HITRUST Control Categories

Industry Standards

Scoping Factors

Regulatory

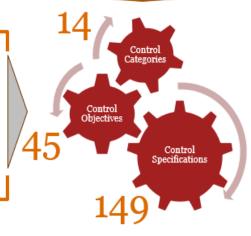
 Federal, state and domain specific compliance requirements

Organization

- Geographic factors
- Number of covered lives

System

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



Control Categories

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

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 2

· Most restrictive controls required for environments with the greatest level of risk