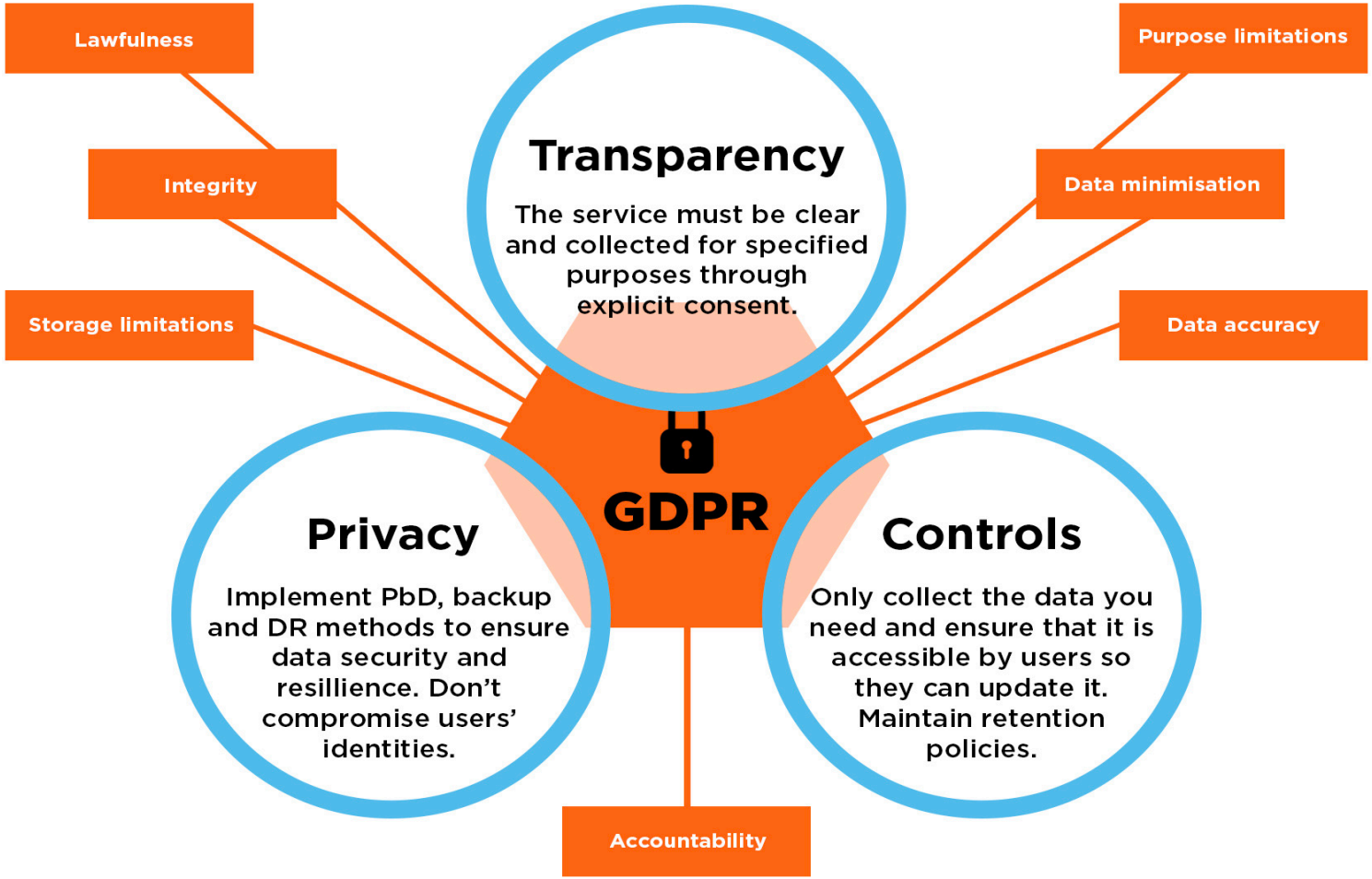
https://t.ly/ATS-2023

Compliance Challenges

Faith-based charities are increasingly regulated.



Compliance Requirements

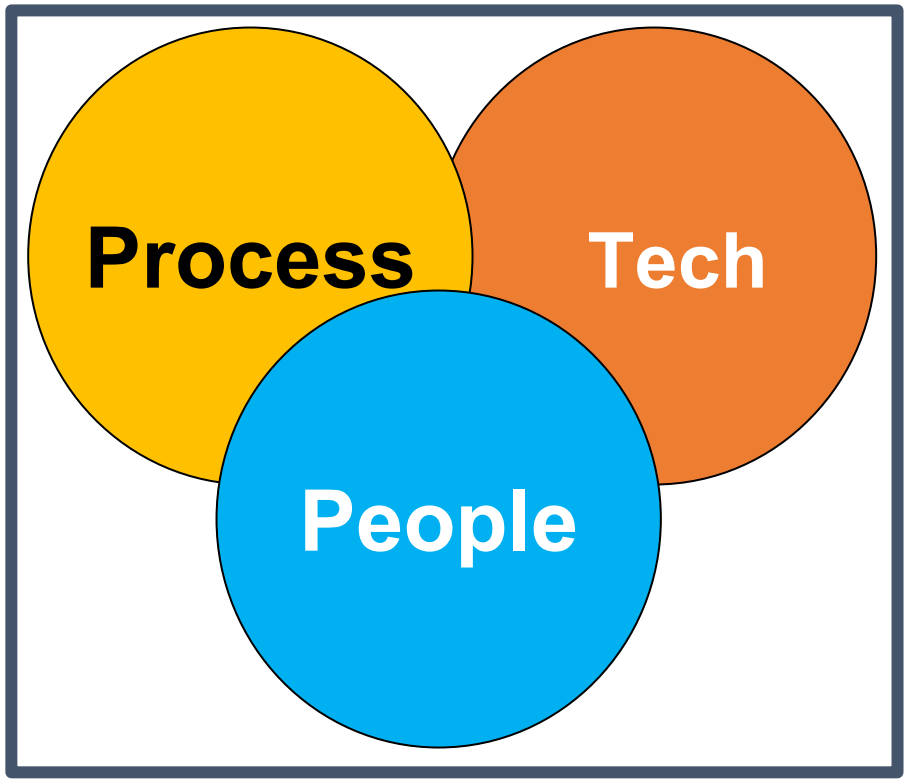


Holistic Data Protection:

Policies set the framework to align People, Processes and Technology.

Policy without enforcement is a suggestion!

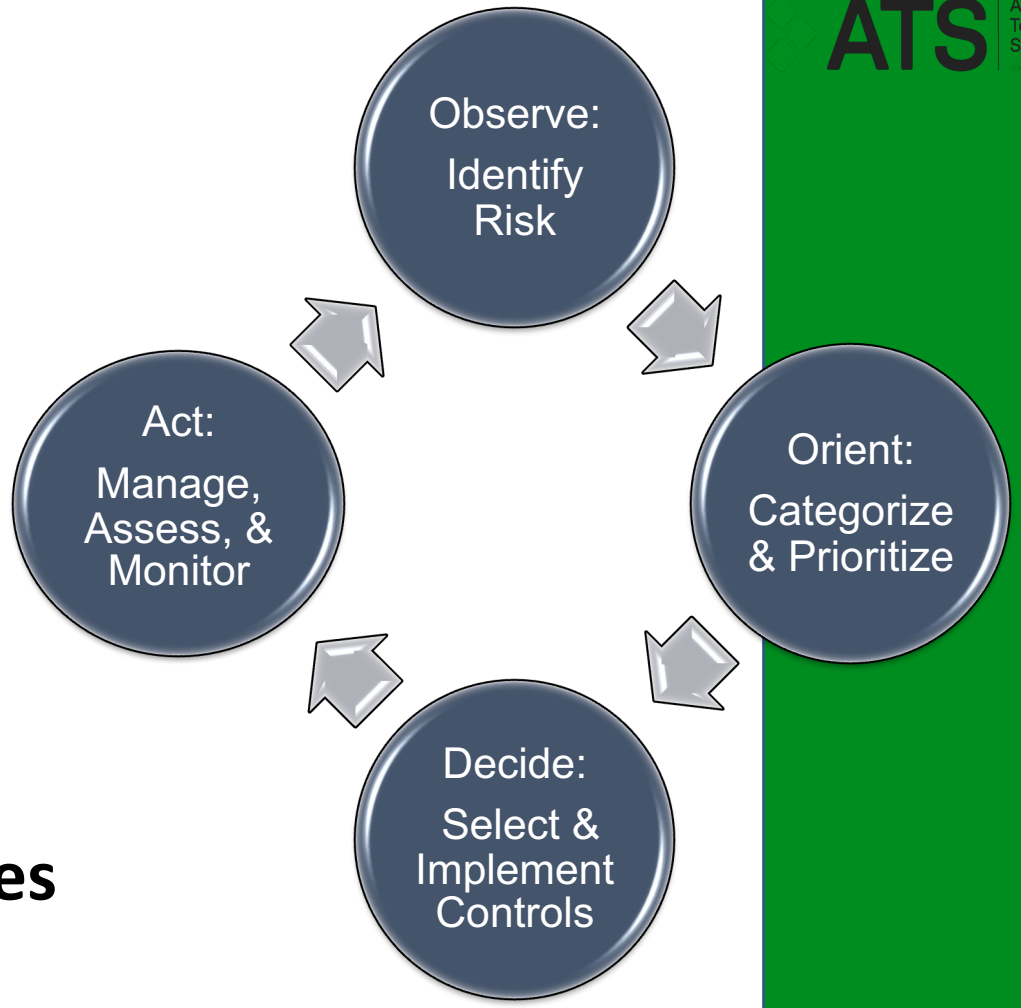
Processes reflect the need of people in relation to policies & Technology



Reduce reliance and burden on people

Start with People

Risk Management should:



- Support the strategic objectives
- Enhance institutional decision-making
- Create a “risk-aware” culture
- Reduce operational surprises and losses
- Assure greater business continuity
- Improve use of funding by aligning resources with objectives
- Bridge departmental silos

Governance Terminology

- **Policies: Formal statements produced and supported by senior management.** (Approved by your board)

- **Standards: Mandatory courses of action or rules that give formal policies support and direction.** (Approved by leadership team)

- **Procedures: Detailed step-by-step technical instructions to achieve a goal or mandate.** (Managed by tech team)

Document Policies and Procedures

- **Data Integrity Procedures** (Backups, *retention, restore (overwrite) authorization, etc.*) *(Link to templates)*
- **Data Governance Procedures** (DATA *handling, lifecycle, deletion, access control, access authentication, etc.*)
- **Data Classification Procedures** (PII, PCI, PHI, *and how the entity stores, accesses, and manages that data*)
- **Email Retention Policy and Procedures** (*email is one of our significant internal liabilities*)
- **Incident Response Plan (Policies & Procedures)** *(Link to templates)*
- **Cyber Security (Policies and Procedures)** *(Link to templates)*

Information Security Must Haves

- Functioning cybersecurity basics.
- Policies and procedures (especially for cybersecurity).
- Incident response plan.
- Out-of-Band secure communication
- Training of all employees -- phish all -- (esp. Leadership).
- Managed antivirus and malware detection 24/7.
- Privilege management & multi-factor authentication (MFA).
- Backups segmented from the network.
- Encryption for sensitive and air-gap for hypersensitive data.
- Defined logging and retention.
- Third-party security and supply chain risk management.

Individuals Enable Hacking

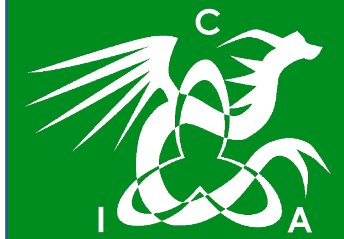
- **People make mistakes by:**
  - **Sharing** passwords
  - Using **outdated** software
  - Losing or **improperly** discarding files
  - **Mishandling** personal information
  - Storing **unencrypted** personal information on laptops or easily lost mobile devices
  - **Circumventing** information **security controls**
    - Intentionally for **their** purposes;
    - In the **mistaken belief** that they can improve efficiency;
    - In narrow-mindedly thinking that they "**just need to get the job done**" regardless of risk

Overlooked Data Issues

- Data Disclosure: (i.e., Websites, Social media, recorded talks, sharing personal data without agreements or consent)

- Untrusted Resources: (Personal devices and storage + downloaded software or apps, opening any and all attachments by staff or contractors)

- Unstructured Information: (i.e., email, cloud storage with little to no oversight, security, or privacy)



Secure Messaging is a Must!

The GC, Divisions, and Unions need an official, secure, and private messaging app.

It must meet international privacy regulations.

There should be <u>ONE</u> official application

Image Source https://www.boardeffect.com

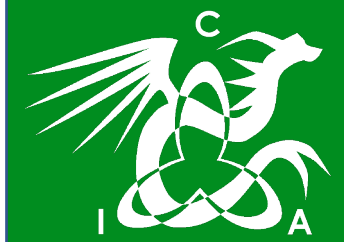
Other SDA's have learned that…

1. We are never as secure as we think we are - Regular and engaging education of users.

2. We need a weapons-grade backup system that has been tested and verified.

3. All data systems are inherently insecure. Know what data you have and where it is located.

- 4. Your response is more important than your data security software. You need a plan!



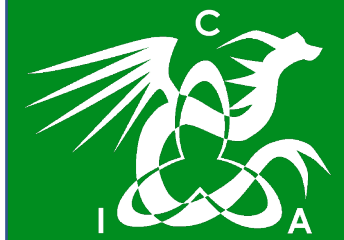
The Twelve Apostles of Policies 1-4

1. **Information Security (IS) Policy –** Includes procedures for controls for unauthorized users or access to data, programs, systems, or the infrastructure.

2. **Access Control Policy -** Includes requirements for managing users and file access using role-based control.

3. **Password Policy** - Includes requirements for password minimum length, complexity, the use of old passwords, and expiration.

4. **Data Classification Policy -** Dictates how the data should be secured and what controls should be put in place to protect the data.



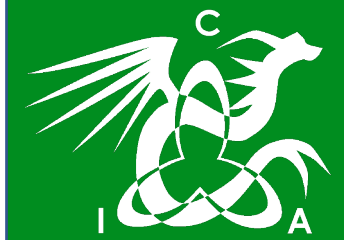
The Twelve Apostles of Policies 5-8

5. **Physical Security Policy -** Defines the requirements for protecting information and technology resources from physical and environmental threats.

6. **Acceptable Use Policy -** Dictates how company resources should be used by employees and contractors.

7. **Backup Policy -** Defines an organization's requirements for the backup of company data and systems.

8. **Logging and Monitoring Policy -** Documents the requirements for logging user activity and the procedures for reviewing the logs.



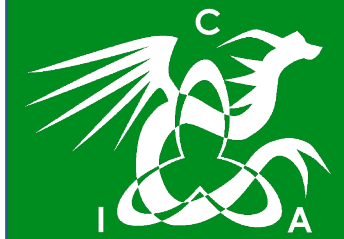
The Twelve Apostles of Policies 9-12

9. **Risk Assessment Policy -** Documents the procedures for performing periodic risk assessments.

10. **Change Management Policy -** Documents the procedures for making changes to IT infrastructure and applications.

11. **Incident Response Policy -** Documents the procedures that security personnel should follow when a security incident has been identified.

12. **Business Continuity Plan -** Documents how to continue operations when affected by different levels of disaster, which can be localized short-term disasters, multi-day-long building-wide problems, or even a permanent loss of a building.



Resources

https://t.ly/ATS-2023

ATS-2023

Name

- 2023 Current Legal and Security Trends
- Backup Risk Assessment
- GDPR
- Incident Response and Business Continuity
- Messaging Tool Issues
- Mobile Device
- Policy Templates and examples
- Ransomware resources
- Technical IT Best Practices
- User Training
- Vendor Vetting

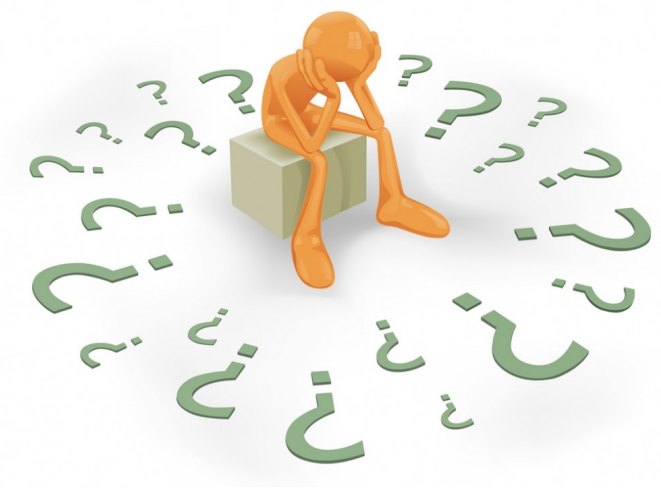
ATS Adventist Technology Summit

Handouts
https://t.ly/ATS-2023

C I A

Where to Start ???

1. Document Policies & Standards
   (organization Incident Response not IT Incident Response)
2. Know "Current" Requirements
3. Prepare For Hidden Costs
4. Test Incident Response with Leadership
5. Chose One Secure Messaging System
6. Learn From Others
7. Driven by Leadership



ATS Adventist Technology Summit

Handouts
https://t.ly/ATS-2023

C I A