InfoSec Compliance

PUTTING THE "C" IN "GRC"

Braun Tacon
BraunsBlog.com

Compliance defined:

- com·pli·ance (kəm-plīˈəns)
  n.
  - The act of complying with a wish, request, or demand; acquiescence.
  - *Medicine*. Willingness to follow a prescribed course of treatment.
- A disposition or tendency to yield to the will of others.
  - Extension or displacement of a loaded structure per unit load.
  - Flexibility.

Compliance reality:

Compliance is a process, not an event

5 Pillars of Compliance:

- Information classification
- People and Access
- Accountability and Traceability
- Confidence
- Endurance

5 Pillars of Compliance:

- Information Classification
- People and Access
- Accountability and Traceability
- Confidence
- Endurance

Information Classification

- What data are you trying to protect, i.e. email, financials, trade-secrets, etc?
- What are you complying with, i.e. HIPPA, GLBA, SOX, EU Directive, etc?
- Who owns it?
- How much do you care? (How much protection? What priority?)

5 Pillars of Compliance:

- Information classification
- People and Access
- Accountability and Traceability
- Confidence
- Endurance

People and Access

- User provisioning and access
  - Top concern for Enterprise
  - Most significant impact
  - No easy fix
  - Ever changing
  - EVERYONE wants it
- Don’t forget those “Roles”

5 Pillars of Compliance:

- Information classification
- People and Access
- Accountability and Traceability
- Confidence
- Endurance

Accountability and Traceability

- Who is accessing the data
  - Unique User ID
  - Smartcards
  - PKI
- What data is being accessed
  - What
  - When
  - Why

Accountability and Traceability

- Training and education
- Ongoing status (Transparency)
- Ownership
  - CFE requirement
  - Make it easy to own
- Centralize management, push responsibility to the lowest levels possible
- Track, report, learn

5 Pillars of Compliance:

- Information classification
- People and Access
- Accountability and Traceability
- Confidence
- Endurance

Confidence

- Policy and standard based architecture
- Accurate auditing and reporting
- 24 X 7 support (SLA)
- Effective incident response

5 Pillars of Compliance:

- Information classification
- People and Access
- Accountability and Traceability
- Confidence
- Endurance

Endurance

- This is not a race
- Make it a part of your process, not an annual event
- Make sure you have a budget to pull this off
- Get lean…automate when possible, always look for ways to improve