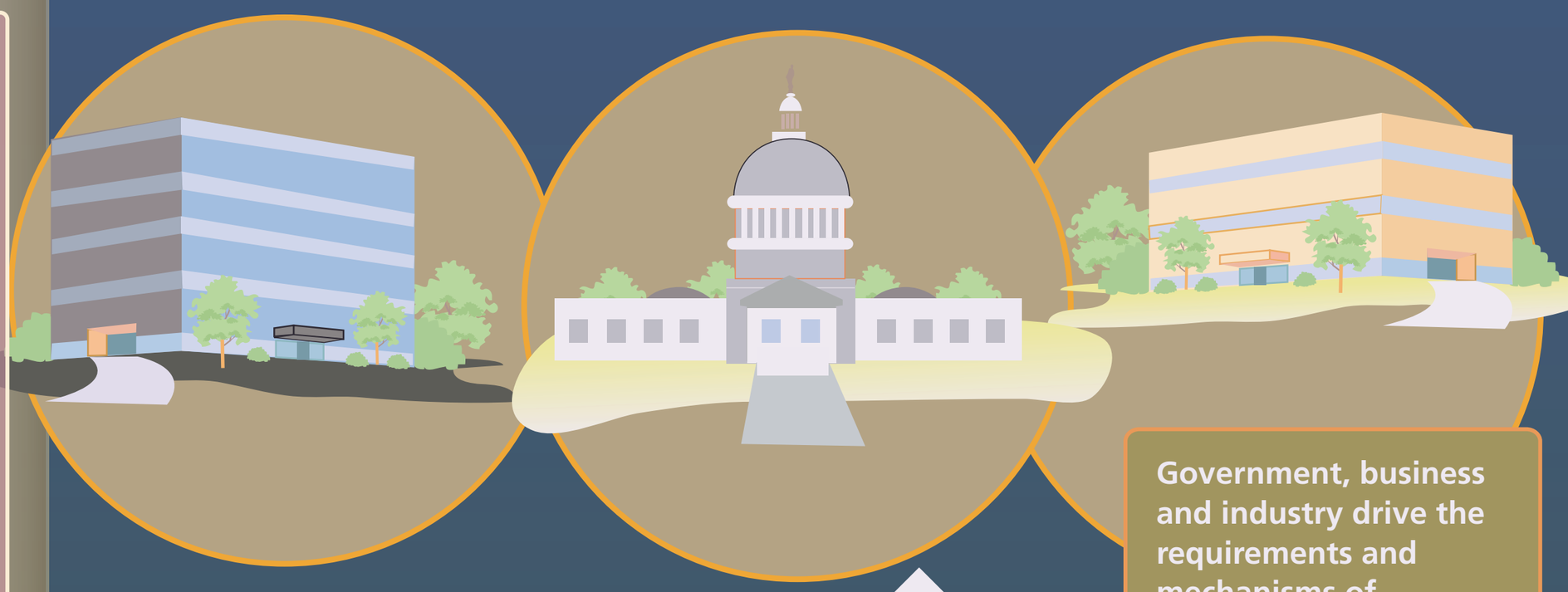
Making Security Measurable

Business and Government

Regulatory Compliance
Sarbanes-Oxley
HIPAA
FISMA
PCI
Future laws

ROI

Risk Management



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

Enterprise Security Management

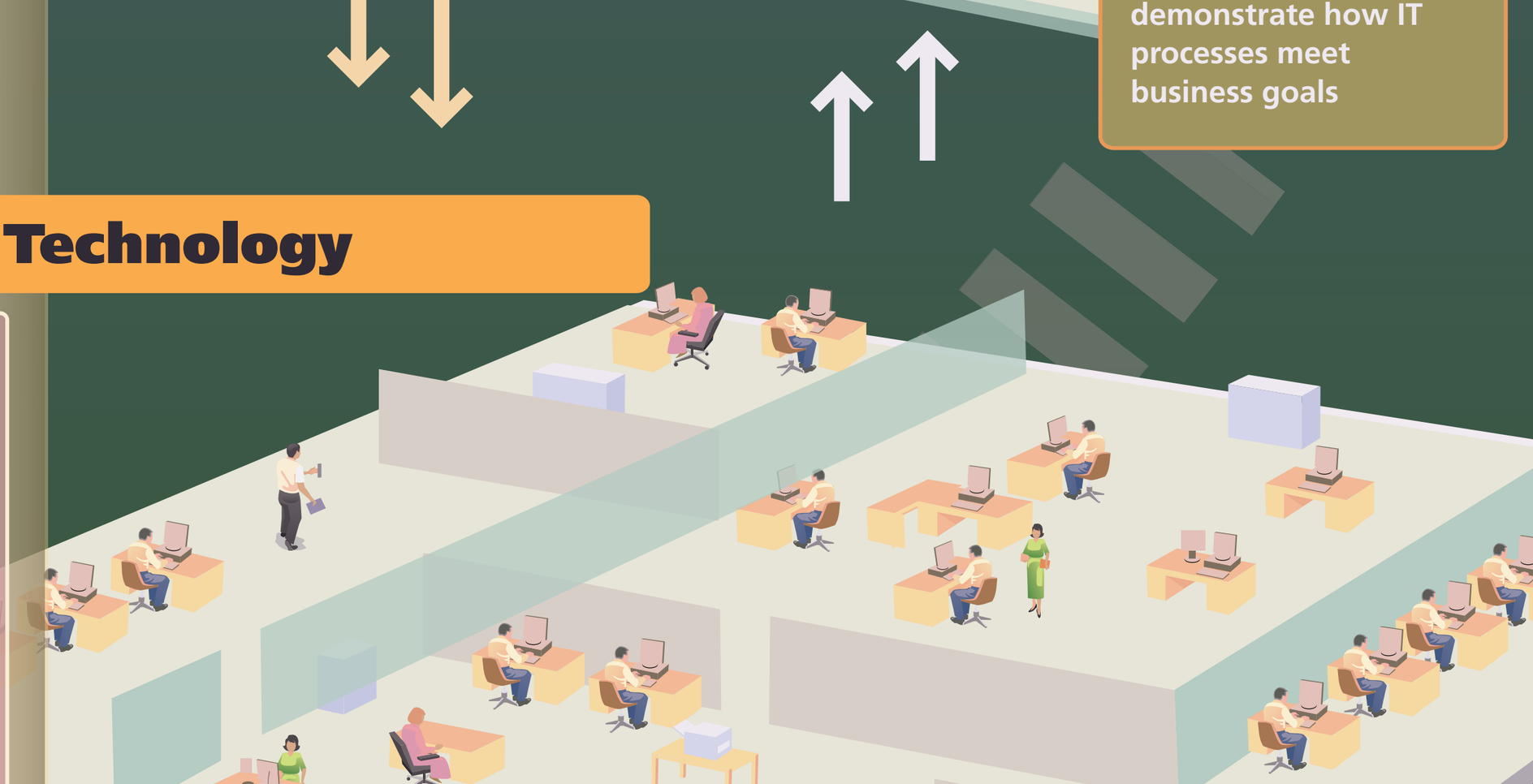
Standards
ISO/IEC 27000
COBIT
NIST SP800-53
ITIL
DoD 8500.2

Security Automation
CND
FDCC/USGCB

Policy makers must demonstrate how IT processes meet business goals

Information Technology

CVE	CWE
OVAL	CWSS
CCE	CAPEC
CPE	CybOX
XCCDF	STIX
CVSS	TAXII
OCIL	MAEC
CCSS	CEE
AI	EMAP
ARF	IODEF
SCAP	RID
SWID	RID-T



Vulnerability Management
Patch Management
System Assessment
Asset Management
Malware Protection
Software Assurance
Intrusion Detection
Indicator Sharing
Incident Coordination

IT processes must inte-grate with each other while demonstrating how they meet security and policy objectives