HITRUST Control Categories

Scoping Factors

- **Regulatory**
  - Federal, state and domain specific compliance requirements

- **Organization**
  - Geographic factors
  - Number of covered lives

- **System**
  - Data stores
  - External connections
  - Number of users/transactions

Control Levels

- **Level 1**
  - Fundamental level of control required during normal business operations

- **Level 2**
  - More restrictive requirements for organizations and systems which have an elevated level of risk

- **Level 3**
  - Most restrictive controls required for environments with the greatest level of risk

Control Categories

1. Information Security Management Program
2. Access Control
3. Human Resources Security
4. Risk Management
5. Security Policy
6. Organization of Information Security
7. Compliance
8. Asset Management
9. Physical and Environmental Security
10. Communications and Operations Management
11. Information Systems Acq, Dev, & Maintenance
12. Information Security Incident Management
14. Privacy Practices