SO YOU THINK YOU KNOW YOUR SaaS SECURITY AGREEMENTS?

APPENDIX

1. **SAAS Security Risk Assessments**
2. **Standard Warranties**

Disclaimer: The views expressed by the presenters are not necessarily the views shared or endorsed by their corporations, law firm or CSC®. This presentation is for informational purposes only and does not constitute legal advice.

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

April 24, 2019

Maryjane Hall Vice President Legal and Government Affairs and Assistant General Counsel, Federal Home Loan Bank of Chicago

APPENDIX

1. SAAS Security Risk Assessments
2. Standard Warranties

SaaS Security Risk Assessments

"Industry Standard" security questionnaires reflect a variety of security control frameworks.

NIST 800-53 Rev 5

20 Security and Privacy Control Groups
All organizations, public/private/non-profit
Maps to HIPAA Security Rule and federal agency guidelines
Also used with other systems to identify improvement opportunities

ISO 27001

Less technical, more risk management-based
6-step planning process for establishing an Information Security Management System
All organizations, public/private/non-profit

SaaS Security Risk Assessments

FFIEC	Federal Financial Institution Examination Council Cybersecurity Assessment Tool for Financial Institutions
PCI-DSS	Credit Card Processors
CIS/SANS20	20 Best Practice Controls Small number of prioritized controls to establish a baseline for cybersecurity and achieve immediate, high-impact results

SaaS Security Risk Assessments

SIG

Standardized Information Gathering Questionnaire developed by Shared Assessments

Incorporates all major Industry Standards, including cloud and mobile device security. Considered the most comprehensive.

Addresses risk controls across 16 risk areas.

Advantage; SaaS vendors fill it out once (annually) and provide to all customers in lieu of responding to multiple proprietary questionnaires.

1500 questions, but vendor or customer can focus the scope on the risk controls relevant to the services provided and the way they are provided (IaaS, PaaS, etc)

SaaS Security Risk Assessments

SIG

"Trust but Verify" Model

Trust Component	Questionnaire
Verify Component	Shared Assessments Agreed Upon Procedures (AUP)

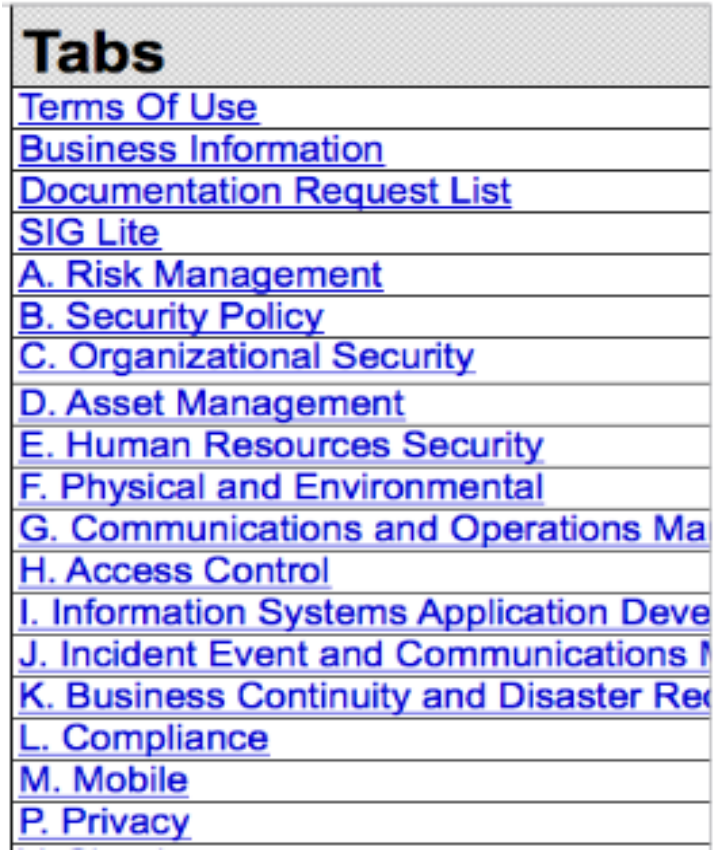
Includes a tool for Standardized **Onsite Assessments**

- Allows Customer to validate the questionnaire answers provided by the SaaS vendor.
- Sets forth the risk control areas to be assessed as part of an onsite assessment, as well as the procedures to be used.

SaaS Security Risk Assessments

SIG

Addresses risk controls across 16 risk areas



Tabs
Terms Of Use
Business Information
Documentation Request List
SIG Lite
A. Risk Management
B. Security Policy
C. Organizational Security
D. Asset Management
E. Human Resources Security
F. Physical and Environmental
G. Communications and Operations Ma
H. Access Control
I. Information Systems Application Deve
J. Incident Event and Communications M
K. Business Continuity and Disaster Rec
L. Compliance
M. Mobile
P. Privacy

SaaS Security Risk Assessments

SIG Lite

Subset of questions duplicated from all of the detail tabs for the full SIG

Intended for vendors offering lower risk services, or for an initial assessment of all vendors (RFP, etc.)

120 questions

SaaS Security Risk Assessments

VSAQ

Google's Vendor Security Assessment Questionnaire for security and privacy evaluation

Plain text and user friendly design

Web Application Security Questionnaire

Security & Privacy Program Questionnaire

Infrastructure Security Questionnaire

Physical & Datacenter Security Questionnaire

SaaS Security Risk Assessments

CAIQ

Consensus Assessments Initiative Questionnaire

Developed by Cloud Security Alliance to help provide “industry-accepted ways to document what security controls exist in IaaS, PaaS, and SaaS offerings, providing security control transparency.”

300 questions across 16 risk areas

2. Standard Warranties

Performance Warranty

- **Performance**
  - In a professional and workmanlike manner
  - In accordance with applicable industry standards
  - By qualified individuals who have suitable training and experience to perform the services

- **Compliance**
  - The customer's policies and requirements, data protection protocols and security policies
  - Laws and regulations
  - Contract requirements

Non-Infringement Warranty

Neither the services
nor the intended use
infringe any intellectual property rights of any third party

Disabling and Hostile Code

Use of the services do not and will not contain any code:

- Designed to disrupt, disable, or harm the operation of the service or any computer network
- Would permit the vendor or any other third party to access the customer's or any computer or network
- Would allow the vendor or any third party to track or monitor the use of the services or any computer or network system

Due Authority

Vendor warrants:

- It is duly registered and in good standing
- Necessary corporate authority
- Execution and performance will not violate the terms of any third party agreement obligation, including any judgment or order