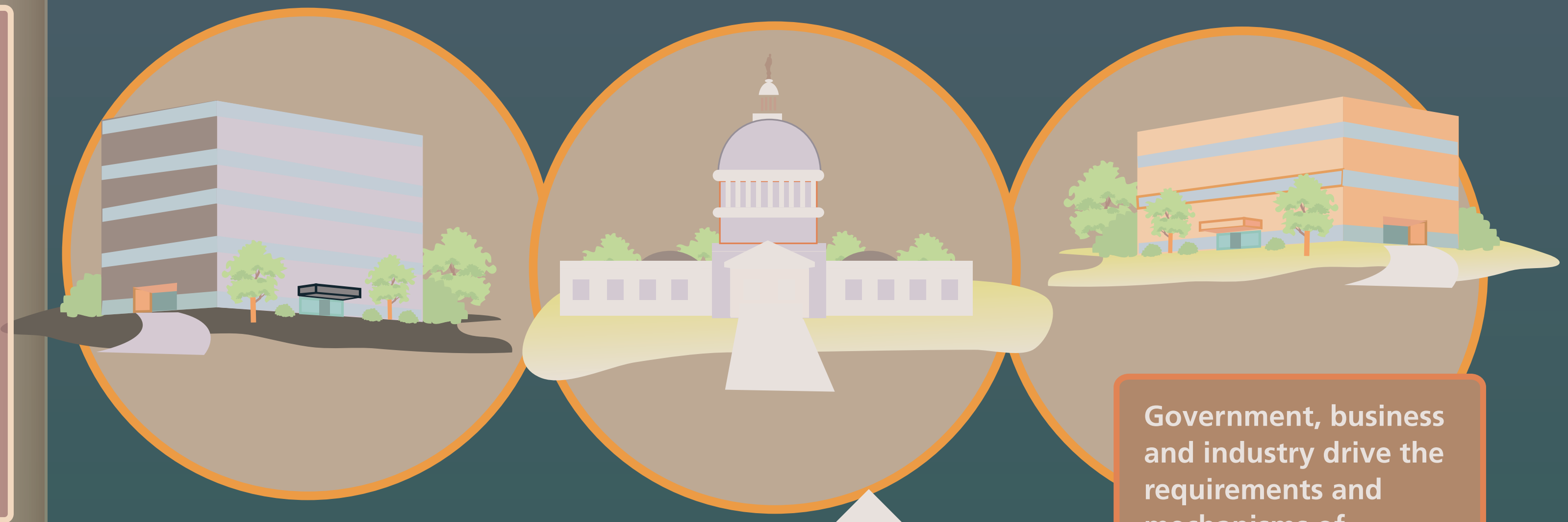
Making Security Measurable

Business and Government

Regulatory Compliance
Sarbanes-Oxley
HIPAA
FISMA
Future laws

ROI

Risk Management



Government, business and industry drive the requirements and mechanisms of information security

Enterprise Security Management

Standards
ISO/IEC 17799
COBIT
NIST SP800-53
ITIL
DoD 8500.2

Security Automation
CND
FDCC/USGCB

Policy makers must demonstrate how IT processes meet business goals

Information Technology

CVE	CWE
OVAL	SBVR
CCE	CAPEC
CPE	SCAP
CVSS	MAEC
XCCDF	CEE
OCIL	SwAAP

Vulnerability Management
Patch Management
System Assessment
Asset Management
Malware Protection
Software Assurance

IT processes must integrate with each other while demonstrating how they meet policy objectives

https://measurablesecurity.mitre.org/