Bringing Compliance Under Control: Key Technologies to Consider

Trent Henry
Senior Analyst
Burton Group

Thesis

- Compliance mandates have many common, overlapping requirements
- technology controls that are reusable
- The market provides no silver bullet, but several technologies offer strong control foundations

Agenda

- Compliance: Focusing on controls
- Regulations and their security impact
- Key technologies and trends
- Recommendations

Compliance: Focusing on Controls

- Industry focus on “compliance” and “regulation” is sometimes a problem
  - Vendors are using compliance as key messaging
  - Organizations are confused about product choice
- A better focus is “controls”
  - What activities should we be doing?
  - What relationships help to define requirements?
- 30 years of infosec has taught us much…

Controls

- Management of configuration
- User separation
- Confidentiality protection
- Infrastructure monitoring
- Perimeter layers and isolation
- Policies, personnel and other well-known program practices

When Regulations Create Control Outliers

- Specific business externalities: Records retention
  - “Preserve this document for seven years”
- Legal realities: E-discovery
  - Electronic information’s status in courts is relatively new; requires new processes to handle
- Controls inadequacy: Private data & segregation
  - Economics in North America haven’t created good customer-data-handling norms; we often over-trust admins
- Proof of action: Evidence
  - It’s not enough simply to put controls in place; third parties must be shown their effectiveness over time

You Know

- Very few regulations will provide definitive guidance for controls
  - Although security practitioners *do* read regulations, they are still left asking questions
- For real requirements, hone critical relationships
  - Internal and external audit
  - Operational groups
  - The legal team
  - Public relations and HR
- These relationships also help to identify outliers
  - Compliance involves negotiating conflicting requirements and interpretations

Impact

- Compliance mandates can often be boiled down to security objectives:

C

Confidentiality: A security objective to prevent disclosure of inappropriate information to subjects

Integrity: A security objective to prevent unauthorized or inappropriate changes and ensure that information maintains internal and external consistency

I

A

Availability: Availability is expressed in terms of the percentage of time a particular object of interest is usable for a particular purpose

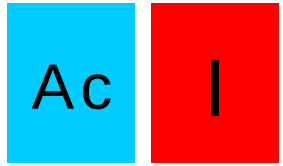
Use Control: A security objective to control which subjects can perform which actions on specific objects

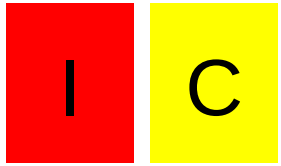
U

Ac

Accountability: A security objective that requires subjects to be held accountable, liable to be called to account for, or held answerable for something

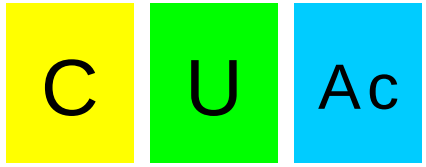
- Both regulations are concerned about consumer financial protection and are relatively prescriptive
- "Guidance" for stronger authentication per risk (transaction integrity)
- PCI: Protect cardholder data, monitor networks, safeguard configs & applications





Customer Data Protection: HIPAA,

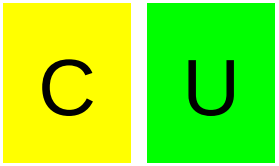
- In addition to security policies, focus on
- Much less prescriptive; more focused on risk assessment and comprehensive controls



- Also considerable requirement for handling data outside technical realm

Others

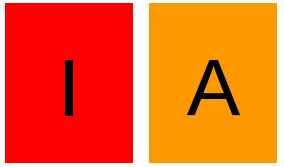
- Disclosure acts have become the great
- Some non-technical controls: Opt-out, non-persistent relationships, relocation
- Technical controls: Heavy confidentiality with some use-control



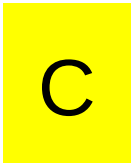
- Blend of preventative and detective tools

The Stalwart: SOX

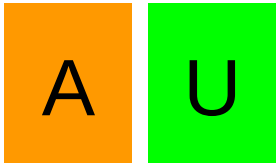
- Security teams were previously so focused on confidentiality that SOX was -up call for other critical objectives
  - Integrity and availability of financial data



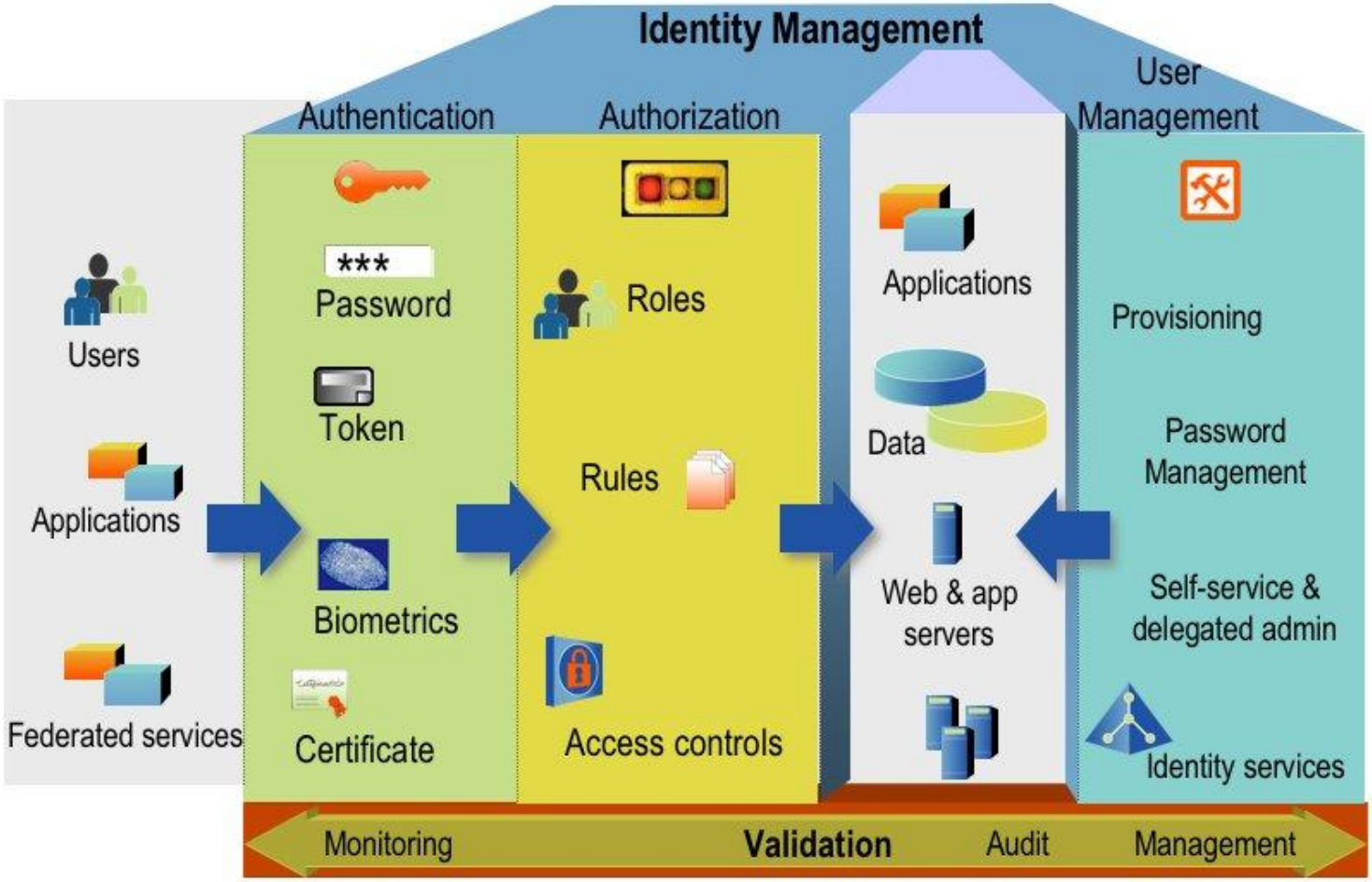
- Pillars are change-control, segregation of duties, & monitoring (many look to

- Note: No 

(for now)



Key Technologies: Identity



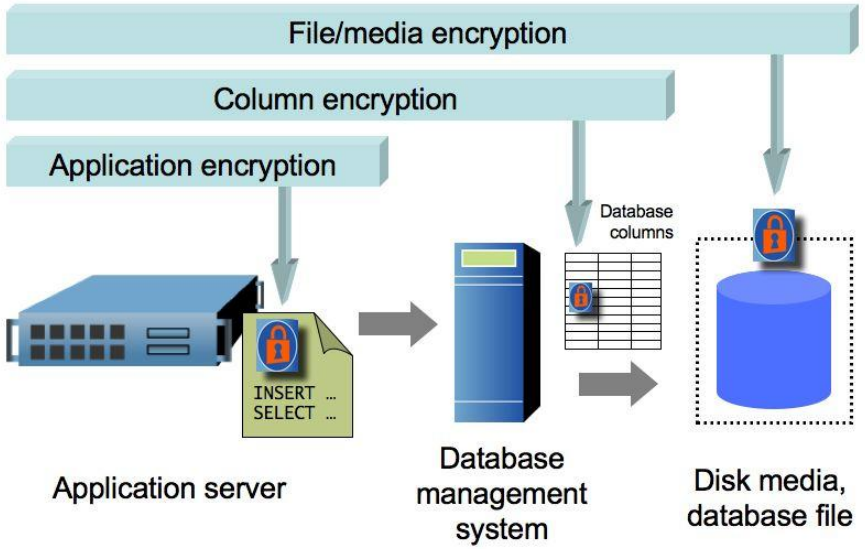
C

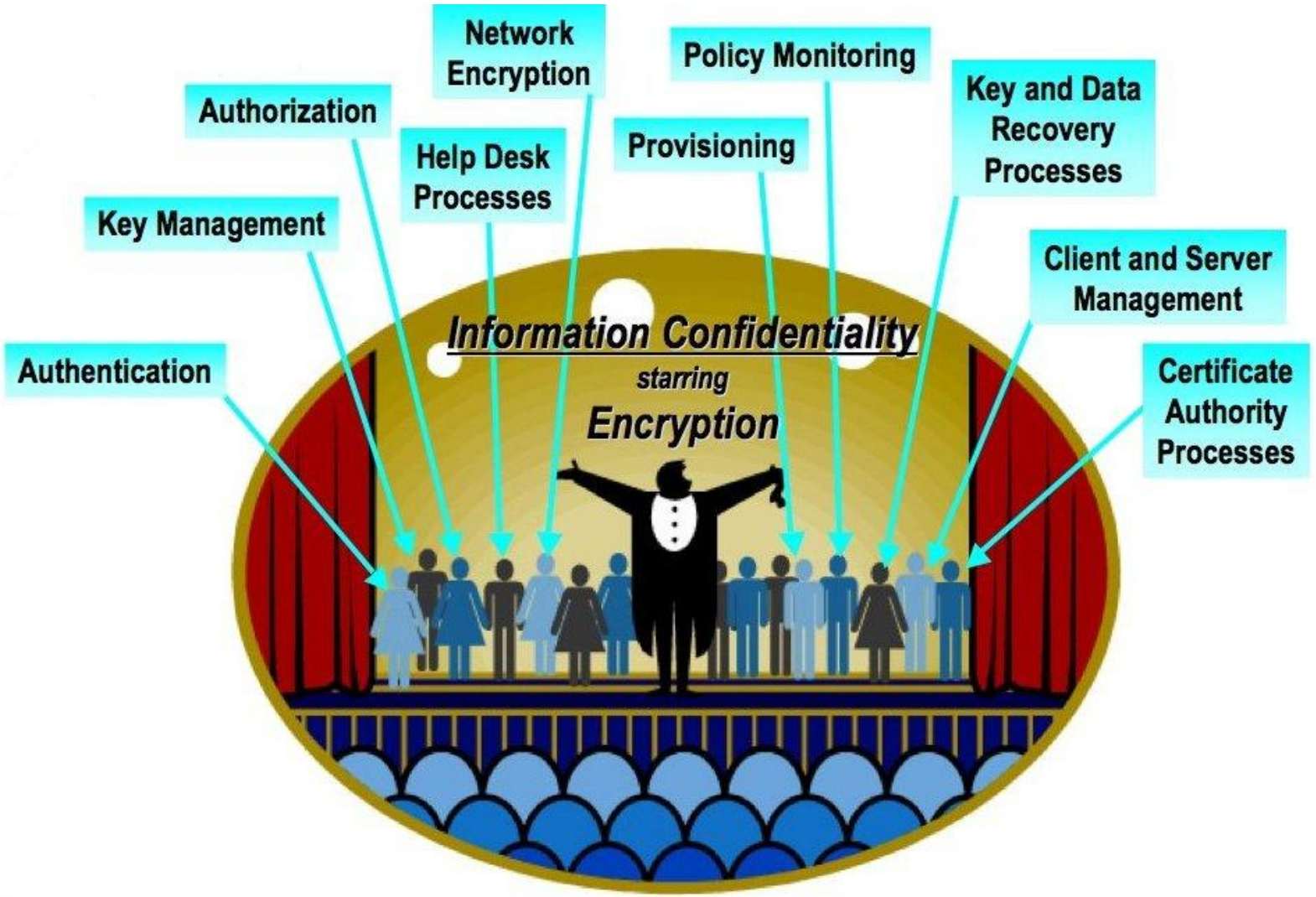
I

Ac

C U

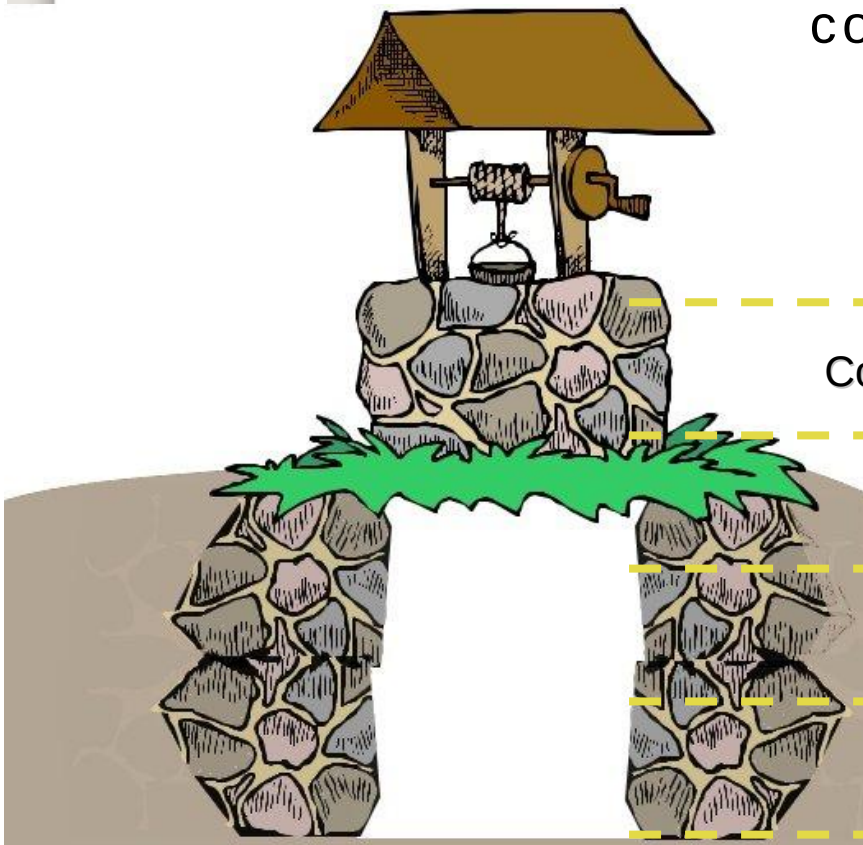
- Aside from SOX, most compliance mandates have a heavy dose of confidentiality
- “Get out of jail” for disclosures
- Encryption layer is of great import
  - Protect against varying threats




Network Encryption
Policy Monitoring
Authorization
Key and Data Recovery Processes
Help Desk Processes
Provisioning
Key Management
Client and Server Management
Information Confidentiality
starring
Encryption
Authentication
Certificate Authority Processes

Trends

- Defense-in-depth brought to content
  - More opportunities to prevent misuse
  - More opportunities to detect failure of protection



Connection-oriented perimeter Æ content-aware

Authenticated users Æ fine-grained authorization

General net monitoring Æ application-aware data auditing & monitoring

“Wild west” users Æ information controls at point-of-use

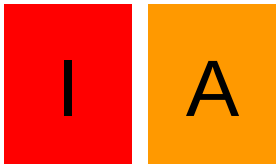
Key Technologies: Data Leakage Protection

C

U

- Access management and encryption are preventive controls
  - Their limitations require detective counterparts
- Two growing technology categories
  - Network content filters (content monitoring & -aware analysis -- moving toward endpoints, also…
  - Database auditing & monitoring: Deep analysis of DBMS transactions -- evolving from SOX-oriented segregation of duties toward PCI privacy protection

Key Technologies: Technical Policy Management



- Products blending system/configuration, patch and vulnerability management
- Apply to all compliance mandates, but PCI and SOX have particularly driven them
- Focus is on preserving endpoint integrity: Both clients and servers
- Huge interest in health-check elements of network admission technologies

Key Technologies: Perimeter Protection

- Although often course-grained, perimeters are essential and contribute to all security objectives
  - And increasingly content-related
- “ ” notwithstanding, perimeters are alive and well
  - And explicitly denoted in PCI
- Both preventive (firewalls) and detective (IDS/IPS)

C

I

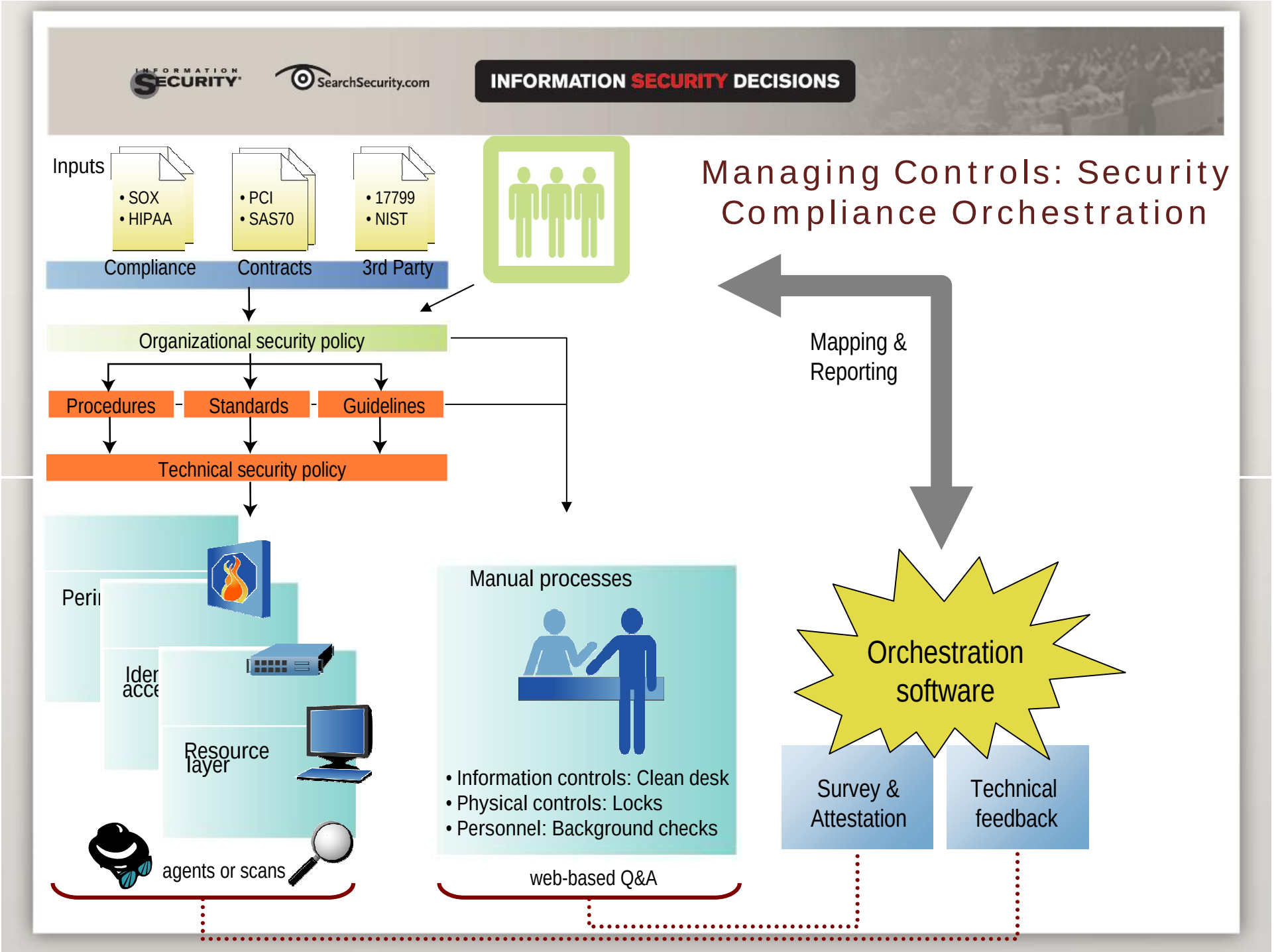
A

U

Ac

Recommendations

- Recognize where technology *shouldn't* be
  - Many controls are non-technical
- List prescriptive compliance requirements and security objectives
  - Then map to the appropriate technologies that cover those objectives
- Ensure that once deployed, products provide evidence of control activity
- Consider compliance orchestration…


INFORMATION SECURITY
SearchSecurity.com
INFORMATION SECURITY DECISIONS
Managing Controls: Security Compliance Orchestration
Inputs
• SOX
• HIPAA
• PCI
• SAS70
• 17799
• NIST
Compliance
Contracts
3rd Party
Organizational security policy
Procedures
Standards
Guidelines
Technical security policy
Mapping & Reporting
Orchestration software
Survey & Attestation
Technical feedback
Manual processes
• Information controls: Clean desk
• Physical controls: Locks
• Personnel: Background checks
Resource layer
agents or scans
web-based Q&A

Conclusion

- Although specific compliance mandates drive particular technologies, security objectives help guide overlap and re-use
  - C, I, A, U, Ac
- Many prudent controls come from a long history of infosec and forged relationships
- encryption, leakage protection, technical policy management, and perimeters
  - Brought together with compliance orchestration

Thanks for joining us!

- See an exclusive tip from Trent Henry on encryption and compliance:

  http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1263634,00.html

- Check out more of the great resources in SearchSecurity.com's Compliance School:

  http://searchsecurity.com/complianceschool