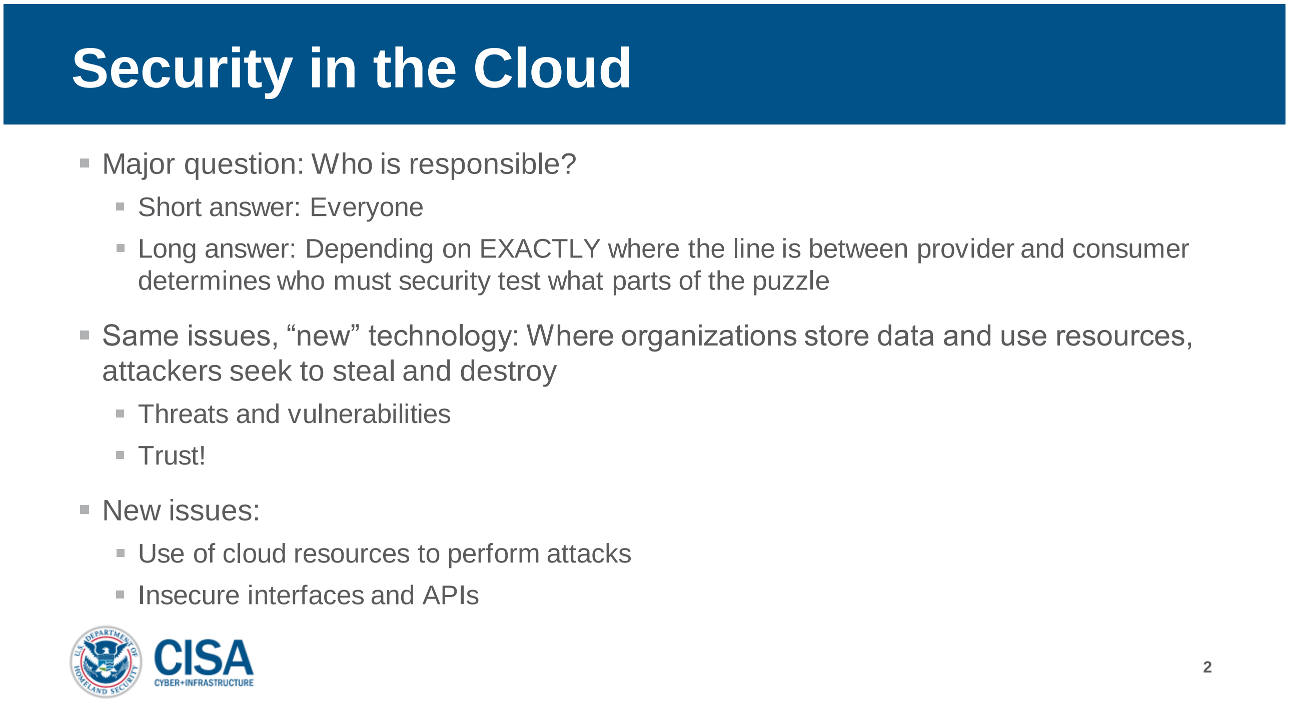
# Cloud Security

## Table of Contents



# Security in the Cloud

- Major question: Who is responsible?
  - Short answer: Everyone
  - Long answer: Depending on EXACTLY where the line is between provider and consumer determines who must security test what parts of the puzzle
- Same issues, “new” technology: Where organizations store data and use resources, attackers seek to steal and destroy
  - Threats and vulnerabilities
  - Trust!
- New issues:
  - Use of cloud resources to perform attacks
  - Insecure interfaces and APIs

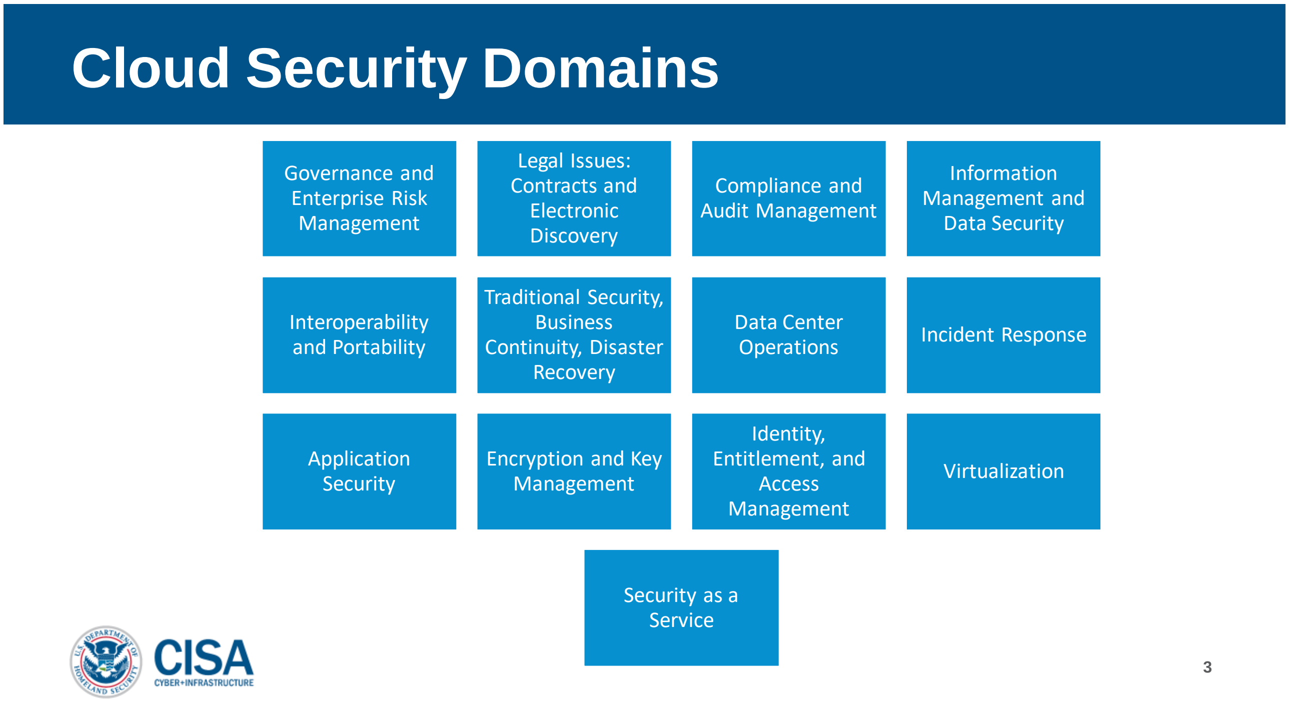
2

**002 The first major question that people ask about the cloud is, "Who is responsible for security in the cloud?" The short answer is, "Everyone." The longer answer really depends on what type of cloud we're actually dealing with? Is it a public cloud? Is it a private cloud? Is it infrastructure as a service? Is it software as a service? Wherever that line is, depends on who controls what part of the cloud.

So some of the security relies on the cloud provider to provide. Some of the security relies on the cloud consumer to provide for themselves. So it really depends on where that line is to determine who has responsibility for what? It's very important to have very clear service level agreements defined, to spell out in a legal document, who is responsible for what. Beyond that, it's all the same issues with a new technology. How the data is stored? Is the data stored securely? What are the threats and the vulnerabilities to that data? How can we trust the cloud provider? It's all the same questions as traditional security, we're just applying it, this new cloud concept. Now we do have some new issues. Primarily, with the use of infrastructure as a service and software as a service, cloud resources can be used to perform a task.

So as before, a distributed denial of service attack, basically required to have some kind of botnet to establish that distributed attack. Now an attacker can simply rent cloud resources to perform that attack without going to the trouble of creating a botnet. We also have insecure interfaces and APIs because the customer has to have some way to control their cloud resources. And that happens through a cloud interface or cloud API. But no software is perfect and those interfaces have issues. They have bugs. They have flaws and vulnerabilities. So that's a new level of software that we have to make sure we secure.

## Cloud Security Domains



# Cloud Security Domains

Governance and Enterprise Risk Management

Legal Issues: Contracts and Electronic Discovery

Compliance and Audit Management

Information Management and Data Security

Interoperability and Portability

Traditional Security, Business Continuity, Disaster Recovery

Data Center Operations

Incident Response

Application Security

Encryption and Key Management

Identity, Entitlement, and Access Management

Virtualization

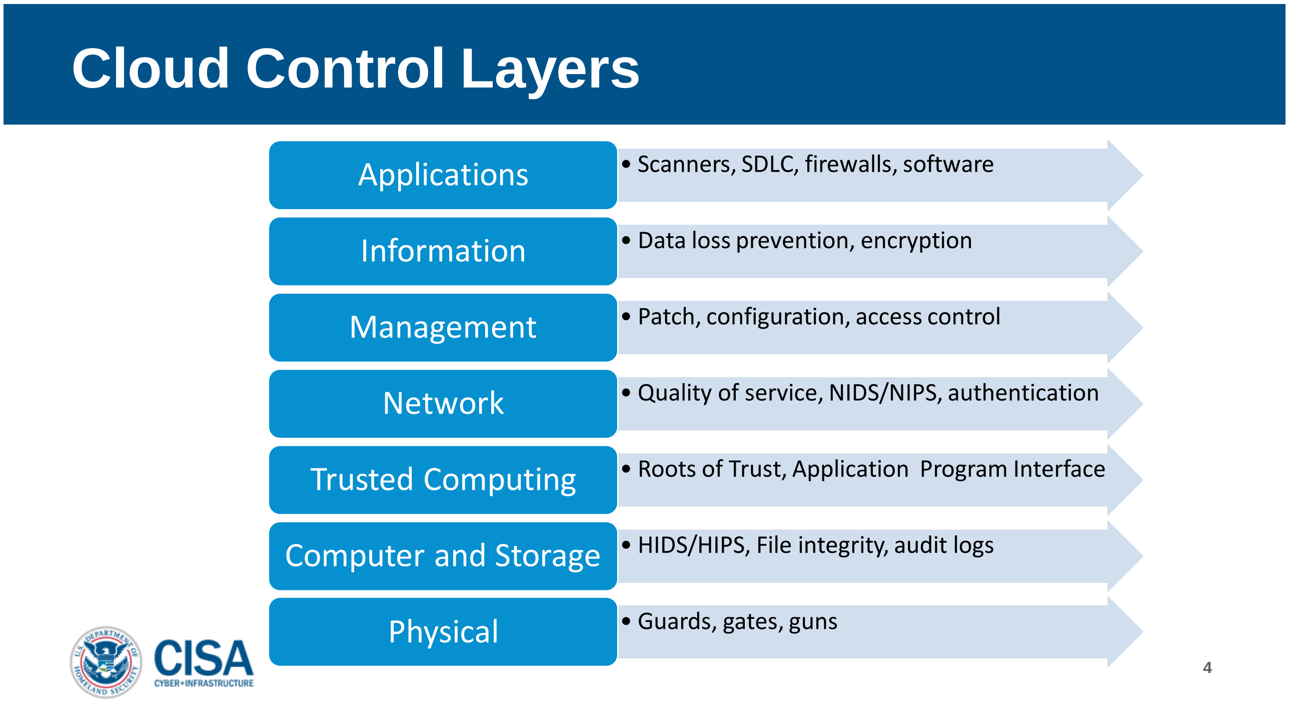
Security as a Service

3

**003 Cloud Security Domains. Some of them are the same as traditional security demands, because we still have incident response. We still have disaster recovery. We still have compliance and audit management. All of those are the same concepts, just in a new space. New demands include security of the service because as we offer software as a service and platforms as a service we can offer security as a service. Maybe it's a firewall as a service, or an intrusion detection as a service. We also have legal issues with contracts and electronic discovery because that cloud provider is now responsible for that data and may not own the data but it's responsible for it because it's sitting on their physical hardware. We also have issues of

Interoperability and Portability because the user needs to be able to access the cloud resources from wherever they have a network connection. The cloud provider can setup certain requirements that are - the consumer must provide. Like, they have to use a certain type of browser. They have to have a certain patch level. But the cloud provider is faced with that portability issue because that's one of the big draws of the cloud, is that we can access it anywhere.

## Cloud Control Layers



Cloud Control Layers

| | |
|---|---|
| Applications | • Scanners, SDLC, firewalls, software |
| Information | • Data loss prevention, encryption |
| Management | • Patch, configuration, access control |
| Network | • Quality of service, NIDS/NIPS, authentication |
| Trusted Computing | • Roots of Trust, Application  Program Interface |
| Computer and Storage | • HIDS/HIPS, File integrity, audit logs |
| Physical | • Guards, gates, guns |

CISA CYBER+INFRASTRUCTURE

**004 And here is some Cloud Control Layers. And this does come from the Cloud Security Alliance, Cloud Security Guide. So we have a physical layer. Same as the physical layer has always been. Guns, gates, guards. We have the computer and storage layer and this is where your host intrusion detection is going to live, as well as audit logs, your file integrity checks, anything that has to do with the storage. And then we have trusted computing and that's where your application program interfaces are going to come in.

Then we have network. That's going to be your quality of service, which is going to be critically important to any cloud provider, is that quality of service. We also have our network intrusion detection and prevention. Then for our management layer, we have patching configuration, access control, all concepts that have existed well before cloud computing. We're just applying it to a new set of technologies. And then, information. We have data loss prevention, encryption. Again, same concepts as before. We're just applying it to this new cloud concept. And then finally, we have the application layer. That's going to be your firewalls, any software solutions, any vulnerability scanners. And this is also going to be where your software development life cycle lives because how are you developing your application? When you're using a platform as a service and developing an application, how are you developing that application? Are you programming it in a secure manner? If you're not programming it in a secure manner, what is the threat, not only to your application, but to the cloud provider as a whole? So these are all different layers that have to be considered when we talk about cloud security.

## Notices

# Notices

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT D] Distribution authorized to the Department of Defense and U.S. DoD contractors only (administrative or operational use) (2016-05-01). Other requests shall be referred to DISA/RME.

DM-0004104