Opening the Black Box:

Vendor Management and Security in a Software as a Service World

CI-ISSA Chapter Meeting- May 9, 2019

Sid Bose, CIPT

IceMiller® LEGAL COUNSEL

icemiller.com

The Vendor Threat

"Third parties are the number one security risk to financial services firms in 2015."

- Booz Allen 2015 Annual Financial Services Cyber Security Trends

IceMiller® LEGAL COUNSEL

icemiller.com

Vendor Originating Threats

IceMiller® LEGAL COUNSEL

icemiller.com

Contract Goals

IceMiller® LEGAL COUNSEL

icemiller.com

Risk Identification and Assessment / Information Security Standard

ISACA Trust in, and value from, information systems

SANS

cloud security alliance® CSA

PCI Security Standards Council

Privacy Technical Assistance Center U.S. Department of Education

Center for Internet Security®

NIST

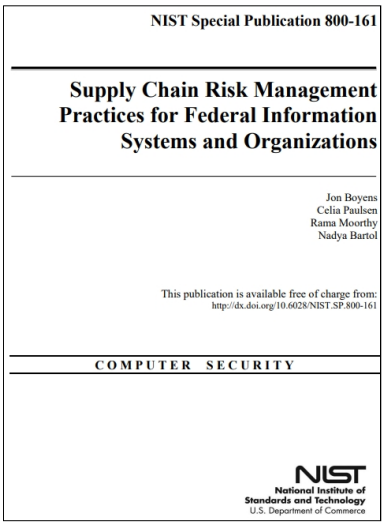
NCCoE National Cybersecurity Center of Excellence

PROTECTING AMERICA'S CONSUMERS

IceMiller® LEGAL COUNSEL

icemiller.com

Diligence



NIST Special Publication 800-161

Supply Chain Risk Management Practices for Federal Information Systems and Organizations

Jon Boyens
Celia Paulsen
Rama Moorthy
Nadya Bartol

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-161

COMPUTER SECURITY

NIST National Institute of Standards and Technology U.S. Department of Commerce

IceMiller® LEGAL COUNSEL

icemiller.com

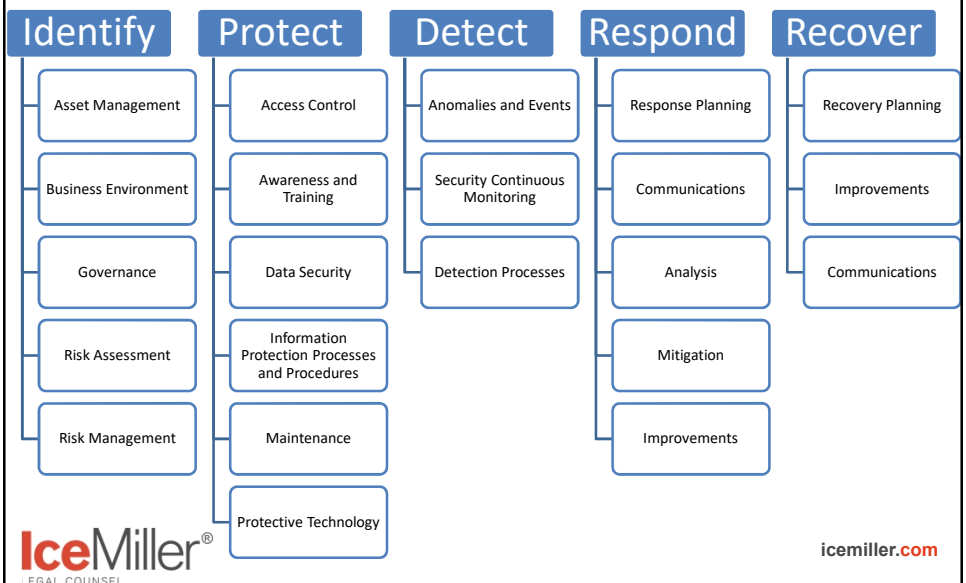
Diligence- Areas of Concern

- Base Controls
- Application Controls
- Cloud Security
- Infrastructure Controls
- Physical Security
- Backup & Recovery
- Electronic Transfer
- Privacy Management
- Physical Transfer
- Decommissioning & Destruction
- Physical "Paper" Management
- External Party Management

IceMiller® LEGAL COUNSEL

icemiller.com

Sample RFP Questionnaire (From NIST)



IceMiller® LEGAL COUNSEL

icemiller.com

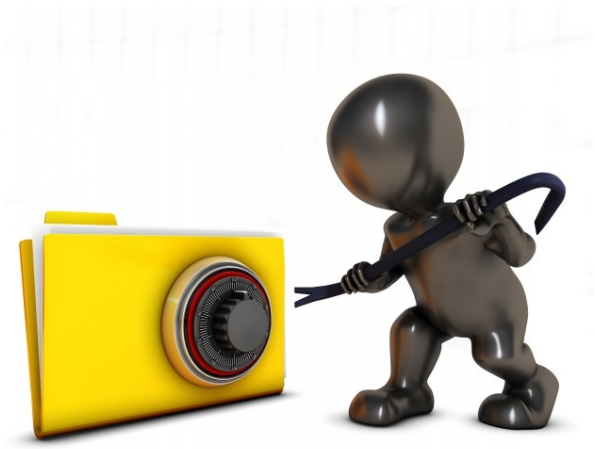
Data Security

Created by Macrovector - Freepik.com

IceMiller® LEGAL COUNSEL

icemiller.com

Data Breach Response and Notification



Created by Kjpargeter - Freepik.com

IceMiller® LEGAL COUNSEL

icemiller.com

Downstream Obligations (e.g. subcontractors)

Photo credit: ePublicist / Foter / CC BY-ND

IceMiller® LEGAL COUNSEL

icemiller.com

Insurance

First-Party Coverages	
Funds Transfer and Computer Fraud	Traditional Coverage
	Social Engineering
Network Interruption	Security Failure
	System Failure
	Contingent BI
Data Restoration	Security Failure
	System Failure
Cyber Extortion	
Breach Response	Notification
	Investigation
	Remediation
	Public Relations

Created by D3images - Freepik.com

Third-Party Coverages	
Privacy Liability	Privacy Claims
	Business Records Claims
	Regulatory Claims
Network Security Liability	
Media Liability	
Technology Errors & Omissions	

IceMiller® LEGAL COUNSEL

icemiller.com

Disaster Recovery & Business Continuity

Created by D3images - Freepik.com

IceMiller® LEGAL COUNSEL

icemiller.com

Audit

Created by Freepik

IceMiller® LEGAL COUNSEL

icemiller.com

Termination and Data Destruction

IceMiller® LEGAL COUNSEL

icemiller.com

Customer Privacy Concerns

IceMiller® LEGAL COUNSEL

icemiller.com

Other Contractual Concerns

- Vendor Business and Location
- Data Access and Segregation
- Personnel Issues
- Data Sharing
- Laws and Regulations

IceMiller® LEGAL COUNSEL

icemiller.com

Warranties, Representation, and Indemnity

- Warranties:
  - Enacted, and maintains an info. sec. program
  - Confidentiality obligations
  - Software and/or services are free of security defects
- Limitations:
  - 3x the contract value
  - Liquidated damages
- Indemnification:
  - Data breaches
    - E.g.: Third party damages
  - Breach of confidentiality obligations
  - Breach of warranties

IceMiller® LEGAL COUNSEL

icemiller.com

Q/A

IceMiller® LEGAL COUNSEL

icemiller.com

Thank You!

Sid Bose
Sid.Bose@icemiller.com
@IMSidBose

IceMiller® LEGAL COUNSEL

icemiller.com