Integrating Cloud Computing into Your Data Security Program

David A. Cass
Senior Vice President & CISO
Elsevier

ELSEVIER

Integrating Cloud Computing into Your Data Security Program

Agenda

- Approach
- Challenges
- Key security risks
- Risk mitigation
- Score card
- Best practices

Integrating Cloud Computing into Your Data Security Program

Elsevier Cloud Approach

- Prevalence
- Business drivers
- Score card

Integrating Cloud Computing into Your Data Security Program

Challenges the classical security attributes

- Confidentiality, integrity, availability
  - System is no longer on premises
  - The infrastructure is shared
  - Access is through the internet

Integrating Cloud Computing into Your Data Security Program

Key Security Risks

- Governance & compliance
- Data management
- Cotenants/isolation failure
- Security procedures of providers
- Outsourcing
- Abuse of privileges by provider
- Regulatory & legal
- Business continuity & disaster recovery

Integrating Cloud Computing into Your Data Security Program

Risk Mitigation

- Contracts & SLAs
- Encryption
- Auditing
- Security certifications
- Provider insurance policy

Integrating Cloud Computing into Your Data Security Program

Cloud Readiness Scorecard

- Technology stack
- Integration complexity
- Business drivers
- SLA
- Regulatory
- Data transfer/networking
- Information security

Integrating Cloud Computing into Your Data Security Program

Best Practices

- Calculate ROI of on-premises vs. cloud
- Evaluate Scorecard rating
- Review information security practices of provider
- Review SLAs
- Evaluate elasticity & scalability

Integrating Cloud Computing into Your Data Security Program

Questions?

David Cass, SVP & CISO
Elsevier
Office: (215) 239-3210
E-mail: d.cass@elsevier.com

Integrating Cloud Computing Into Your Data Security Program

Michael Garson

Former Chief Compliance Officer & Technology Control Officer

LGS Innovations

LGS

BELL LABS INNOVATIONS

COMPLIANCE WEEK 2012

Integrating Cloud Computing
Into Your Data Security Program

About LGS Innovations

- Delivers advanced networking and communications solutions to U.S. federal government
- Subsidiary of Alcatel-Lucent, provider of mobile, fixed, IP, and optics communications technologies
- More than 650 employees; offices in Colorado, Illinois, Maryland, New Jersey, North Carolina, and Virginia

Integrating Cloud Computing Into Your Data Security Program

Chief Compliance Officer & Technology Control Officer Role at LGS

- Responsible for development and implementation of LGS compliance program and infrastructure
- Educate and train LGS personnel on particular aspects of doing business with U.S. government
- Manage compliance audits and reviews
- Create policies and infrastructure for control of proprietary, technical, and non-public information

Integrating Cloud Computing Into Your Data Security Program

Compliance Coordination and Implementation

- LGS compliance committee
- Compliance manager/administration
- LGS legal department
- LGS security department
- LGS functional leaders (IT, Finance, Marketing, HR)
- Designated facility personnel

Integrating Cloud Computing Into Your Data Security Program

Data Security and Managed IT Services

- Background:
    - *Certain portions of LGS network outsourced to and managed by third party*
    - *Data maintained on servers or network subject to export controls or restrictions on access/dissemination*
- Issue:
    - *Limiting non-LGS physical and logical access to data at rest and in transit*
- Resolution:
    - *Contract standards, audit provisions, certifications, training*

Cloud Computing and Your Data Security Program

Laurel Geise
Vice President
Chief Compliance and Information Security Officer

CoreLogic®

About CoreLogic

CoreLogic (NYSE: CLGX) is a leading global provider of information, analytics and business services.

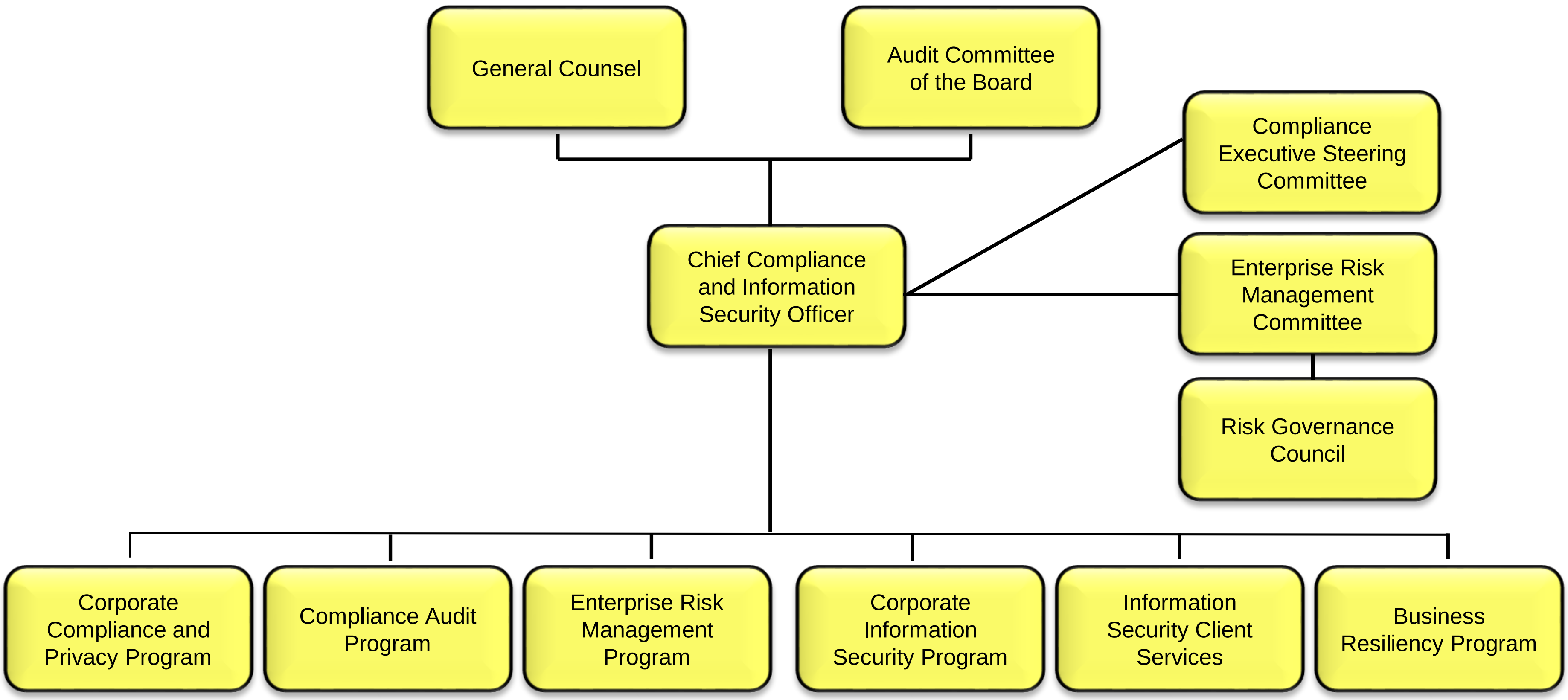
Based in Santa Ana, Calif., CoreLogic has 5,000 employees globally with 1.3 Billion in revenue in 2011.

CoreLogic has built the largest and most comprehensive U.S. real estate, mortgage application, fraud, and loan performance databases including public, contributory and proprietary data covering:

- National, state and city real estate trends, including foreclosure/delinquency rates, sales and pricing trends, negative equity rates and positive equity forecasts, distressed sales and shadow inventory
- Property-level residential real estate and foreclosure activity
- Mortgage fraud rates and risk assessments
- Flood and geospatial analytics
- Credit reports
- Property Tax records

Industries				
Automotive	Credit Card Services	Legal	Real Estate-Commercial	Telecommunications
Cable	Employment	Mortgage-Commercial	Real Estate-Multifamily	Title Agencies
Capital Markets-Investor	Government	Mortgage-Residential	Real Estate-Residential	Utility
Capital Markets-Issuer	Insurance	Oil and Gas	Retail	

Global Compliance Organization



General Counsel

Audit Committee of the Board

Chief Compliance and Information Security Officer

Compliance Executive Steering Committee

Enterprise Risk Management Committee

Risk Governance Council

Corporate Compliance and Privacy Program

Compliance Audit Program

Enterprise Risk Management Program

Corporate Information Security Program

Information Security Client Services

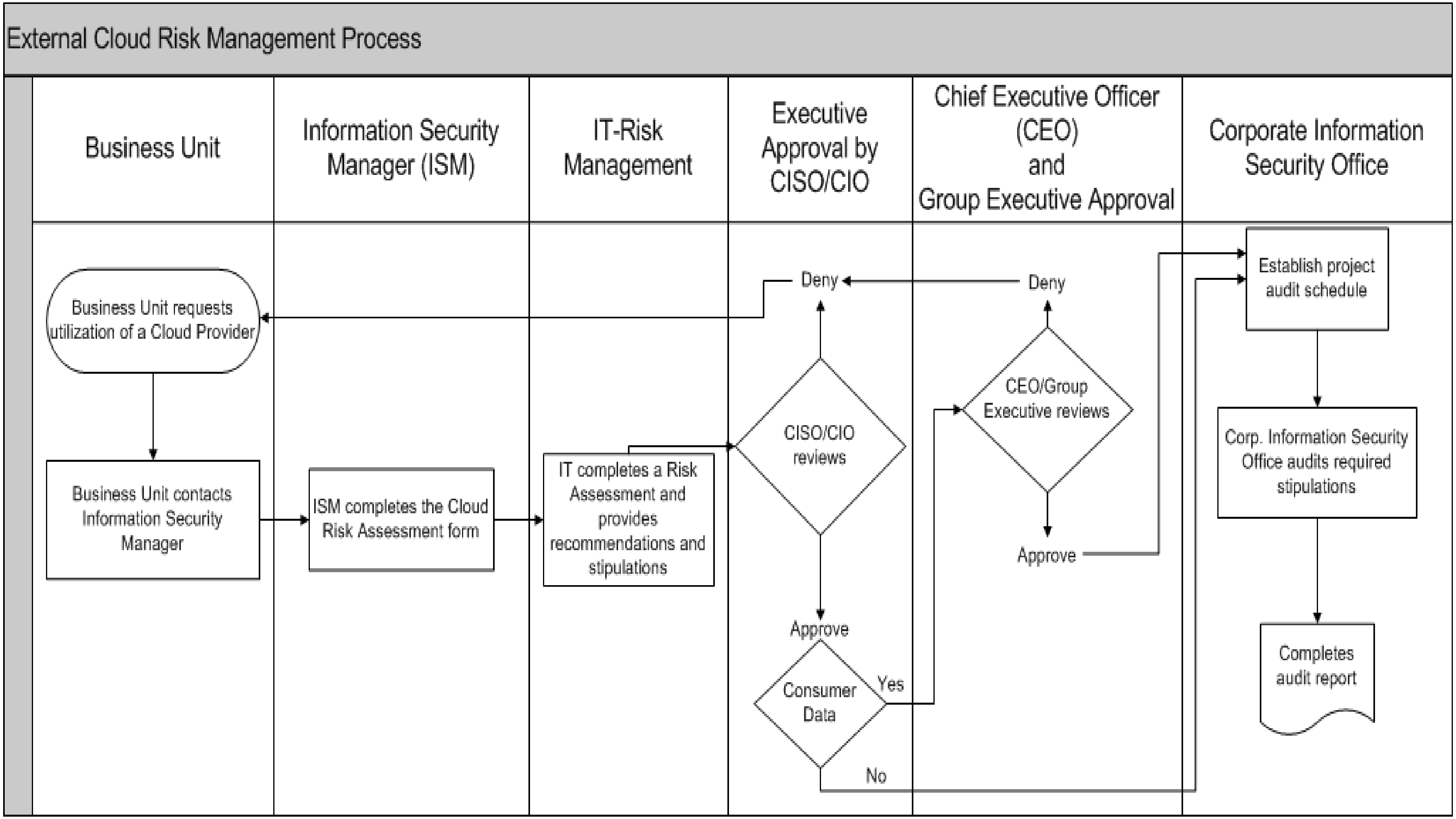
Business Resiliency Program

External Cloud Risk Management

Third Party Software Usage Policy

- CoreLogic uses a risk-based approach to moving assets to the cloud and identifying mandatory security controls.
- The Third-Party Software Usage Policy prohibits the use of external and hybrid cloud computing unless approved by the Chief Compliance and Information Security Officer and the Chief Information Officer.
- If the proposed use of cloud computing includes consumer data, it must also be approved by the Group Executive and Chief Executive Officer.

External Cloud Risk Management Process


External Cloud Risk Management Process
Business Unit
Information Security Manager (ISM)
IT-Risk Management
Executive Approval by CISO/CIO
Chief Executive Officer (CEO) and Group Executive Approval
Corporate Information Security Office
Business Unit requests utilization of a Cloud Provider
Business Unit contacts Information Security Manager
ISM completes the Cloud Risk Assessment form
IT completes a Risk Assessment and provides recommendations and stipulations
CISO/CIO reviews
Deny
Approve
Consumer Data
Yes
No
CEO/Group Executive reviews
Deny
Approve
Establish project audit schedule
Corp. Information Security Office audits required stipulations
Completes audit report

Information Security Audit Program

External Cloud Risk Management

- The Corporate Information Security Program Office audits all cloud vendors in order to assess and manage the overall risk of cloud vendors by determining their Information Security and Compliance risk posture.

- The goal is to help the business achieve strategic operating and financial objectives by providing information about the effectiveness of compliance controls, and by recommending a course of action to improve performance and reduce risk.

Training and Awareness

- Communication to business leadership on compliance with the Third-Party Software Usage Policy
- Monthly reminders in Information Security business line reports
- Quarterly status reporting to the Compliance Executive Steering Committee
- Annual Information Security awareness training
- Annual Information Security attestation