WITH THE CLOUD COMES GREAT RESPONSIBILITY — AND ROI

BARR ADVISORY

Table of Contents

THE PROMISES (AND PERILS) OF THE GREAT CLOUD MIGRATION

Today's business leaders see opportunity in cloud services. Unfortunately, they also see peril.

According to RightScale, 95 percent of businesses use cloud services in some form. Despite progress in cloud adoption, Gartner's annual cloud adoption survey found that security and privacy concerns loom large in leaders' minds. About two-thirds of surveyed organizations — the same as in past years — point to these issues as their top inhibitors to greater cloud use.

Cloud service providers (CSPs) are understandably excited about the business world's migration to the cloud. They're still grappling, however, with the shared security challenges of such a shift.

In the cloud, data security isn't a simple matter. Consider the interdependencies associated with an insurance company that's reliant on cloud services. It outsources call processing to HealthOps, a software-as-a-service (SaaS) provider. HealthOps, in turn, uses a platform-as-a-service (PaaS) provider to manage software updates and customer configurations. That PaaS provider then partners with an infrastructure-as-a-service (IaaS) company to host its data.

Although the insurer may not be aware, its sensitive information is handled by three separate CSPs. Because the cloud is layered like an onion, the SaaS, PaaS, and IaaS providers must all do their part to safeguard the insurance company's data.

With new breaches announced daily, CSPs need to cooperatively address data security risks and build trust with business leaders. In doing so, the entire industry benefits from accelerated cloud adoption.

DID YOU KNOW?

In the next three years, **83%** of data center traffic will be cloud-based.

The average enterprise uses **1,427 distinct cloud services**. This is a **23.7% increase** from Q4 2015 to Q4 2016.

Of the 20,000 cloud services in use today, only **1 in 10** providers encrypt data at rest.

57% of enterprises have cloud malware, and only **23%** know about it.

A **50% increase** in cloud storage usage increases an enterprise's data breach costs by 46 percent, from **$3.3 million to $5.89 million**.

CSPs: SHARED RESPONSIBILITY STARTS HERE

All CSPs — IaaS, PaaS, and SaaS providers alike — share similar responsibilities in managing the following eight of the Cloud Security Alliance's "Treacherous 12" risks. What's more, taking steps to address each risk can help CSPs fulfill one or more related data security frameworks (see Appendix "Cloud Service Providers and Compliance Mappings" for detailed information).

1. Data Breaches

Data breaches are a part of doing business in a digital world. Prepare for them by updating data flows, conducting risk and privacy assessments, assigning security and privacy responsibilities, and proactively establishing an incident management program. Not only are these best practices in cloud security, but they can also help CSPs serving healthcare companies fulfill HIPAA requirements:

- 164.308(a)(1)(ii)(B) risk management (R)
- 164.308(a)(2) assigned security responsibility
- 164.308(a)(6)(i) security incident procedures

When data is stolen or misused, it doesn't matter who owns that data. Any business with custodial responsibilities for it must communicate the breach to IaaS, PaaS, and client partners. Evolving regulations could impose fines of up to 4 percent of revenue on CSPs found to be negligently responsible for a data breach.

THE TRUE COST OF A BREACH

Medical:
$402
per HIPAA-protected record

Life Sciences:
$301
per record

Financial Services:
$264
per record

Average Across Fields:
$158
per record

Source: 2016 Ponemon Cost of Data Breach Study

CSPs: SHARED RESPONSIBILITY STARTS HERE

2. Malicious Intruders

From international hackers to former employees, unauthorized intruders can destroy infrastructure and steal data. CSPs can limit this threat with access management safeguards such as multifactor authentication, infrastructure segmentation, and automatic anomaly detection. Beyond technical safeguards, CSPs can secure ecosystems through segregation of duties, key rotation policies, vendor SLA management, and production automation.

By following these access management practices, CSPs serving New York-registered financial services firms can help their clients fulfill New York's cybersecurity requirements:

- 500.12 (multifactor authentication)
- 500.07 (access privileges)

The access management protocols described above can also help CSPs in New York and elsewhere meet:

- NIST's identification and authentication (IA) control family
- 27001 A.15 supplier relationships

WHAT ARE NEW YORK'S CYBERSECURITY REQUIREMENTS?

Last September, New York Gov. Andrew Cuomo unveiled the nation's first cybersecurity regulations that call for financial institutions, including banks and insurance companies, to greatly improve cybersecurity protections. The rules, which took effect March 1, serve to further protect consumers' and businesses' sensitive financial data. Among other things, the rules require that affected companies must:

↓

CYBERSECURITY REQUIREMENTS

- Establish a robust cybersecurity program that is fully staffed and funded, managed competently, and regularly reported on to the organization's top governing body.
- Create risk-based standards for technological systems, which must include access controls, data protection, encryption, and frequent penetration testing.
- Institute an incident response plan, including data preservation protocols and prompt reporting to New York's Department of Financial Services.
- Identify and document system deficiencies and remediation plans.
- Undergo annual compliance certification with the Department of Financial Services.

3. Advanced Persistent Threats

APTs can be particularly dangerous for off-guard CSPs. After establishing a foothold in an insecure system, they silently ship data to third-party recipients. Baseline hardening that is consistently applied to address configuration drifts of APTs can help. When other safeguards fail, a business continuity plan is a CSP's best defense.

Ideally, the plan should include a disposable infrastructure that can refresh an environment infiltrated by an APT. Given APTs' "low and slow" nature, disposable infrastructure can almost completely eliminate such threats. Business continuity planning can help CSPs meet SOC 2 2017 A1.0 availability.

In addition, baseline hardening for server and firewall environments can help CSPs address:

- SOC 2 2017 CC6.0 logical access
- PCI requirement 1 firewall configuration

4. Data Loss

Data losses occur for multiple reasons, most notably misaligned client-CSP retention policies. CSPs and their clients can reduce uncertainty by cooperatively establishing data backup plans.

WHAT IS DISPOSABLE INFRASTRUCTURE?

Disposable infrastructure, sometimes referred to as "immutable infrastructure," refers to cloud architecture that has been preserved in case of infrastructural failure. A component of disposable infrastructure uses "golden images" that contain the application's configured code ready for deployment at any time. Servers and code thrown away make way for entirely new servers.

For example, a golden image can be leveraged for disposable infrastructure as a base image of a virtual server that contains the application's configured code. If the infrastructure is compromised, administrators can simply launch a new virtual server from the golden image.

CSPs: SHARED RESPONSIBILITY STARTS HERE

5. Cloud Service Abuses

Malicious actors can commandeer cloud services for illicit activities such as the distributed denial of service attacks or the brute-force breaking of encryption keys. CSPs should assign asset tags across their environments, train employees and threat intelligence tools to spot suspicious network activity, and include critical infrastructure in regular monitoring and asset management plans.

6. Denial of Service

When systems are overly taxed, they may slow to a crawl or simply time out. As with many threats, CSPs can mitigate the damage by creating business continuity plans before a DoS attack.

7. Misconfigured or Vulnerable Shared Technology

When it's unclear who's responsible for shared technology, miscommunications can jeopardize providers' entire systems. Before sharing infrastructure, partners should explain in writing which party will be responsible for configuring, updating, and maintaining it.

AVOID CLOUD SERVICE ABUSE

CSPs should:

Assign asset tags across their environments.

Train employees and threat intelligence tools to spot suspicious network activity.

Include critical infrastructure in regular monitoring and asset management plans.

CSPs: SHARED RESPONSIBILITY STARTS HERE

8. Insufficient Due Diligence

Interdependencies create a range of commercial, financial, legal, and technical risks for CSPs. Before entering a partnership, carefully think through what-if scenarios and implement protective redundancies.

What happens, for example, if an upstream CSP's systems go down? Something as simple as a typo can shut down operations for dependent CSPs. Providers must also pay attention to technical compatibilities. A Windows-based SaaS company, for example, might seek a PaaS partner running Microsoft Azure to be consistent with their environment.

Don't forget about financial and legal risks. If a partnered CSP goes bankrupt, does the contract provide for data retrieval? SaaS providers, in particular, should look at geographic locations where data will be stored. European clients must comply with the General Data Protection Regulation, which prescribes privacy safeguards that U.S. federal and state laws may not, while Chinese cybersecurity statutes require that sensitive data be stored within the nation's bounds.

HOW CSP SYSTEM FAILURES CAN CASCADE

Remember when Amazon Web Services shut down this past March? Services ranging from Netflix to Spotify to Trello (not to mention thousands of smaller sites) that run on the AWS platform slowed or became unavailable to consumers worldwide.

The cause of the shutdown? A single command-line typo made by an engineer debugging a billing service issue.

IAAS, PAAS, AND SAAS PROVIDERS' UNIQUE CLOUD DATA RESPONSIBILITIES

Each CSP has a particular role to play in ensuring cloud data is safely stored, transported, and delivered on the information highway.

IaaS: "The Road"

The IaaS model (e.g., Amazon Web Services, Rackspace, and GoGrid) is like the interstate highways and roads. These CSPs provide the server and network infrastructure upon which other cloud services run.

PaaS: "The Vehicles"

The PaaS model (e.g., Heroku, Google App Engine, and Microsoft Azure) is like the vehicles that carry the precious cargo. These CSPs provide a development framework that enables companies to create and manage their cloud applications without requiring developers to manage back-end databases and servers.

SaaS: "The People and Supplies"

The SaaS model (e.g., NetSuite, Microsoft 365, Workday, Zendesk, and Salesforce) is like the people and shipments that get transported on the roads. These CSPs provide web-hosted applications that the end user generally interacts with via a front-end interface. Their services are sometimes seen as the ultimate reason for the "roads" and the "vehicles."

IAAS, PAAS, AND SAAS PROVIDERS' UNIQUE CLOUD DATA RESPONSIBILITIES

In addition to managing the prior eight threats, IaaS, PaaS, and SaaS providers' model-specific responsibilities for mitigating the following four of the CSA's "Treacherous 12" risks include:

1. Insecure Interfaces and APIs

Weak interfaces and outdated application programming interfaces are common targets for intruders seeking to steal data or disrupt services. By responsibly designing, testing, and deploying APIs, CSPs can improve security while also working to fulfill ISO A.14 and PCI requirement 6.

For **IaaS** providers, managing APIs is typically the client's responsibility, but maintaining underlying infrastructure, including APIs into the hypervisor, remains the CSP's role. IaaS providers should also be aware of virtual machines clients are running on their servers, as well as what efforts clients have made to secure them. All parties should take steps to protect APIs, such as encrypting storage files or attaching hardware security modules (HSMs).

Although all CSPs are responsible for securing their APIs, **PaaS** companies' duties extend even further. Because they're deeply integrated into their clients' environments (such as with code deployment tools), it's essential that these providers educate clients on how to use the platform and the associated tools securely.

In the **SaaS** model, the client might manage the APIs, which should include trusted source validation, or they might share this responsibility with the CSP. Regardless, SaaS providers should secure any APIs that plug into clients' environments according to leading practices such as OWASP standards.

2. Inadequate Identity, Credential, and Access Management

Unauthorized entrants into a system, whether due to compromised credentials or mishandled permissions, can steal data and damage infrastructure. The client should ensure all user accounts use unique IDs and secure authentication practices, but **IaaS** providers must protect the underlying infrastructure with strong authentication.

Compared to the IaaS model, **PaaS** providers retain significant administrative access rights. Still, it's incumbent upon these CSPs to provide credential management tools to clients.

SaaS providers, again, possess greater responsibility here than their IaaS and PaaS peers. In fact, with the notable exception of customer-provisioned user accounts, SaaS companies must manage access to all levels of their applications. Customers' responsibilities include setting complex, unique passwords for each user account and, in some cases, creating user accounts. To help them do so securely, SaaS CSPs should furnish features such as password complexity checkers, user management tools, and multifactor authentication capabilities.

3. System Vulnerabilities

Because the cloud is a shared-resource environment, threats that infiltrate one provider's system can compromise those of partnered CSPs. Any vulnerabilities in a CSP's system inevitably become vulnerabilities in the end user's environment. Identifying and eliminating these vulnerabilities is key to fulfilling standards such as:

- SOC 2 2016 CC6.0 system operations incident management
- ISO 27001 A.12 operations security

While **IaaS** providers often manage monitoring and activity logging for underlying devices and infrastructure, including hypervisors, clients are responsible for monitoring and logging within their own virtual environments. After a breach, IaaS providers might be required to share logs with other CSPs and end customers to reconstruct a chain of events.

In contrast, **PaaS** providers often provide activity monitoring services to clients. While the extent of these services varies widely, what's important is that CSPs and clients explicitly agree on what data will be captured, when it will be shared, how it will be shared, and what parties it will be shared with.

SaaS providers should expect to perform all monitoring and logging within their applications. In some cases, clients are provided application-level logging features such as log on/log off, basic reporting, and account management, which they're responsible for using securely.

4. Account Hijacking

Phishing and fraud are constant concerns for CSPs, particularly because such attacks can slip past first-line network defenses. Account hijackers can eavesdrop on private information, manipulate data, modify transactions, and even launch further cloud attacks.

To keep out hijackers, **IaaS** providers (and, in fact, all models) should employ multifactor login authentication. Again, clients should ensure user accounts use unique IDs, but the CSP must own this responsibility for the underlying infrastructure.

Because **PaaS** providers often retain more administrative rights, their responsibilities in preventing unauthorized account access are even broader. PaaS providers and their clients must explicitly agree upon each party's account-level security responsibilities.

Account hijacking is a particularly complex threat for SaaS providers, which retain ultimate control of accounts at all levels. Given that networks are often convoluted and hijacked accounts can be tough to identify, prevention is the best approach.

To prevent hijacking, **SaaS** companies should implement multifactor authentication, establish public and private subnetworks for secure shell (SSH) access, and segment security groups. They should also establish strong controls over administrative accounts provisioned to partnered CSPs. In the event of a breach, "disposable infrastructure" that returns the environment to its prebreach state can undo the damage from a hijacked account.

BEYOND RISK MANAGEMENT: BUSINESS OPPORTUNITIES FOR SECURITY- AND COMPLIANCE-MINDED CSPs

Too often, cloud security is discussed only in the context of risk reduction. Although this is an important benefit of data security, it's hardly the only one.

1. Strengthen the Brand

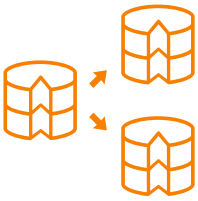
With security and privacy concerns topping the list of cloud customer worries, CSPs that tackle data security vulnerabilities head-on position themselves as secure providers. Such CSPs can provide additional value to their customers by credibly advising them on cloud security.

2. Add Value Through Hands-Off Security

For business leaders, data security is a necessary evil. They know they need it, but they'd rather spend their time serving their own customers. CSPs that know their customers' security responsibilities, including which can be taken on by the CSP, can increase the value of their services.

3. Support System Migrations

Everywhere in business, cybersecurity skills are in short supply. In refining their security protocols, CSPs can learn to migrate data to industry leaders such as AWS and Google. As developers roll out new tools for these platforms, regional CSPs that add data migration services to their roster of offerings powerfully differentiate themselves from peers. CSPs should view this as an opportunity to meet market demand rather than as a cannibalization of their own services.



BEYOND RISK MANAGEMENT: BUSINESS OPPORTUNITIES FOR SECURITY- AND COMPLIANCE-MINDED CSPs

4. Segment Services According to Security Needs

Not every customer needs (or can afford) state-of-the-art cloud security. CSPs that segment their services according to client risk levels can broaden their target market and create customized packages. For instance, a financial services firm may need a more robust credential management system than a weather app startup.

5. Expand Into Consulting Services

Because it's such a niche field, CSPs that master security regulations open doors to consulting opportunities. Customers affected by New York's cybersecurity standards, for example, are required to have a chief information security officer, but they may outsource the role. CSPs that offer CISO consulting services can generate revenue and improve client relationships through a deeper understanding of security needs.

For CSPs, cloud security is no longer about meeting regulatory requirements; it's about answering clients' calls for increased protection against breaches and data loss. It's about moving beyond "tick the boxes" tedium and building trust with old and new customers. It's about leveraging cloud security as a strategic asset.

ABOUT BARR

BARR Advisory is a leading provider of IT governance, risk, and compliance services to some of the fastest-growing cloud service providers (IaaS, PaaS, SaaS) in the country. Its experienced specialists help enterprises of all sizes strengthen their security, meet complicated mandates, and take business operations to the next level.

BARR defines a single standard to meet compliance challenges and then delivers reporting services tailored to each organization's needs and goals. Based in Kansas City, Missouri, BARR has resources in Salt Lake City, New York, Los Angeles, Europe, and Southeast Asia.

CONTACT THE AUTHOR

Brad Thies | Principal
Phone: 913-579-8314
Email: info@barradvisory.com

CONNECT WITH BARR

With BARR, you can expect a partner on your path to security and compliance every step of the way.

OFFICE LOCATIONS

APPENDIX

COMPLIANCE REQUIREMENTS BY MODEL AND SECURITY FRAMEWORK

When it comes to cloud data security, compliance frameworks help CSPs and their customers speak a common language. They enable CSPs to delineate responsibilities for mitigating risks common to cloud ecosystems. By fulfilling one or more frameworks, CSPs gain a powerful way to demonstrate the security of their cloud offerings.

CSPs that have yet to choose a security or compliance framework should select the standard(s) most relevant to them. CSPs with significant business in the healthcare space, for example, might select HITRUST guidelines as a starting point while building a program customized to their unique risks.

CSPs should understand, however, that compliant is not necessarily secure. No compliance standard can completely eliminate security threats.

Still, given the large range of industries that CSPs serve, it's essential that they shape their security programs around one or more applicable standards. Compliant CSPs create a security baseline that enables them to move from a compliance-based approach to a risk-based approach to information security.

COMPLIANCE REQUIREMENTS BY MODEL AND SECURITY FRAMEWORK

	Customer, Shared, or CSP Responsibility				High-Level Compliance Mappings		
SOC 2 2016	**Iaas**	**PaaS**	**SaaS**	**Colo**	**SOC 2 2017**	**Cloud Security Alliance**	**NIST**
CC1.0 - Organization and Management	Shared	Shared	Shared	Shared	CC1.0 - Control Environ.	GRM - Gover. and Risk Mgmt. HRS - Human Resources	AT Awareness & Training PL Planning PS Personnel Security
CC2.0 - Communications	Shared	Shared	Shared	Shared	CC2.0 - Communication and Information	STA - Supply Chain Management, Transparency, and Accountability	PL Planning
CC3.0 - Risk Mgmt, Design & Implem. Controls	Shared	Shared	Shared	Shared	CC3.0 - Risk Assessment CC5.0 - Control Activities CC9.0 - Risk Mitigation	GRM - Governance and Risk Management SEF - Security Incident Mgmt., E-Discovery, & Cloud Forensics	CA Security Assess. & Auth. MA Maintenance MP Media Protection RA Risk Assessment
CC4.0 - Monitoring of Controls	Shared	Shared	Shared	Shared	CC4.0 - Monitoring Activities	AAC - Audit Assurance & Compliance DCS - Datacenter Security	AU Audit & Accountability CA Security Assess. & Auth. SA System & Services Acquis
CC5.0 - Logical Access	Shared	Shared	Shared	Shared	CC6.0 - Logical Access	EKM - Encrypt. & Key Mgmt. AIS - Applic. & Interface Security IAM - Identity & Access Mgmt IVS - Infrast. & Virtualization Security MOS - Mobile Security	AC Access Control IA Identification & Authentication MP Media Protection SC System & Communications Protection
CC5.0 - Physical Access	CSP	CSP	CSP	Colo	CC6.0 - Physical Access	DCS - Data Center Security	MP Media Protection PE Physical & Environ. Protec
CC6.0 - System Ops: Incident Mgmt	CSP	CSP	CSP	Colo	CC7.0 - System Operations	SEF - Security Incid. Mgmt., E-Discov., & Cloud Forensics TVM - Threat & Vulnerability Mgmt.	IR Incident Response
CC7.0 - Change Mgmt: Change Auth. & Imple. Control	Shared	Shared	CSP	Cust.	CC8.0 - Change Management	CCC - Change Control & Configuration Management	CM Configuration Management MA Maintenance SA System & Services Acquis
A1.0 - Availability: BCP / DRP / Capacity	Shared	Shared	CSP	Shared	A1.0 - Availability	BCR - Business Continuity Mgmt. & Operat. Resilience	CP Contingency Planning
PI1.0 - Processing Integrity	Cust.	Cust.	Shared	Cust.	PI1.0 - Processing Integrity	STA - Supply Chain Mgmt, Transp., & Accountability	MP Media Protection SI System & Info. Integrity
C1.0 - Confidentiality	Cust.	Cust.	Shared	Cust.	C1.0 - Confidentiality	EKM - Encrypt. & Key Mgmt DSI - Data Security & Info. Lifecycle Mgmt	MP Media Protection SC System & Comm. Protect.
P1.0 - Privacy	Cust.	Cust.	Shared	Cust.	P1.0 - Privacy	N / A	Privacy Control Catalog

COMPLIANCE REQUIREMENTS BY MODEL AND SECURITY FRAMEWORK

	High-Level Compliance Mappings				
SOC 2 2016	**HITRUST**	**HIPAA**	**ISO 27001**	**PCI**	**N.Y. Cyber Security Req.**
CC1.0 - Organization & Management	0 - Info. Security Mgmt. Program 2.0 - Human Res. Sec. 4.0 - Security Policy 5.0 - Organization of Info. Security	164.308(a)(1)(i) Secur. Mgmt Process 164.308(a)(2) Assigned Secur. Responsibility 164.308(a)(3)(i) Workforce Security 164.308(a)(5)(i) Secur. Awareness & Training	A.5 - Information Security Policies A.6 - Organization of Information Security A.7 - Human Resource Security	PCI Req. 12 - InfoSec Policy	500.02 Cybersecurity Program 500.03 Cybersecurity Policy 500.04 Chief Info. Security Offic. 500.10 Cybersecurity Personnel and Intelligence 500.14 Training and Monitoring
CC2.0 - Communications	9.0 - Communications & Operations Mgmt.	164.308(a)(2) Assigned Security Responsibility 164.308(a)(5)(i) Secur. Awareness & Training BA & Other Contracts	N / A	N / A	500.17 Notices to Superintendent
CC3.0 - Risk Mgmt, Design, & Implem. Controls	3.0 - Risk Mgmt. 7.0 - Asset Mgmt.	164.312(b) Audit Control 164.308(a)(8) Evaluation 164.308(a)(1)(ii)(A) Risk Analysis (R) 164.308(a)(1)(ii)(B) Risk Mgmt (R)	A.8 - Asset Mgmt. A.15 - Supplier Relationships	N / A	500.09 Risk Assessment
CC4.0 - Monitoring of Controls	6.0 - Compliance	164.308(a)(8) Evaluation BA & Other Contracts	A.15 - Supplier Relationships A.18 - Compliance	PCI Req. 10 - Audit & Accountability	500.06 Audit Trail 500.11 Third Party Service Provider Security Policy
CC5.0 - Logical Access	1.0 - Access Control	164.308(a)(3)(i) Workforce Security 164.308(a)(4)(i) Informaiton Access Mgmt. 164.310(c) Workstation Security 164.310(d)(1) Device and Media Control 164.312(a)(1) Access Control 164.312(e)(1) Transmission Security 164.312(d) Person or Entity Authorization 164.308(a)(1)(ii)(D) Info. System Activity Review (R)	A.9 - Access Control A.10 - Cryptography A.13 - Communications Security	PCI Req. 1 - Firewall Config. PCI Req. 2 - System Passwords & Config. PCI Req. 3 - Cardholder Data PCI Req. 4 - Encrypted Trans. PCI Req. 7 - Access Control PCI Req. 8 - Identification & Authentication	00.07 Access Privileges 500.08 Application Security 500.12 Multifactor Authentication 500.15 Encryption of Nonpublic Information
CC5.0 - Physical Access	8.0 - Physical & Environ. Security	164.310(a)(1) Facility Access 164.310(b) Workstation Use	A.11 - Physical & Environ. Security	PCI Req. 9 - Physical Access	N / A
CC6.0 - System Ops: Incident Mgmt.	9.0 - Commun. & Operations Mgmt. 11.0 - Info. Security Incident Mgmt.	164.308(a)(6)(i) Security Incident Procedures 164.312(b) Audit Control 164.312(e)(1) Transmission Security 164.410(a)(1) General Rule 164.410(a)(2) Breaches Treated as Discovered	A.12 -Operations Security A.16 - Info. Security Incident Mgmt.	PCI Req. 5 - Antivirus Protection PCI Requirement 11 - Security Operations	500.05 Penetration Testing & Vulnerability Assessments 500.16 Incident Response Plan 500.17 Notices to Superintendent
CC7.0 - Change Mgmt: Change Auth. & Imple. Control	10.0 - Info. Systems Acquisition, Develop., & Maintenance	N / A	A.14 - System Acquisition, Development, & Maintenance	PCI Req. 6 - Secure Development & Maintenance	N / A
A1.0 - Availability BCP / DRP / Capacity	12.0 - Business Continuity Mgmt.	164.308(a)(7)(i) Contigency Plan	A.17 - Info. Security Aspects of Business Continuity Mgmt.	N / A	N / A
PI1.0 - Processing Integrity	N / A	164.312(c)(1) Integrity	Shared	N / A	N / A
C1.0- Confidentiality	6.0 - Compliance	164.410(b) Timeliness of Notification	A.10 - Cryptography A.13 - Comm. Security A.18 - Compliance	N / A	500.13 Limits on Data Retention 500.15 Encryp. of Nonpublic Info 500.18 Confidentiality
P1.0 - Privacy	13.0 - Privacy Practices	164.410(b) Timeliness of Notification 164.410(c)(1) Content Notification	Reference ISO 27018	N / A	N / A