
*Cobb County...Expect the Best!*

# *INTERNAL AUDIT DEPARTMENT*

## *Report Number: 2022-010*

# *FINAL REPORT – Payment Card Industry (PCI) Readiness Assessment*

## *(Performed by RSM US, LLP[1])*

***October 14, 2022***

***Latona Thomas, CPA, CIA, Director***
***Erica Brooks Peters, CPA, Senior Internal Auditor***

[1] RSM US, LLP is a vendor selected through the County's selection process to perform supplemental internal auditing services. [Source: Cobb County Contract No. 18955, dated April 21, 2020]

# PCI READINESS ASSESSMENT

**Version 1.0**

September 30, 2022


**PREPARED BY:**

**RSM US LLP**
1201 West Peachtree Street Northwest
Suite 800
Atlanta, Georgia 30309
www.rsmus.com

**K.J. Sedjro**
+1 470 283 6767
kj.sedjro@rsmus.com

**SUBMITTED TO:**

**Cobb County Internal Audit Department**
100 Cherokee Street, Suite 250
Marietta, Georgia 30090
www.cobbcounty.org/audit

**Latona Thomas**
+1 770 528 2559
latona.thomas@cobbcounty.org

# EXECUTIVE SUMMARY

Cobb County (or the County) accepts customers' payment cards as a form of payment for staff-related services rendered by the County. In an effort to reduce data breaches that could be used to commit credit card fraud or identity theft, controls need to be in place to protect cardholder data (CHD or credit card data). Because several County departments accept payment cards, Cobb County should do what is required to protect its customers' payment card information. The risk of not doing so can result in a loss of trust, diminished reputation and costs related to fines and penalties. As such, Cobb County must comply with the Payment Card Industry (PCI) Data Security Standard (DSS) Version 3.2.1. This requirement is imposed by the County's acquiring banks and the payment brands (e.g., Visa, Mastercard, AMEX, Discover). Cobb County engaged RSM US LLP (RSM) to conduct a PCI DSS readiness assessment. During May 4–June 24, 2022, an RSM PCI Qualified Security Assessor (QSA) assessed Cobb County using the PCI DSS v3.2.1 to identify weaknesses and create a prioritized road map to meet the compliance requirements. We conducted interviews, reviewed documentation and examined system settings to assess Cobb County's ability to protect cardholder data.

The PCI DSS provides a detailed, 12-requirement structure for securing CHD that is stored, processed and/or transmitted by merchants and other organizations. The PCI Security Standards Council (SSC) has created a prioritized approach that groups the requirements to help organizations understand and prioritize risk reduction and compliance progress. By implementing and following the prioritized guidelines as determined by the QSA, the organization can expedite the process of securing CHD. The prioritized approach provides six security milestones that will help the organization protect against the highest risk factors and escalating threats while developing and maturing their PCI DSS compliance.

We reviewed 24 Cobb County departments[1], of which 21 confirmed that they accept credit card payments. For each of the 21 departments, we performed interviews and document reviews and determined that the County departments accept payment cards using multiple methods, including online, over the phone, via interactive voice response (IVR) and in person. We also noted that Cobb County's department of Information Services provides shared services to all departments. As an internal service provider, the shared services provided by the Information Services department include, but are not limited to, network management and vendor infrastructure, vulnerability management, policy development and the training and awareness program.

A breakdown of payment processes for each department is provided in this report. For each department's payment methods, we reviewed the people, processes and technologies in use against the PCI DSS v3.2.1 controls. According to our analysis, Cobb County, along with each of its departments, has taken the needed steps to mitigate risk by leveraging PCI DSS-compliant third-party vendors for payment acquisition and processing. However, additional action is necessary to ensure that all aspects of Cobb County's payment card environment are PCI DSS-compliant.

[1] For the purposes of this report, departments represent County agencies, departments, divisions, units and elected officials' offices.

## Observation Summary

Our review found that Information Services (as a service provider) and the following 21 departments accept card payments (as merchants) and are required to be PCI DSS-compliant:

| | |
|---|---|
| Alternative Dispute Resolution | Law Library |
| Animal Services | Library |
| Community Development | Parks and Recreation[2] |
| Department of Transportation (DOT)/Transit | Police |
| Drug Lab | Probate Court |
| Fire | Senior Services |
| Government Service Center | State Court |
| Human Resources | Superior Court |
| Information Services—Geographic Information Systems (GIS/Cobb Web) | Tax Commissioner |
| Juvenile Court | Water |
| Magistrate Court | |

The Sustainability, Waste and Beautification department was reviewed in this assessment but transferred their payment acceptance operations to a third-party provider. As such, no further information to be reported.

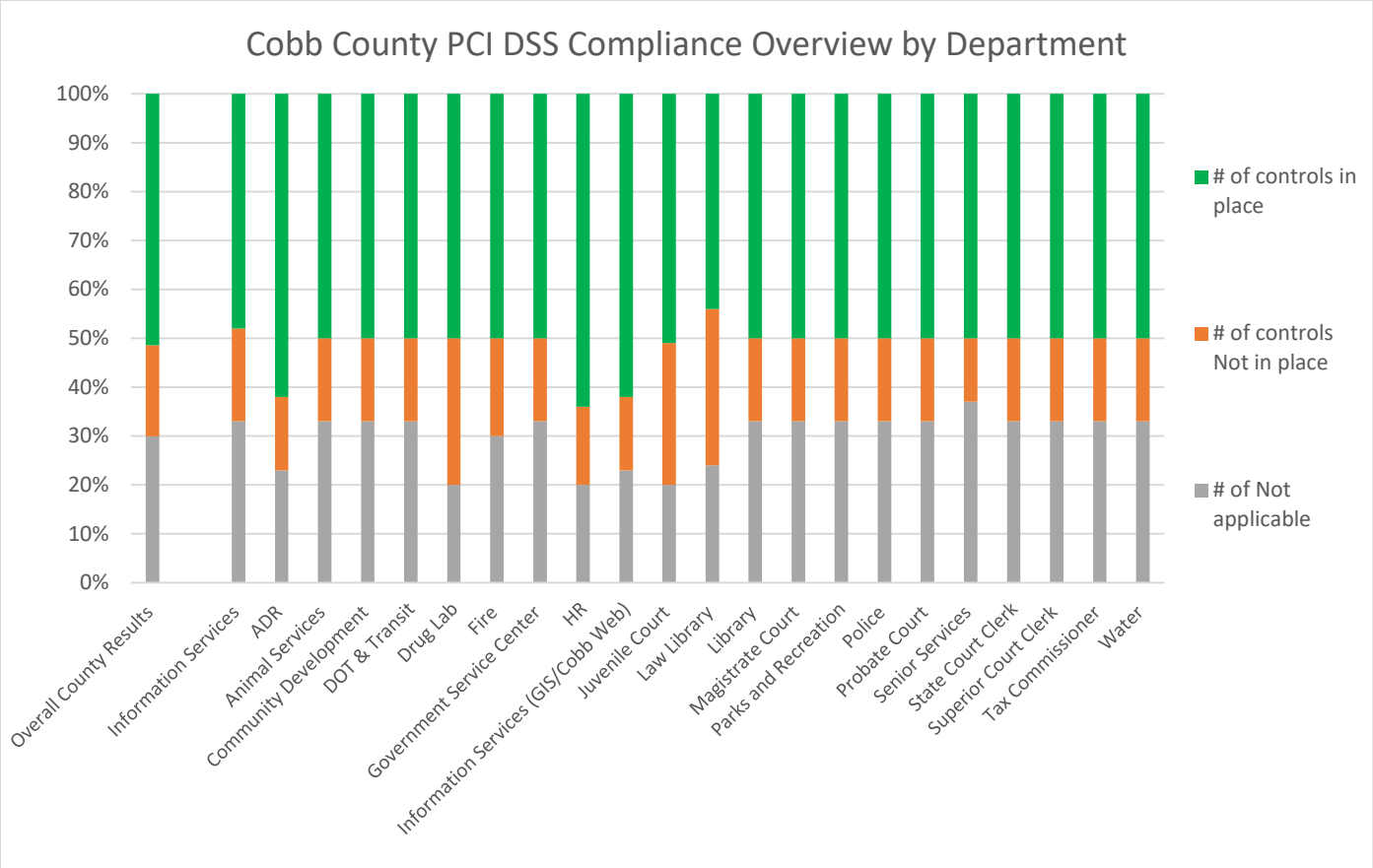
Several departments are responsible for the parking decks; however, the payment operations are administered by a third-party provider. The parking decks were excluded from this assessment, and a supplemental letter report will be issued by the County.

The Finance department does not currently accept credit card payments and is not required to be PCI DSS-compliant.

Although there are some differences in payment methods across departments, most share a common level of effort to achieve and maintain PCI compliance. The departments heavily rely on third-party service providers and the Information Services department (as an internal service provider) for many of the PCI DSS controls that are applicable to their payment processes. A majority of the County's controls deemed not to be in place are the responsibility of the Information Services department. Additionally, during our review we were not able to validate that the third-party service providers used by the departments were all PCI DSS compliant. In each department's section later in this report, we have noted whether the provider is PCI compliant or if the compliance status has not been determined. As a next step for the County, the compliance status of each third-party service provider will need to be confirmed. If a service provider is found to not be PCI DSS compliant, the impacted departments may need to perform additional remediation to achieve compliance.

The Information Services department, as an internal service provider, will need to be integrated within each department's overall compliance effort. Information Services is required to maintain separate controls that address the security services that it provides to the County in support of the departments' payment processes.

[2] The box offices at Mable House Amphitheater, the Civic Center and Jeannie T. Anderson were not reviewed during this assessment. A supplemental letter report will be issued by the County for these locations.




## Strategic Areas of Improvement

### Centralize PCI Compliance Governance

Cobb County should designate a team to manage the PCI compliance program, including the governance over the annual assessments and business-as-usual activities necessary to maintain PCI DSS continual compliance. The team should consult with their acquirer and the payment brands (e.g., Visa, Mastercard, American Express, Discover) to determine the County's and each department's merchant level based on the number of annual payment card transactions. The team should also have the authority to define, enforce and monitor the County's compliance with the PCI requirements for Information Services and the departments that accept credit cards for payment. The team should also oversee the assessment of Information Services as an internal service provider and determine the best approach for assessing each department.

### Network Segmentation

For the departments that have desktops on which credit card data is manually typed in via the keyboard or captured using a credit card swipe device that does not encrypt the data, these desktops, and the network they are on, are not segmented from the rest of the network. This effectively brings most, if not all, of the Cobb County network into scope for the PCI assessment.

Network segmentation (i.e., isolating) of the systems that are part of the credit card processing environment from the remainder of the organization's network is not a PCI DSS requirement. However, segmentation is recommended to reduce the scope and cost of the PCI DSS assessment, the cost and difficulty of implementing and maintaining PCI controls, and the risk to the organization.

The County should review the current configurations of the impacted systems and networks to identify opportunities to isolate the systems and networks or change the business processes or technologies in use to remove the need to segment them.

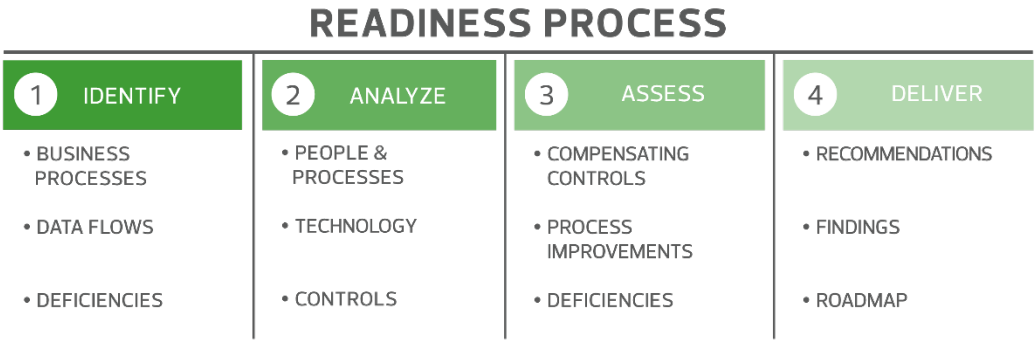
### Standardization

The departments that store, process and transmit credit card data use numerous third-party service providers and payment processors. Cobb County should look for opportunities to consolidate and standardize the services provided by third parties. Standardizing helps minimize the management of the third-party service providers and the complexity of the annual PCI assessment.

Where desktop computers are used to process credit cards via the computer keyboard or captured using credit card swipe devices that do not encrypt data, the County should look at the alternatives available to use secure payment card devices or point-to-point encryption (P2PE) solutions. P2PE solutions usually help remove the computer systems and networks from the scope, since the credit card data that is captured is encrypted when captured by the device and transmitted securely to the payment processor.

# APPENDIX A: PCI READINESS ASSESSMENT METHODOLOGY

Engaging in a PCI readiness assessment actively evaluates an organization's information security controls as they relate to the PCI DSS and identifies the issues that are preventing or impairing full compliance. The process involves interviewing key individuals within the organization, reviewing documentation relevant to the exercise and observing functions while on-site.




**Assessment process**

The PCI readiness assessment performed for Cobb County reviewed security measures currently in place within the organization as they relate to the security controls in their infrastructure, according to the PCI DSS. It is important to note that PCI DSS compliance is an all-or-nothing proposition; there is no partial compliance with regard to PCI. The PCI DSS groups controls into the following 12 requirements:

| Requirement Areas | |
|---|---|
| Requirement 1—Firewalls/Routers/Switches | Requirement 7—Access Restrictions |
| Requirement 2—Default Settings And Baseline Configurations | Requirement 8—Accountability |
| Requirement 3—Protecting Data At Rest | Requirement 9—Physical Security |
| Requirement 4—Protecting Data In Motion | Requirement 10—Logging |
| Requirement 5—Antivirus | Requirement 11—Scanning |
| Requirement 6—Vulnerability Management | Requirement 12—Policies And Personnel |

The PCI readiness assessment serves the following purposes:

- Identify your organization's SAQ level and the associated compliance requirements.
- Provide an independent verification that ensures that the current infrastructure and applications meet the organization's security expectations and compliance requirements.
- Reduce the organization's IT security costs and provide a better return on security investment by identifying and resolving vulnerabilities and weaknesses.
- Adopt best practices by conforming to legal and industry regulations.

COBB COUNTY MANAGER'S OFFICE
100 Cherokee Street, Suite 300
Marietta, GA 30090-7000
Phone: (770) 528-2600 Fax: (770) 528-2606
jackie.mcmorris@cobbcounty.org

Jackie R. McMorris, EdD
*County Manager*

DATE: October 12, 2022

TO: Latona Thomas, CPA, CIA, Internal Audit Director

FROM: Dr. Jackie McMorris, County Manager

SUBJECT: Audit Response – PCI Readiness Assessment

Several recommendations were made and my response to those recommendations are below.

## Recommendations

The County Manager should:

**Recommendation 1:** Designate a team to manage the PCI compliance program, including the governance over the annual assessments and business-as-usual activities necessary to maintain PCI DSS continual compliance. The team should consult with their acquirer and the payment brands to determine the County's and each department's merchant level based on the number of annual payment card transactions. The team should also have the authority to define, enforce and monitor the County's compliance with the PCI requirements for Information Services and the departments that accept credit cards for payment. The team should also oversee the assessment of Information Services as an internal service provider and determine the best approach for assessing each department.

**Response:**

Concur. A team of appropriate staff have been identified to address this recommendation. Over the coming months, they will work on administrative tasks to ensure compliance.

**Recommendation 2:** Designate the team in Recommendation 1 to review the current configurations of the impacted systems and networks to identify opportunities to isolate the systems and networks or change the business processes or technologies in use to remove the need to segment them.

**Response:**

Concur. The designated team mentioned in recommendation 1 will also address this particular issue.

**Recommendation 3:** Designate the team in Recommendation 1 to look for opportunities to consolidate and standardize the services provided by third parties. Standardizing helps minimize the management of the third-party service providers and the complexity of the annual PCI assessment. The team should also look at the alternatives available to use secure payment card devices or point-to-point encryption (P2PE) solutions.

**Response:**

Concur.