

Appendix D

Appendix D-1	<i>Illustrative Management Assertion and Service Auditor's Report for a Type 2 Examination (Carved-Out Controls of a Subservice Organization and Complementary Subservice Organization and Complementary User Entity Controls)</i>
Appendix D-2	<i>Illustrative Service Organization and Subservice Organization Management Assertions and Service Auditor's Report for a Type 2 Examination (Subservice Organization Presented Using the Inclusive Method and Complementary User Entity Controls)</i>
Appendix D-3	<i>Illustrative Service Auditor's Report for a Type 2 Examination in Which the Service Auditor Disclaims an Opinion Because of a Scope Limitation</i>
Appendix D-4	<i>Illustrative Type 2 Report (Including Management's Assertion, Service Auditor's Report, and the Description of the System)</i>

Appendix D-1

Illustrative Management Assertion and Service Auditor's Report for a Type 2 Examination (Carved-Out Controls of a Subservice Organization and Complementary Subservice Organization and Complementary User Entity Controls)

This appendix is nonauthoritative and is included for informational purposes only.

*In the following illustrative management assertion and service auditor's report, XYZ Service Organization has engaged the service auditor to examine and report on the description of the service organization's medical claims processing system and the suitability of design and operating effectiveness of controls relevant to security, availability, processing integrity, confidentiality, and privacy to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. The example assumes that XYZ Service Organization outsources certain aspects of its system to a subservice organization and has elected to use the carve-out method for the subservice organization. In addition, complementary user entity and complementary subservice organization controls are required for XYZ Service Organization to achieve certain service commitments and system requirements based on the applicable trust services criteria. Language that has been added to the illustrative management assertion and to the service auditor's report to reflect the use of the carve-out method and the need for complementary user entity controls and complementary subservice organization controls is shown in **boldface italics**.*

Illustrative Assertion by Service Organization Management

[XYZ Service Organization's Letterhead]

Assertion of XYZ Service Organization Management

We have prepared the accompanying description of XYZ Service Organization's (XYZ's) medical claims processing system titled "XYZ Service Organization's Description of its Medical Claims Processing System" throughout the period January 1, 20XX, to December 31, 20XX, (description) based on the criteria for a description of a service organization's system in [DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2[®] Report](#) (AICPA, *Description Criteria*) (description criteria).^{fn 1} The description is intended to provide report users with information about the medical claims processing system that may be useful when assessing the risks arising from interactions with XYZ's system, particularly information about system controls that XYZ has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in [TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy](#), (AICPA, *Trust Services Criteria*).^{fn 2}

^{fn 1} The description criteria presented in this document (2018 description criteria) have been designed to be used in conjunction with the 2017 trust services criteria set forth in [TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy](#), in a SOC 2[®] report. The 2018 description criteria are codified as [DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2[®] Report](#), in AICPA *Description Criteria*. The description criteria included in paragraphs 1.26–.27 of the 2015 AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2[®])* (2015 description criteria) are codified as [DC section 200A, 2015 Description Criteria for a Description of a Service Organization's System in a SOC 2[®] Report](#).

When preparing a description of the service organization's system as of December 15, 2018, or prior (type 1 examination) or a description for periods ending as of December 15, 2018, or prior (type 2 examination), either the 2018 description criteria or 2015 description criteria may be used. (To ensure that the 2015 description criteria are available to report users, such criteria will remain in [DC section 200A](#) through December 31, 2019.) During this transition period, management should identify in the description whether the 2018 description criteria or the 2015 description criteria were used.

When preparing a description of the service organization's system as of or after December 16, 2018, (type 1 examination) or a description of the system for periods ending as of or after that date (type 2 examination), the 2018 description criteria should be used.

^{fn 2} The extant trust services criteria (2016 trust services criteria) are codified in [TSP section 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy \(2016\)](#), and will be available through December 15, 2018. After that date, the 2016 trust services criteria will be considered superseded. Until that date, service auditors should distinguish in their reports whether the 2016 or the 2017 trust services criteria have been used as the evaluation criteria.

In addition, the AICPA will continue to make available the 2014 trust services criteria codified in [TSP section 100A-1, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy \(2014\)](#), until March 31, 2018, to ensure they remain available to report

XYZ uses a subservice organization to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at XYZ, to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria. The description presents XYZ's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of XYZ's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at XYZ, to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria. The description presents XYZ's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of XYZ's controls.

We confirm, to the best of our knowledge and belief, that

- a. the description presents XYZ's medical claims processing system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, ***and if the subservice organization and user entities applied the complementary controls assumed in the design of XYZ's controls throughout that period.***
- c. the controls stated in the description operated effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria, ***if complementary subservice organization controls and complementary user entity controls assumed in the design of XYZ's controls operated effectively throughout that period.***

Illustrative Independent Service Auditor's Type 2 Report

Independent Service Auditor's Report^{fn 3}

To: XYZ Service Organization

Scope

users. Those criteria were considered superseded for service auditor's reports for periods ended on or after December 15, 2016.

^{fn 3} The report may also be titled "Report of Independent Service Auditors."

We have examined XYZ Service Organization's (XYZ's) accompanying description of its medical claims processing system titled "XYZ Service Organization's Description of its Medical Claims Processing System" throughout the period January 1, 20XX, to December 31, 20XX,^{fn 4} (description) based on the criteria for a description of a service organization's system in [DC section 200](#), *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2[®] Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in [TSP section 100](#), *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).^{fn 5}

XYZ uses a subservice organization to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at XYZ, to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria. The description presents XYZ's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of XYZ's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at XYZ, to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria. The description presents XYZ's controls, the applicable trust services criteria, and the complementary user entity controls assumed in

^{fn 4} The title of the description of the service organization's system in the service auditor's report should be the same as the title used by service organization management in its description of the service organization's system.

^{fn 5} A statement such as the following is added to the service auditor's report when information that is not covered by the report is included in the description of the service organization's system:

The information included in section X, "Other Information Provided by XYZ Service Organization That Is Not Covered by the Service Auditor's Report," is presented by XYZ management to provide additional information and is not a part of XYZ's description. Information about XYZ's [*describe the nature of the information, for example, planned system changes*] has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of controls to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

the design of XYZ's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

XYZ is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that XYZ's service commitments and system requirements were achieved. XYZ has provided the accompanying assertion titled "Assertion of XYZ Service Organization Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. XYZ is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in section XX.

Opinion

In our opinion, in all material respects,

a. the description presents XYZ's medical claims processing system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period **and if the subservice organization and user entities applied the complementary controls assumed in the design of XYZ's controls throughout that period.**

c. the controls stated in the description operated effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria, **if complementary subservice organization controls and complementary user entity controls assumed in the design of XYZ's controls operated effectively throughout that period.**

Restricted Use

This report, including the description of tests of controls and results thereof in section XX, is intended solely for the information and use of XYZ, user entities of XYZ's medical claims processing system during some or all of the period January 1, 20XX, to December 31, 20XX, business partners of XYZ subject to risks arising from interactions with the medical claims processing system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- ***Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements***
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

[Service auditor's signature]

[Service auditor's city and state]

[Date of the service auditor's report]

Appendix D-2

Illustrative Service Organization and Subservice Organization Management Assertions and Service Auditor's Report for a Type 2 Examination (Subservice Organization Presented Using the Inclusive Method and Complementary User Entity Controls)

This appendix is nonauthoritative and is included for informational purposes only.

In the following illustrative management assertions and service auditor's report, XYZ Service Organization has engaged the service auditor to examine and report on the description of the service organization's medical claims processing system and its controls relevant to security, availability, processing integrity, confidentiality, and privacy to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. The example assumes that XYZ Service Organization outsources certain aspects of its system to a subservice organization and has elected to use the inclusive method for the subservice organization. In addition, it assumes that service organization management has designed the controls that it expects the subservice organization to implement and operate. The example also assumes that complementary user entity controls are necessary to provide reasonable assurance that XYZ's service

*commitments and system requirements are achieved based on the applicable trust services criteria. Language that has been added to the illustrative service organization management assertion and to the service auditor's report to reflect the use of the inclusive method and the need for complementary user entity controls is shown in **boldface italics**.*

Illustrative Assertion by Service Organization Management

[XYZ Service Organization's Letterhead]

Assertion of XYZ Service Organization Management

We have prepared the accompanying description of XYZ Service Organization's (XYZ's) medical claims processing system titled "XYZ Service Organization's Description of its Medical Claims Processing System" throughout the period January 1, 20XX, to December 31, 20XX, (description) based on the criteria for a description of a service organization's system in [DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2[®] Report](#) (AICPA, Description Criteria), (description criteria).^{fn 1} The description is intended to provide report users with information about the medical claims processing system that may be useful when assessing the risks arising from interactions with XYZ's system, particularly information about system controls that XYZ has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in [TSP section 100, 2017 Trust](#)

^{fn 1} The description criteria presented in this document (2018 description criteria) have been designed to be used in conjunction with the 2017 trust services criteria set forth in [TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy](#), in a SOC 2[®] report. The 2018 description criteria are codified as [DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2[®] Report](#), in AICPA Description Criteria. The description criteria included in paragraphs 1.26–.27 of the 2015 AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2[®])* (2015 description criteria) are codified as [DC section 200A, 2015 Description Criteria for a Description of a Service Organization's System in a SOC 2[®] Report](#).

When preparing a description of the service organization's system as of December 15, 2018, or prior (type 1 examination) or a description for periods ending as of December 15, 2018, or prior (type 2 examination), either the 2018 description criteria or 2015 description criteria may be used. (To ensure that the 2015 description criteria are available to report users, such criteria will remain in [DC section 200A](#) through December 31, 2019.) During this transition period, management should identify in the description whether the 2018 description criteria or the 2015 description criteria were used.

When preparing a description of the service organization's system as of or after December 16, 2018, (type 1 examination) or a description of the system for periods ending as of or after that date (type 2 examination), the 2018 description criteria should be used.

Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).^{fn 2}

XYZ uses ABC Subservice Organization (ABC) to provide application maintenance and support services. XYZ's description includes a description of ABC's application maintenance and support services used by XYZ to process transactions for user entities and business partners, including the controls of XYZ and the controls designed by XYZ and operated by ABC that are necessary for XYZ to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria. ABC's assertion is presented on page XX in section YY.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at XYZ, to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria. The description presents XYZ's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of XYZ's controls.

We confirm, to the best of our knowledge and belief, that

- a. the description presents XYZ's medical claims processing system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria.
- b. the controls stated in the description, including the controls designed by XYZ and operated by ABC, were suitably designed throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, ***and if user entities applied the complementary controls assumed in the design of XYZ's controls throughout that period.***
- c. the controls stated in the description, including the controls designed by XYZ and operated by ABC, operated effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based

^{fn 2} The extant trust services criteria (2016 trust services criteria) are codified in [TSP section 100A](#), *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)*, and will be available through December 15, 2018. After that date, the 2016 trust services criteria will be considered superseded. Until that date, service auditors should distinguish in their reports whether the 2016 or the 2017 trust services criteria have been used as the evaluation criteria.

In addition, the AICPA will continue to make available the 2014 trust services criteria codified in [TSP section 100A-1](#), *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2014)*, until March 31, 2018, to ensure they remain available to report users. Those criteria were considered superseded for service auditor's reports for periods ended on or after December 15, 2016.

on the applicable trust services criteria, ***if complementary user entity controls assumed in the design of XYZ's controls operated effectively throughout that period.***

Illustrative Assertion by Subservice Organization Management

[ABC Subservice Organization's Letterhead]

Assertion of ABC Subservice Organization Management

ABC Subservice Organization (ABC) provides application maintenance and support services to XYZ Service Organization (XYZ). The services provided by ABC are part of XYZ's medical claims processing system. We have prepared the portion of the accompanying description of XYZ Service Organization's medical claims processing system titled "XYZ Service Organization's Description of its Medical Claims Processing System" throughout the period January 1, 20XX, to December 31, 20XX, (description) disclosing ABC's application maintenance and support services provided to XYZ based on the criteria for a description of a service organization's system in [DC section 200](#), *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2[®] Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about XYZ's medical claims processing system that may be useful when assessing the risks arising from interactions with XYZ's system, particularly information about system controls that XYZ has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in [TSP section 100](#), *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

We confirm, to the best of our knowledge and belief, that

- a. the description presents ABC's application maintenance and support services made available to XYZ throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria.
- b. ABC's controls stated in the description, which were designed by XYZ, operated as described throughout the period January 1, 20XX, to December 31, 20XX, based on the applicable trust services criteria.

Illustrative Independent Service Auditor's Type 2 Report

Independent Service Auditor's Report^{fn 3}

To: XYZ Service Organization

Scope

We have examined XYZ Service Organization's (XYZ's) accompanying description of its medical claims processing system, ***including application maintenance and support services provided by and controls***

^{fn 3} The report may also be titled "Report of Independent Service Auditors."

operated by ABC Subservice Organization (ABC), titled "XYZ Service Organization's Description of its Medical Claims Processing System" throughout the period January 1, 20XX, to December 31, 20XX, (description) based on the criteria for a description of a service organization's system in [DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report](#) (AICPA, Description Criteria), (description criteria) and the suitability of the design and operating effectiveness of XYZ's controls, ***including the controls designed by XYZ and operated by ABC,*** stated in the description throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in [TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy](#) (AICPA, Trust Services Criteria).

ABC is an independent subservice organization providing application maintenance and support services to XYZ. The description includes those elements of the application maintenance and support services provided to XYZ and the controls designed by XYZ and operated by ABC that are necessary for XYZ to achieve its service commitments and system requirements based on the applicable trust services criteria.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at XYZ, to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria. The description presents XYZ's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of XYZ's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

XYZ is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that XYZ's service commitments and system requirements were achieved. XYZ has provided the accompanying assertion titled "Assertion of XYZ Service Organization Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. XYZ is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Subservice Organization's Responsibilities

ABC has provided the accompanying assertion titled "Assertion of ABC Subservice Organization Management," (ABC assertion) about the description and the controls stated therein. ABC is responsible for preparing the portion of the description related to the application maintenance and support services provided to XYZ and the ABC assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; and implementing, operating, and documenting controls designed by XYZ, which enable XYZ to achieve its service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in section XX.

Opinion

In our opinion, in all material respects,

- a. the description presents XYZ's medical claims processing system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria.
- b. the controls stated in the description, including the controls designed by XYZ and operated by ABC, were suitably designed throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period **and if the user entities applied the complementary controls assumed in the design of XYZ's controls throughout that period.**
- c. the controls stated in the description including the controls designed by XYZ and operated by ABC, operated effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria, **if complimentary user entity controls assumed in the design of XYZ's controls operated effectively throughout that period.**

Restricted Use

This report, including the description of tests of controls and results thereof in section XX, is intended solely for the information and use of XYZ, user entities of XYZ's medical claims processing system during some or all of the period January 1, 20XX, to December 31, 20XX, business partners of XYZ subject to risks arising from interactions with the medical claims processing system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations

- ***Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements***
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

[Service auditor's signature]

[Service auditor's city and state]

[Date of the service auditor's report]

Appendix D-3

Illustrative Service Auditor's Report for a Type 2 Examination in Which the Service Auditor Disclaims an Opinion Because of a Scope Limitation

This appendix is nonauthoritative and is included for informational purposes only.

In the following illustrative service auditor's report, XYZ Service Organization has engaged the service auditor to examine and report on the description of the service organization's medical claims processing system and the controls relevant to security, availability, processing integrity, confidentiality, and privacy, which XYZ designed, implements, and operates to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. The example assumes that XYZ Service Organization management refused to provide written representations at the end of the examination. Because of that limitation on the scope of the engagement, the service auditor decided to disclaim an opinion about whether the description presents XYZ Service Organization's medical claims processing system that was designed and implemented in accordance with the description criteria and about whether the controls included in the description were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Illustrative Independent Service Auditor's Type 2 Report

Independent Service Auditor's Report^{fn 1}

To: XYZ Service Organization

^{fn 1} The report may also be titled "Report of Independent Service Auditors."

We were engaged to examine XYZ Service Organization's (XYZ's) accompanying description of its medical claims processing system titled "XYZ Service Organization's Description of its Medical Claims Processing System" throughout the period January 1, 20XX, to December 31, 20XX, (description) based on the criteria for a description of a service organization's system in [DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2° Report](#) (AICPA, Description Criteria), (description criteria)^{fn 2} and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in [TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy](#) (AICPA, Trust Services Criteria).^{fn 3}

^{fn 2} The description criteria presented in this document (2018 description criteria) have been designed to be used in conjunction with the 2017 trust services criteria set forth in [TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy](#), in a SOC 2° report. The 2018 description criteria are codified as [DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2° Report](#), in AICPA Description Criteria. The description criteria included in paragraphs 1.26–.27 of the 2015 AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2°)* (2015 description criteria) are codified as [DC section 200A, 2015 Description Criteria for a Description of a Service Organization's System in a SOC 2° Report](#).

When preparing a description of the service organization's system as of December 15, 2018, or prior (type 1 examination) or a description for periods ending as of December 15, 2018, or prior (type 2 examination), either the 2018 description criteria or 2015 description criteria may be used. (To ensure that the 2015 description criteria are available to report users, such criteria will remain in [DC section 200A](#) through December 31, 2019.) During this transition period, management should identify in the description whether the 2018 description criteria or the 2015 description criteria were used.

When preparing a description of the service organization's system as of or after December 16, 2018, (type 1 examination) or a description of the system for periods ending as of or after that date (type 2 examination), the 2018 description criteria should be used.

^{fn 3} The extant trust services criteria (2016 trust services criteria) are codified in [TSP section 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy \(2016\)](#), and will be available through December 15, 2018. After that date, the 2016 trust services criteria will be considered superseded. Until that date, service auditors should distinguish in their reports whether the 2016 or the 2017 trust services criteria have been used as the evaluation criteria.

In addition, the AICPA will continue to make available the 2014 trust services criteria codified in [TSP section 100A-1, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy \(2014\)](#), until March 31, 2018, to ensure they remain available to report

XYZ is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that XYZ's service commitments and system requirements were achieved. XYZ has provided the accompanying assertion titled "Assertion of XYZ Service Organization Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. XYZ is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria. Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants.

Attestation standards established by the American Institute of Certified Public Accountants require that we request certain written representations from management, including a representation that all relevant matters are reflected in the evaluation of the description of its medical claims processing system and the suitability of design and operating effectiveness of controls within the system. We requested that management provide us with such a representation, but management refused to do so.

Because of the limitation on the scope of our examination discussed in the preceding paragraph, the scope of our work was not sufficient to enable us to express, and we do not express, an opinion on whether XYZ's description of its medical claims processing system presents the system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria, or on whether the controls stated therein were suitability designed and operating effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria, in all material respects.

Appendix D-4

Illustrative Type 2 Report (Including Management's Assertion, Service Auditor's Report, and the Description of the System)

This appendix is nonauthoritative and is included for informational purposes only.

Although this guide specifies the components of a SOC 2[®] report and the information to be included in each component, it is not specific about the format for SOC 2[®] reports. Service organizations and service auditors may organize and present the required information in a variety of formats. The format of the illustrative type 2 report presented in this appendix is not meant to be prescriptive but, rather, illustrative. The illustrative report contains all the components of a service auditor's type 2 report;

users. Those criteria were considered superseded for service auditor's reports for periods ended on or after December 15, 2016.

however, for brevity, it does not include everything that might be described in a type 2 report. Ellipses (...) or notes to readers indicate places where detail has been omitted.

The trust services categories being reported on, the controls specified by the service organization, and the tests performed by the service auditor in this appendix are presented for illustrative purposes only. They are not intended to represent the categories that would be addressed in every type 2 engagement or the controls or tests of controls that would be appropriate for all service organizations. The trust services categories being reported on, the controls a service organization would include in its description, and the tests of controls a service auditor would perform for a specific type 2 examination will vary based on the specific facts and circumstances of the engagement.

In the following illustrative type 2 report, XYZ Service Organization has engaged the service auditor to examine and report on the description of the service organization's transportation management system and its controls relevant to security to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. The example assumes that XYZ Service Organization management has included information in [section 5](#), "Other Information Provided by XYZ Service Organization That Is Not Covered by the Service Auditor's Report," which is not a part of the description or the service auditor's examination.

Report on XYZ Service Organization's Description of Its Transportation Management System and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security Throughout the Period January 1, 20X1, to December 31, 20X1

CONTENTS

[Section 1](#)—Assertion of XYZ Service Organization Management

[Section 2](#)—Independent Service Auditor's Report

[Section 3](#)—XYZ Service Organization's Description of Its Transportation Management System

Services Provided

Principal Service Commitments and System Requirements

Components of the System Used to Provide the Services

Infrastructure

Software

People

Data

Processes and Procedures

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

Control Environment

Management Philosophy
Security Management
Security Policies
Personnel Security
Physical Security and Environmental Controls
Change Management
System Monitoring
Problem Management
Data Backup and Recovery
System Account Management
Risk Assessment Process
Information and Communication Systems
Monitoring Controls
Changes to the System During the Period

[Section 4](#)—Trust Services Category, Criteria, Related Controls, and Tests of Controls

Applicable Trust Services Criteria Relevant to Security

[Section 5](#)—Other Information Provided by XYZ Service Organization That Is Not Covered by the Service Auditor's Report

Section 1—Assertion of XYZ Service Organization Management

Illustrative Assertion by Service Organization Management

[XYZ Service Organization's Letterhead]

Assertion of XYZ Service Organization Management

We have prepared the accompanying description in [section 3](#) titled "XYZ Service Organization's Description of Its Transportation Management System" throughout the period January 1, 20XX, to December 31, 20XX, (description), based on the criteria for a description of a service organization's system in [DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2° Report](#) (AICPA, Description Criteria), (description criteria).^{fn 1} The description is intended to

^{fn 1} The description criteria presented in this document (2018 description criteria) have been designed to be used in conjunction with the 2017 trust services criteria set forth in [TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy](#), in a SOC 2° report. The 2018 description criteria are codified as [DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2° Report](#), in AICPA Description Criteria. The

provide report users with information about the transportation management system that may be useful when assessing the risks arising from interactions with XYZ Service Organization's (XYZ's) system, particularly information about system controls that XYZ has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in [TSP section 100](#), *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).^{fn 2}

We confirm, to the best of our knowledge and belief, that

- a. the description presents XYZ's transportation management system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and

description criteria included in paragraphs 1.26–.27 of the 2015 AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (2015 description criteria) are codified as [DC section 200A](#), *2015 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*.

When preparing a description of the service organization's system as of December 15, 2018, or prior (type 1 examination) or a description for periods ending as of December 15, 2018, or prior (type 2 examination), either the 2018 description criteria or 2015 description criteria may be used. (To ensure that the 2015 description criteria are available to report users, such criteria will remain in [DC section 200A](#) through December 31, 2019.) During this transition period, management should identify in the description whether the 2018 description criteria or the 2015 description criteria were used.

When preparing a description of the service organization's system as of or after December 16, 2018, (type 1 examination) or a description of the system for periods ending as of or after that date (type 2 examination), the 2018 description criteria should be used.

^{fn 2} The extant trust services criteria (2016 trust services criteria) are codified in [TSP section 100A](#), *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)*, and will be available through December 15, 2018. After that date, the 2016 trust services criteria will be considered superseded. Until that date, service auditors should distinguish in their reports whether the 2016 or the 2017 trust services criteria have been used as the evaluation criteria.

In addition, the AICPA will continue to make available the 2014 trust services criteria codified in [TSP section 100A-1](#), *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2014)*, until March 31, 2018, to ensure they remain available to report users. Those criteria were considered superseded for service auditor's reports for periods ended on or after December 15, 2016.

system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period.

c. the controls stated in the description operated effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria.

Section 2—Independent Service Auditor's Report

Independent Service Auditor's Report^{fn 3}

To: XYZ Service Organization

Scope

We have examined XYZ Service Organization's (XYZ's) accompanying description in [section 3](#) titled "XYZ Service Organization's Description of its Transportation Management System" throughout the period January 1, 20XX, to December 31, 20XX, (description)^{fn 4} based on the criteria for a description of a service organization's system in [DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report \(AICPA, Description Criteria\)](#), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in [TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy \(AICPA, Trust Services Criteria\)](#).

The information included in [section 5](#), "Other Information Provided by XYZ Service Organization That Is Not Covered by the Service Auditor's Report," is presented by XYZ management to provide additional information and is not a part of the description. Information about XYZ's [*describe the nature of the information, for example, planned system changes*] has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve XYZ's service commitments and system requirements based on the applicable trust services criteria.

Service Organization's Responsibilities

XYZ is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that XYZ's service commitments and system requirements were achieved. In [section 1](#), XYZ has provided its

^{fn 3} The report may also be titled "Report of Independent Service Auditors."

^{fn 4} The title of the description of the service organization's system in the service auditor's report should be the same as the title used by service organization management in its description of the service organization's system.

assertion titled "Assertion of XYZ Service Organization Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. XYZ is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in [section 4](#), "Trust Services Security Criteria, Related Controls, and Tests of Controls," of this report in columns 2, 3, and 4, respectively.

Opinion

In our opinion, in all material respects,

- a. the description presents XYZ's transportation management system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period.
- c. the controls stated in the description operated effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria.

Restricted Use

This report, including the description of tests of controls and results thereof in [section 4](#), is intended solely for the information and use of XYZ, user entities of XYZ's transportation management system during some or all of the period January 1, 20XX, to December 31, 20XX, business partners of XYZ subject to risks arising from interactions with the transportation management system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties

- Internal control and its limitations
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

[Service auditor's signature]

[Service auditor's city and state]

[Date of the service auditor's report]

Section 3—XYZ Service Organization's Description of Its Transportation Management System

Note to Readers: *The following system description is for illustrative purposes only and is not meant to be prescriptive. For brevity, the illustration does not include everything that might be described in the description of the service organization's system. Ellipses (...) or notes to readers indicate places where detail has been omitted from the illustration.*

Services Provided

XYZ Service Organization (XYZ) provides medical transportation (MT) services throughout the United States. The Company was founded in 19XX to provide MT services to Medicaid recipients.

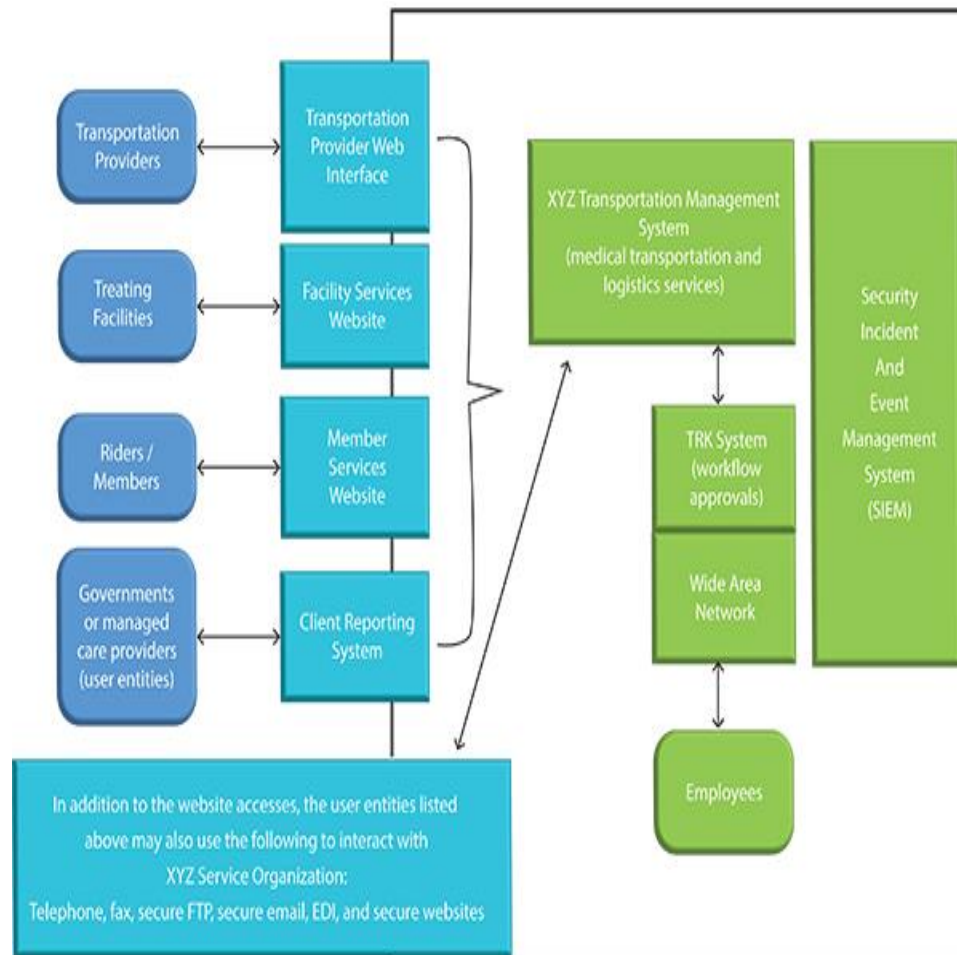
XYZ's core application, Transportation Management System (TMS), is a multiuser, transaction-based application suite that enables the processing and delivery of transportation and logistics services. The TMS enables processing of the following tasks related to MT trips:

- Capturing data for transportation providers, governments, and managed care providers (user entities), treating facilities, and riders
- Determining rider eligibility
- Providing gate keeping and ride authorization
- Managing complaints and verifying compliance with transportation agreements
- Managing transportation providers
- Reconciling billing to completed rides
- Providing operational, management, and ad hoc reports
- Providing data reporting in a variety of formats

Trips are tracked through the order cycle, from initial ride assignment to completion or reassignment of the ride, and by payments. Transportation providers send XYZ daily trip information, including information about trips completed or cancelled (or no-shows) and weekly driver logs, which are entered

into the TMS. System-generated reports provide supporting documentation for trips, including date, transportation provider, rider, and actual trip via a unique job number.

Information is shared with user entities by telephone, fax, secure electronic exchange (FTP [file transfer protocol], email, EDI [electronic data interchange]), and secured websites.



Principal Service Commitments and System Requirements

XYZ designs its processes and procedures related to TMS to meet its objectives for its MT services. Those objectives are based on the service commitments that XYZ makes to user entities, the laws and regulations that govern the provision of MT services, and the financial, operational, and compliance requirements that XYZ has established for the services. The MT services of XYZ are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which XYZ operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the TMS that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit

XYZ establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in XYZ's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the TMS.

Components of the System Used to Provide the Services

Infrastructure

The TMS runs on Microsoft Windows file servers using a wide area network.

Employees access the application either through their desktop on company-supplied computers or through a Citrix Access Gateway. Data communications between offices are encrypted with Cisco virtual private networking (VPN) technology using Advanced Encryption Standard 256-bit encryption to protect data and intra-company communications.

The TMS uses the IBM DB2 relational database management system. These database servers and file servers are housed in XYZ's secured network operations centers (NOCs).

Software

The TMS is a Microsoft Windows client-server application developed and maintained by XYZ's in-house software engineering group. The software engineering group enhances and maintains the TMS to provide service for the company's transportation providers, governments and managed care providers (user entities), treating facilities, and riders. XYZ's software is not sold on the open market.

The TMS tracks information in real time. The information is immediately stored in the database and is accessible for daily operations, service authorization, trip scheduling, provider reimbursement, agency monitoring, and report generation. The information can be retrieved, reviewed, and reported as needed to create the history of approvals and denials for any rider. Information can be retrieved by rider identification number, rider name, trip date, facility attended, and transportation provider.

External websites are supplied to supplement XYZ's ability to communicate and exchange information with transportation providers, governments and managed care providers (user entities), treating facilities, and riders. Each website targets a specific audience and is designed to address their business needs. These include a site for the transportation providers, governments and managed care providers, treating facilities, and riders.

The XYZ transportation provider web interface is a multiuser, web-based application that helps to manage the flow of information between XYZ and the transportation providers. This website allows transportation providers to enter and retrieve certain information about trips they were assigned by XYZ. It also provides some specific performance reports to help them manage their work with XYZ. To access the site, transportation providers must sign up for the site and fill out certain EDI forms.

The XYZ facility services website supports transportation requests from treating facilities on behalf of their clients. The purpose of the site is to provide a means to request trips and to manage trip requests online without the need to call an XYZ call center. The facility services website allows a treating facility to enter a single trip or standing order request for review and approval by an XYZ facility representative, look up and view trip requests, modify or update pending requests, and withdraw pending requests.

The XYZ member services website is like the facility services website, except its focus is on the riders. After a rider has successfully logged in, he or she is able to request new trip reservations, view pending requests and processed reservations, edit pending requests, withdraw pending requests, and cancel existing reservations. Requests are placed in a request queue within the TMS database for review by call center personnel through the TMS.

The XYZ client reporting interface is provided as a service to XYZ's government agencies and managed care providers (user entities). This interface allows them to monitor basic statistics of their business and resolve simple questions and complaints. Summary reports of trip volume, complaints, and utilization are available in addition to detailed reports for single trips, single complaints, and rider eligibility.

People

XYZ has a staff of approximately 500 employees organized in the following functional areas:

- *Corporate.* Executives, senior operations staff, and company administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance, human resources, and transportation provider relations. These individuals use the TMS primarily as a tool to measure performance at an overall corporate level. This includes reporting done for internal metrics as well as for XYZ's user entities.
- *Operations.* Staff that administers the scheduling and administration of transportation providers and riders. They provide the direct day-to-day services, such as transportation reservation intake, trip distribution to transportation providers, quality assurance monitoring, medical facility support, service claims adjudication, transportation network support, and reporting.
 - Customer service representatives take phone calls directly from riders to arrange transportation. These requests are entered into the TMS and initiate the life cycle of a trip.
 - Transportation coordinators use the TMS to assign trips to transportation providers. They also manage rerouting and dispensing work from the TMS to the transportation providers on daily trip lists via fax. Transportation managers maintain the transportation provider network database, including updates for training, violations, screenings, and other compliance measures.

- Quality assurance (or utilization review) employees use reports generated by the TMS to select samples of trips that are tested for contractual compliance and to monitor for fraud and abuse. They also take complaints from riders, facilities, and transportation providers and work them to resolution, using tools within the TMS.
 - The facility staff manages the facility database for the TMS. They also maintain the transportation standing orders within the system and take single trip requests from facilities only.
 - The claims staff receives requests for payment and adjudicates these claims in the software. This includes invoice management, trip verification, and billing support.
 - A reports manager typically uses the TMS to produce contract-level specific reports for XYZ's user entities.
- *IT.* Help desk, IT infrastructure, IT networking, IT system administration, software systems development and application support, information security, and IT operations personnel manage electronic interfaces and business implementation support and telecom.
 - The help desk group provides technical assistance to the TMS users.
 - The infrastructure, networking, and systems administration staff typically has no direct use of the TMS. Rather, it supports XYZ's IT infrastructure, which is used by the software. A systems administrator will deploy the releases of the TMS and other software into the production environment.
 - The software development staff develops and maintains the custom software for XYZ. This includes the TMS, supporting utilities, and the external websites that interact with the TMS. The staff includes software developers, database administration, software quality assurance, and technical writers.
 - The information security staff supports the TMS indirectly by monitoring internal and external security threats and maintaining current antivirus software.
 - The information security staff maintains the inventory of IT assets.
 - IT operations manage the user interfaces for the TMS. This includes processing user entity-supplied membership and eligibility files, producing encounter claims files, and other user-oriented data (capitation files, error reports, remittance advice, and so on).
 - Telecom personnel maintain the voice communications environment, provide user support to XYZ, and resolve communication problems. This group does not directly use the TMS, but it provides infrastructure support as well as disaster recovery assistance.

Data

Data, as defined by XYZ, constitutes the following:

- Master transportation file data
- Transaction data
- Electronic interface files
- Output reports
- Input reports
- System files
- Error logs

Transaction processing is initiated by the receipt of a trip or standing order request. This request typically comes directly from a rider or treating facility by telephone or via the websites, or it may arrive by fax from a treating facility. After the trip is completed, the transportation provider sends XYZ paper documents with daily trip information, including information about completed trips, cancellations or no-shows, and weekly driver logs, all of which is entered into the system's verification module; a portion of this trip completion information may be entered on the XYZ transportation provider web interface.

Output reports are available in electronic PDF, comma-delimited value file exports, or electronically from the various websites. The availability of these reports is limited by job function. Reports delivered externally will only be sent using a secure method—encrypted email, secure FTP, or secure websites—to transportation providers, treating facilities, and governments or managed care providers using XYZ-developed websites or over connections secured by trusted security certificates. XYZ uses Transport Layer Security to encrypt email exchanges with government or managed care providers, facility providers, and transportation providers.

Processes and Procedures

Management has developed and communicated to transportation providers, governments and managed care providers, treating facilities, and riders procedures to restrict logical access to the TMS. Changes to these procedures are performed annually and authorized by senior management. These procedures cover the following key security life cycle areas:

- Data classification (data at rest, in motion, and output)
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access

- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (for example, firewalls)

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

The security category and applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Security criteria and controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services security criteria are included in [section 4](#) of this report. Although the applicable trust services criteria and related controls are included in [section 4](#), they are an integral part of XYZ's description of the TMS.

Control Environment

Management Philosophy

XYZ's control environment reflects the philosophy of senior management concerning the importance of security of medical transportation and logistics data and information. XYZ's Security Steering Committee meets quarterly and reports to the board annually. The committee, under the direction of the XYZ board, oversees the security activities of XYZ. The committee members are from each of the business lines. The committee is charged with establishing overall security policies and procedures for XYZ. The importance of security is emphasized within XYZ through the establishment and communication of policies and procedures and is supported by investment in resources and people to carry out the policies. In designing its controls, XYZ has taken into consideration the relevance of controls to meet the relevant trust criteria.

Security Management

XYZ has a dedicated information security team consisting of a security officer and a senior security specialist responsible for management of information security throughout the organization. They hold positions on the Security Steering Committee and maintain security credentials and are required to annually sign and acknowledge their review of the information security policies. They are responsible for developing, maintaining, and enforcing XYZ's information security policies. The information security policy is reviewed annually by the security officer, CIO, and vice president of operations, and it is approved by the Security Steering Committee.

As the information security team maintains security, it monitors known incidents and patches as well as results from recent vulnerability assessments and addresses necessary changes to the policies and procedures. Such changes can include a reclassification of data, a reassessment of risk, changes in

incident response plans, and a verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during weekly IT maintenance meetings or through system alerts.

During annual security training and awareness programs, management ensures communication of the latest security policies as well as written job descriptions for security management.

Additionally, management is responsible for ensuring business associate agreements are current for third parties and for updating the annual IT risk assessment.

Security Policies

The following security policies and related processes are in place for the TMS:

- Data classification and business impact assessment
- Selection, documentation, and implementation of security controls
- Assessment of security controls
- User access authorization and provisioning
- Removal of user access
- Monitoring of security controls
- Security management

Application TRK is installed to enhance the workflow and approval process in support of the policies. This application enables tracking of

- changes to data classification;
- additions, modifications, or deletions of users;
- changes to authority levels in access approvals;
- tests of new security components prior to installation; and
- reviews of significant security monitoring events.

Personnel Security

Background checks are performed on new information security employees, who are also required to review and acknowledge their receipt of relevant security policies. The new positions are supported by job descriptions. Once employed, employees are subject to XYZ's procedures for accessing systems and sanctions for violating XYZ's information security policy. Employees are instructed to report potential security incidents to the help desk.

XYZ's business associate agreement instructs user entities and transportation providers to notify their respective account representative if they become aware of a possible security breach.

Physical Security and Environmental Controls

The TMS is located in XYZ's NOCs. NOC access is monitored by video surveillance and on-site personnel, and it is controlled through the use of card reader systems. Access to the NOC is limited to authorized personnel based on job function, and physical security access permissions are reviewed quarterly by the security administration team.

XYZ's NOCs employ UPS power systems, air conditioning systems, fire detection and suppression systems, and environmental monitoring and alert notification systems.

Change Management

XYZ has a formalized change management process in place, which requires identification and recording of significant changes, assessment of risk and potential effect of such changes, approval of proposed changes, and testing of changes to verify operational functionality. Proposed changes are evaluated to determine if they present a security risk and what mitigating actions, including employee and user entity notifications, must be performed. The IT management team meets weekly to review and schedule changes to the IT environment.

Emergency changes follow the formalized change management process, but at an accelerated timeline. Prior to initiating an emergency change, necessary approvals are obtained and documented.

Changes to infrastructure and software are developed and tested in a separate development or test environment before implementation. Additionally, developers do not have the ability to migrate changes into production environments.

XYZ has a formalized security and systems development methodology that includes project planning, design, testing, implementation, maintenance, and disposal or decommissioning.

XYZ uses a standardized server build checklist to help secure its servers, and it conducts monthly vulnerability assessments to identify potential system vulnerabilities. Patches are applied regularly in accordance with XYZ's patch management process.

System Monitoring

The security administration team uses a variety of security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, firewall notifications, intrusion detection system (IDS) or intrusion prevention system (IPS) alerts, vulnerability assessment reports, and operating system event logs. These alerts and notifications are reviewed daily by the security administration team using a security incident and event monitoring (SIEM) product.

Additionally, the security administration team has developed and will review the following SIEM reports:

- Failed object level access
- Daily IDS or IPS attacks
- Critical IDS or IPS alerts
- Devices not reporting in the past 24 hours
- Failed login detail
- Firewall configuration changes

- Windows policy changes
- Windows system shutdowns and restarts
- Security events requiring further investigation are tracked using a help desk ticket and monitored until resolved

Problem Management

Security incidents and other IT-related problems are reported to the help desk. Issues are tracked using a help desk ticket and monitored until resolved.

Data Backup and Recovery

XYZ uses data replication and tapes to back up its data files and software. Access to backup devices, scheduling utilities, systems, and media is restricted to authorized personnel.

System Account Management

XYZ has implemented role-based security to limit and control access within the TMS. Employees are granted logical and physical access to in-scope systems based on documented approvals by appropriate management personnel. XYZ's transportation providers, governments and managed care providers (user entities), treating facilities, and riders are approved for access by an authorized user. The ability to create or modify user access accounts and user access privileges is limited to authorized personnel. User access is reviewed quarterly to verify whether individuals' access is necessary for their job functions and to identify the existence of inappropriate accounts.

The human resources department provides IT personnel with an employee termination report every two weeks. IT reconciles the termination report with current access privileges to determine if access has been appropriately removed or disabled. Dormant network accounts are disabled after 90 days of inactivity, and dormant TMS accounts are disabled after 45 days of inactivity.

Administrative access to Active Directory, Unix, and TMS servers and databases is restricted to authorized employees.

Unique user identification numbers, names, and passwords are required to authenticate all users to the TMS, as well as to the facility services, transportation provider, member services, and client reporting websites. Password parameters consist of the following:

- Passwords contain a minimum of six characters, including one non-alphanumeric character.
- Passwords expire every 120 days for non-privileged accounts and 60 days for privileged accounts.
- Log-on sessions are terminated after three failed log-on attempts.
- Users cannot reuse the last three passwords (five passwords for privileged accounts).

Risk Assessment Process

XYZ regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to security based on the applicable trust services criteria set forth in [TSP section 100](#), *2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The information security team assesses security risks on an ongoing basis. This is done through regular management meetings with IT personnel, reviewing and acting upon security event logs, performing vulnerability assessments, and conducting a formal annual IT risk assessment in conjunction with the company-wide risk assessment.

An IT strategic plan is developed annually by the CIO and is communicated to and approved by senior management and the Security Steering Committee. As part of this plan, strategic IT risks affecting the organization and recommended courses of action are identified and discussed.

Senior management, as part of its annual information security policy review, considers developments in technology and the impact of applicable laws and regulations on XYZ's security policies.

Changes in security threats and risks are reviewed by XYZ, and updates to existing control activities and information security policies are performed as necessary.

Information and Communication Systems

XYZ has an information security policy to help ensure that employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of email to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems.

XYZ uses checklists to help facilitate the upload of user (rider or member) information, such as encounter data, trip report, and client complaints, to the appropriate repository (for example, a portal or secure FTP folder) in accordance with the user's instructions.

Monitoring Controls

In addition to the daily oversight, monthly vulnerability assessments, and use of SIEM, management provides further security monitoring through the internal audit department, which performs periodic audits to include information security assessments.

Changes to the System During the Period

There were no changes that are likely to affect report users' understanding of how the TMS is used to provide the service during the period from January 1, 20XX, through December 31, 20XX.

Section 4—Trust Services Category, Criteria, Related Controls, and Tests of Controls

Note to Readers: *Although the applicable trust services criteria, related controls, and management responses to deviations, if any, are presented in this section, they are an integral part of XYZ's description of its transportation management system throughout the period January 31, 20X1, to December 31, 20X1. XYZ's controls and test of controls presented in this section are for illustrative purposes and, accordingly, are not all-inclusive and may not be suitable for all service organizations and examinations.*

Applicable Trust Services Criteria Relevant to Security

The trust services criteria relevant to security address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization's ability to achieve its service commitments and system requirements.

Security refers to the protection of

- i.* *information* during its collection or creation, use, processing, transmission, and storage and
- ii.* *systems* that use electronic information to process, transmit or transfer, and store information to enable the achievement of XYZ's service commitments and system requirements. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
Control Environment			
CC1.1 The entity demonstrates a commitment to integrity and ethical values.	XYZ has documented the code of business conduct and ethical standards which are reviewed, updated if applicable, and approved by the board of directors and senior management annually.	Inspected the code of business conduct and ethical standards of XYZ noting the conduct and standards outlines the service organization's commitments to integrity and ethical values and that the conduct and standards were updated and approved by the board of directors and senior management within the examination period.	No exceptions noted.
	Personnel, including contractors, are required to read and accept the code of business conduct and ethical standards	For a selection of new hires including contract hires, inspected the code of business conduct and ethical standards signed	Two of 45 new hires selected, did not sign the conduct and

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	<p>upon their hire and formally reaffirm them annually thereafter.</p> <p>Agreements are established with service providers and business partners (governments or managed care providers and transportation providers) that include clearly defined terms, conditions, and responsibilities for service providers and business partners.</p>	<p>and determined that the conduct and the standards were acknowledged by each hire selected.</p> <p>For a selection of current personnel, including contractors, inspected the code of business conduct and ethical standards signed and determined that the conduct and the standards were acknowledged annually by each person selected.</p> <p>For a selection of agreements with the service providers and business partners, inspected the agreements and determined that the agreement outlined XYZ's requirements, including terms, conditions, and responsibilities for the service providers and business partners.</p>	standards acknowledgement.
	Management monitors personnel compliance with the code of business conduct and ethical standards through monitoring of customer and workforce member complaints and the use of an anonymous third-	Inspected XYZ's website and test dialed the hotline number provided and determined that an anonymous third-party administered hotline is available.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	party administered ethics hotline. XYZ's code of business conduct includes a sanctions policy for personnel who violate the code of business conduct. The sanctions policy is applied to personnel who violate the code of business conduct.	Inspected XYZ's code of business conduct and determined that it included a sanctions policy for personnel who violate the code of business conduct. For a selection of customer and workforce member complaints logged via the third-party administered hotline, inspected the related documentation and determined that personnel who violated the code of business conduct were sanctioned as per the policy.	
	Prior to employment, personnel are verified against regulatory screening databases, including at a minimum, credit, criminal, drug, and employment checks.	For a selection of new hires, inspected the background checks and determined that selected personnel successfully completed background checks including, credit, criminal, drug and employment checks prior to being hired by XYZ.	No exceptions noted.
	Before a third party is engaged by XYZ, the third-party personnel undergo background screening. A background check includes, at a minimum, credit,	For a selection of third-party personnel engaged by XYZ, inspected the background checks and determined that selected third-party personnel successfully completed background checks including, credit, criminal,	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	criminal, drug, and employment checks.	drug and employment checks prior to being engaged by XYZ.	
CC1.2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	<p>The board of directors are appointed to act on behalf of the shareholders. Roles and responsibilities of the board of directors as outlined in the Board of Directors' Charter are segregated from the roles and responsibilities of management.</p> <p>The board of directors understand and acknowledge the Board of Directors' Charter to accept its oversight responsibilities in relation to established requirements and expectations.</p>	<p>Inspected the Board of Directors' Charter and determined that the board of directors are appointed to act on behalf of the shareholders and the roles and responsibilities are segregated from the roles and responsibilities of management.</p> <p>Inspected the board of directors' acknowledgement of the Board of Directors' Charter to accept its oversight responsibilities in relation to established requirements and expectations.</p>	No exceptions noted.
CC1.2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	<p>The board of directors are appointed to act on behalf of the shareholders. Roles and responsibilities of the board of directors as outlined in the Board of Directors' Charter are segregated from the roles and responsibilities of management.</p> <p>The board of directors understand and acknowledge the Board</p>	<p>Inspected the Board of Directors' Charter and determined that the board of directors are appointed to act on behalf of the shareholders and the roles and responsibilities are segregated from the roles and responsibilities of management.</p> <p>Inspected the board of directors' acknowledgement of the</p>	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	of Directors' Charter to accept its oversight responsibilities in relation to established requirements and expectations.	Board of Directors' Charter to accept its oversight responsibilities in relation to established requirements and expectations.	
	<p>The Board of Directors' Charter includes the minimum background and skills required of board of directors.</p> <p>During the annual board meeting, the background and skills of each board member is compared to the background and skills noted in the Board of Directors' Charter.</p>	<p>Inspected the Board of Directors' Charter and determined that the minimum background and skills required of board of directors is documented.</p> <p>For the annual board meeting, inspected the meeting minutes and determined that the background and skills of each board member was compared to the background and skills noted in the Board of Directors' Charter.</p>	No exceptions noted.
	The board of directors consist of majority of independent members as per the Board of Directors' Charter to maintain independence from management.	<p>Inspected the Board of Directors' Charter and determined that it notes the board of directors should consist of majority of independent members.</p> <p>Inspected the board of directors' structure and determined that the board of directors consisted of majority of independent members.</p>	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	<p>XYZ has a Security Steering Committee governed by the Security Steering Committee Charter that provides support to the board of directors.</p> <p>The Security Steering Committee Charter includes roles and responsibilities relevant to security.</p>	<p>Inspected the Security Steering Committee structure and determined that a Security Steering Committee is in place.</p> <p>Inspected the Security Steering Committee Charter and determined that it included roles and responsibilities relevant to security.</p>	No exceptions noted.
CC1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	XYZ management and the board of directors evaluate its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revise these when necessary to support the achievement of objectives.	Inspected the annual business planning and risk assessment documentation and determined that organizational structure, reporting lines, authorities, and responsibilities were revised.	No exceptions noted.
	Job descriptions are reviewed by XYZ management on an annual basis for needed changes and where job duty changes are required necessary changes to these job descriptions are also made to enable execution of authorities	Inspected the annual business planning and risk assessment documentation and determined that organizational structure, reporting lines, authorities, and responsibilities were revised.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	and responsibilities and flow of information to manage the activities of XYZ.		
	<p>Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors taking into consideration segregation of duties as necessary at the various levels of the organization and requirements relevant to security.</p> <p>Personnel are required to sign a copy of their job description to acknowledge their understanding of their responsibilities.</p> <p>Reporting relationships and organizational structures are reviewed periodically by senior management and the board of directors as part of organizational planning and adjusted as needed based on changing commitments and requirements.</p>	<p>Inspected the organizational structure and job descriptions and determined that organizational structure, reporting lines, authorities, and responsibilities were documented taking into consideration segregation of duties as necessary relevant to security.</p> <p>For a selection of personnel hired or transferred to a new role during the period, obtained the file copy of their job description and determined that the employees had acknowledged their understanding of their responsibilities.</p> <p>Inspected the annual business planning and risk assessment documentation and determined that organizational structure, reporting lines, authorities, and</p>	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		responsibilities were revised.	
	<p>The security commitments and obligations of transportation providers, governments and managed care providers (user entities), treating facilities, and riders are posted on XYZ's websites and the web interface and included in business associate agreements.</p> <p>Roles and responsibilities for external party interaction and activity monitoring are defined in written job descriptions and communicated to personnel. Personnel are required to sign a copy of their job description to acknowledge their understanding of their responsibilities.</p>	<p>Inspected XYZ websites, web interface, and the standard business associate agreement and determined that the security commitments and obligations of user entities, treating facilities, and riders are posted on XYZ's websites and the web interface and included in business associate agreements.</p> <p>For a selection of user entities, transportation providers, governments and treating facilities, inspected the signed business associate agreements and compared those to the standard agreements for consistency.</p> <p>For a selection of personnel hired or transferred to a new role with roles that requires interaction with the external parties during the period, obtained the file copy of their job description and determined that the employees had acknowledged their</p>	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		understanding of their responsibilities.	
CC1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	<p>Job requirements are documented in the job descriptions and candidates', whether an employee, contractor, or vendor employee, abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process to support the achievement of objectives.</p> <p>The experience and training of candidates, whether an employee, contractor, or vendor employee, for employment of transfer are evaluated before they assume the responsibilities of their position to support the achievement of objectives. Existing personnel are evaluated at least annually.</p>	<p>For a selection of new hires, whether an employee, contractor, or vendor employee, and transfers, whether an employee, contractor, or vendor employee, who have transferred internally, inspected the personnel file and determined that job requirements were documented in the job descriptions.</p> <p>For a selection of new hires, whether an employee, contractor, or vendor employee, and transfers, whether an employee, contractor, or vendor employee, who have transferred internally, inspected the personnel file and determined that offer letter and management notes were maintained evidencing that the selected personnel were evaluated before they assume the responsibilities of their position.</p> <p>For a selection of personnel, whether an employee, contractor, or</p>	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		vendor employee, inspected the personnel file and determined that annual performance evaluations were performed including action items for any shortcomings or decision to terminate the employment.	
	Personnel competence across XYZ and in outsourced service providers is measured against established policies and practices as part of the annual evaluation process or when new outsourced service provider relationships are established to support the achievement of XYZ's service commitments and system requirements. Any shortcomings noted during the evaluation are addressed with action items and reevaluated in the following year's evaluation process or sooner.	<p>For a selection of personnel, whether an employee, contractor, or vendor employee, inspected the personnel file and determined that annual performance evaluations were performed including action items for any shortcomings or decision to terminate the employment.</p> <p>For a selection of outsourced service providers, including existing and new providers, inspected the annual service provider risk assessments performed and determined that external service provider performance and risks were assessed, including action items for any shortcomings as well as follow-up on prior year's</p>	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		action items as necessary.	
	<p>Management establishes requisite skillsets for personnel, whether an employee, contractor, or vendor employee, and provides continued training about its commitments and requirements for personnel to support the achievement of objectives.</p> <p>Management monitors compliance with training requirements.</p>	<p>Obtained the dates of and attendance sheets for the annual security training, as well as the quarterly security compliance updates for employees and determined that employees had signed the attendance sheet for training sessions and updates on the specified dates.</p> <p>For a selection of personnel, obtained the dates of and attendance sheets for role-specific trainings and determined that the employee, contractor, or vendor employee selected had signed the attendance sheet for training sessions and updates on the specified dates.</p> <p>For a selection of personnel not present during the training dates, inspected management's training related documentation and determined that the selected personnel were required to take the training subsequently</p>	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		within the examination period.	
	During its ongoing and periodic business planning, business continuity planning and budgeting process, management and the board of directors evaluate the need for additional tools and resources to achieve business objectives including contingency plans for assignments of responsibility important for internal control.	Inspected XYZ's annual business planning, business continuity planning and budgeting related documentation and determined that XYZ continually evaluated its need for additional tools and resources as well as contingency plans for assignments of responsibility important for internal control.	No exceptions noted.
	Prior to employment, personnel, including contractors and vendor employees, are verified against regulatory screening databases, including at a minimum, credit, criminal, drug, and employment checks. For personnel with responsibility important for internal control, such back ground checks are re-performed every two years.	For a selection of new hires, including contractors and vendor employees, inspected the background checks and determined that selected personnel successfully completed background checks including, credit, criminal, drug and employment checks prior to being hired by XYZ. For a selection of personnel with responsibility important for internal control, inspected the background checks and determined that selected personnel successfully completed background	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		checks including, credit, criminal, drug and employment checks every two years.	
CC1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	<p>XYZ management and the board of directors perform annual performance evaluations to communicate and hold individuals accountable for performance of internal control responsibilities. The performance evaluation is signed by the manager and employee. Corrective actions, including training or sanctions, as necessary.</p> <p>Each XYZ department, such as Software Development, Information Security, Infrastructure, Networking and Systems Administration, IT Operations, Help Desk, Human Resources, Legal, Compliance, Internal Audit, Finance, Customer Support, IT Operations, hold periodic (weekly) meetings to monitor and manage respective department's progress or lack thereof as it relates to their achievement of</p>	<p>For a selection of personnel, whether an employee, contractor, or vendor employee, inspected the personnel file and determined that annual performance evaluations were performed including action items for any shortcomings or decision to terminate the employment, and whether evaluations were signed by the manager and the employee.</p> <p>For a selection of weekly department meetings that impacted security criteria, inspected the meeting minutes and determined that department's progress is monitored and measured by respective department heads, including escalation or taking of corrective action as necessary.</p>	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	department's responsibilities.		
	<p>Management and the board of directors establish measurable goals and performance evaluation criteria, including, incentives, other rewards, and sanctions appropriate for responsibilities at all levels of XYZ, considering the achievement of both short-term and longer-term objectives. Established short-term and longer-term XYZ goals and performance evaluation, reward and sanctions criteria for XYZ executives are reviewed and approved annually by the Compensation Committee.</p>	<p>For a selection of roles, inspected XYZ's documented goals, performance evaluation criteria and compensation matrix including incentives and rewards and determined that a formal process has been implemented for performance measures, incentives and rewards and that the goals documented for selected roles included both short-term and longer-term goals that aligned with XYZ's short-term and longer-term goals.</p> <p>Inspected the annual Total Executive Compensation Package and determined that the Compensation Committee approved the package.</p>	No exceptions noted.
	<p>Management and the board of directors establish measurable goals and performance evaluation criteria, taking into consideration pressures associated with the achievement of objectives. XYZ personnel with internal control</p>	<p>For a selection of roles, inspected XYZ's documented goals, performance evaluation criteria and compensation matrix including incentives and rewards and determined that a formal process has been implemented for</p>	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	responsibility are not rewarded based on number of exceptions noted or lack thereof by the external auditor. Established short-term and longer-term XYZ goals and performance evaluation, reward and sanctions criteria for XYZ executives are reviewed and approved annually by the Compensation Committee.	performance measures, incentives and rewards and that the goals documented for selected roles considers excessive pressures or conflicting goals and evaluation criteria. Inspected the annual Total Executive Compensation Package and determined that the Compensation Committee approved the package.	
	Management and the board of directors evaluate performance of internal control responsibilities, providing rewards and sanctions appropriate for responsibilities, considering the achievement of both short-term and longer-term objectives.	For a selection of personnel, inspected the personnel file and determined that annual performance evaluations were performed including action items for any shortcomings and that rewards or disciplines documented were consistent with the goals and performance evaluation criteria established by.	No exceptions noted.
Information and Communication			
CC2.1 The entity obtains or generates and uses relevant, quality information to support the	XYZ performs assessment at least annually to identify the information required and expected to support the internal control and the achievement of XYZ's	Inspected XYZ's annual assessment and determined that it identifies the information required to support internal controls and the achievement of XYZ's	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
functioning of internal control.	service commitments and system requirements. XYZ's most valuable and sensitive digital data and mission-critical systems, "crown jewels" are identified during the assessment, including internal and external sources of data.	service commitments and system requirements, including identification of most valuable data and mission critical systems, i.e., "crown jewels" whether those are internal or external to XYZ.	
	XYZ performs assessment at least annually to identify key information system processes that process relevant data into information to support the internal control and the achievement of XYZ's service commitments and system requirements.	Inspected XYZ's annual assessment and determined that it identifies the key information system processes that process relevant data into information required to support internal controls and the achievement of XYZ's service commitments and system requirements.	No exceptions noted.
	XYZ has implemented various processes and procedures relevant to security to produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. XYZ has logical and physical security, change management, incident monitoring, and data classification, integrity, and retention controls, as	Inspected XYZ's documented policies and procedures as it relates to security of most valuable data and mission critical systems and determined that those document XYZ's internal controls for producing, timely, current, accurate, complete, accessible, protected, verifiable and retained information, as applicable. [Also refer to controls and service	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	necessary, with checks and balances woven into each applicable process to ensure quality of processing.	auditor's tests of controls under CC4 through CC9.]	
CC2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security of the system, is provided to personnel to carry out their responsibilities.	Inspected XYZ's intranet and determined that documented policies and procedures as it relates to security of most valuable data and mission critical systems is available to internal personnel on the intranet.	No exceptions noted.
	<p>XYZ management and the board of directors meet quarterly and annually to communicate information needed to fulfill their roles with respect to the achievement of XYZ's service commitments and system requirements.</p> <p>XYZ has incident response policies and procedures in place that includes an escalation plan based on the nature and severity of the incident to senior management and the board of directors as necessary.</p>	<p>For a selection of quarters and the year, inspected the quarterly and annual board meeting minutes and determined that those minutes documented discussion of key items with respect to the achievement of XYZ's service commitments and system requirements, including, progress, delays, risks, challenges related to those key items as applicable.</p> <p>Inspected XYZ's documented Incident Response policies and procedures and</p>	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		determined that it includes escalation tree and communication plans depending on the nature of the incident, including escalation to the Board, as necessary.	
	XYZ has anonymous third-party administered whistle-blower hotlines available to internal and external users. Management monitors customer and workforce member complaints reported via the hotlines.	<p>Inspected XYZ's website and test dialed the hotline number provided and determined that an anonymous third-party administered hotline is available.</p> <p>For a selection of customer and workforce member complaints logged via the third-party administered hotline, inspected the related documentation and determined that personnel who violated the code of business conduct were sanctioned as per the policy.</p>	No exceptions noted.
	XYZ holds quarterly and annual Board meetings. In addition, for communication of an unforeseen event, incident response policies and procedures are in place that includes escalation plan based on the nature and severity of the incident to senior management and the	For a selection of quarters and the year, inspected the quarterly and annual board meeting minutes and determined that those documented discussion of key items with respect to the achievement of XYZ's service commitments and system requirements, including,	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	board of directors as necessary.	<p>progress, delays, risks, challenges related to those key items as applicable.</p> <p>Inspected XYZ's documented incident response policies and procedures and determined that it includes escalation tree and communication plans depending on the nature of the incident, including escalation to the Board, as necessary.</p>	
	<p>XYZ's security commitments are communicated to external users (governments or managed care providers and transportation providers), as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.</p> <p>The responsibilities of internal users whose roles affect system operation are communicated to those parties.</p>	<p>Inspected XYZ's intranet, customer portal, and websites and determined that documented responsibilities, policies and procedures as they relate to security commitments and responsibilities are available to internal personnel on the intranet and external personnel on XYZ's websites and customer portals as applicable.</p> <p>For a selection of responsibilities, policies and procedures posted on the intranet, inspected the documents and determined that history of changes with</p>	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	Responsibilities and policies and procedures posted on XYZ's intranet are updated as necessary.	the date of change was documented.	
	Internal and external users have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected XYZ's documented incident response policies and procedures and determined that it includes escalation tree and communication plans depending on the nature of the incident, including escalation to the Board, as necessary.	No exceptions noted.
	Changes to XYZ's commitments and system requirements are communicated to internal and external users, vendors, and other third parties (governments or managed care providers and transportation providers) whose services are part of the system.	Inspected XYZ's intranet, customer portal, and websites and determined that documented responsibilities, policies and procedures as it relates to security commitments and responsibilities are available to internal personnel on the intranet and external personnel on XYZ's websites and customer portals as applicable, and that those responsibilities, policies and procedures documented history of changes with the date of change. For a selection of agreements with the service providers and	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		business partners, inspected the agreements and determined that the agreement outlined XYZ's requirements, including terms, conditions, and responsibilities for the service providers and business partners and that signed addendum to agreements were also maintained when changes to commitments and requirements occurred, as necessary.	
	<p>Management provides continued training about its security commitments and requirements for personnel to support the achievement of objectives.</p> <p>Management monitors compliance with security training requirements.</p> <p>XYZ also provides user guides, security alerts and known issues on its websites and customer portal with information to improve security knowledge and awareness.</p>	<p>Obtained the dates of and attendance sheets for the annual security training, as well as the quarterly security compliance updates for employees and determined that employees had signed the attendance sheet for training sessions and updates on the specified dates.</p> <p>For a selection of personnel not present during the training dates, inspected management's training related documentation and determined that the selected personnel were required to take the</p>	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		<p>training subsequently within the examination period.</p> <p>Inspected XYZ's customer portal and websites and determined that user guides and history of security alerts and known issues with information to improve security knowledge and awareness was available.</p>	
	XYZ posts a description of its system, system boundaries, and system processes that include infrastructure, software, people, processes and procedures, and data on its intranet for internal users and on the internet for external users.	Inspected XYZ's intranet and internet descriptions of XYZ's system, system boundaries, and system processes and determined that the description addressed infrastructure, software, people, processes and procedures, and data for the in-scope technology and locations.	No exceptions noted.
	Agreements are established with service providers and business partners (governments or managed care providers and transportation providers) that include clearly defined terms, conditions, and responsibilities for service providers and business partners.	For a selection of agreements with the service providers and business partners, inspected the agreements and determined that the agreement outlined XYZ's requirements, including terms, conditions, and responsibilities for the service providers and business partners.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	<p>Planned changes to system components are reviewed, scheduled, and communicated to management as part of the weekly IT maintenance process.</p> <p>Planned changes to system components are communicated to external users (governments, managed care providers, and transportation providers) via the XYZ's website.</p>	<p>For a selection of weeks, inspected weekly IT maintenance schedules and communications and determined that planned system changes were included and had been reviewed and signed off by IT management.</p> <p>Inspected XYZ's customer portal and determined that it published a calendar of upcoming system changes existed and that it communicated upcoming changes and their impact on users, if any.</p>	No exceptions noted.
CC2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.	XYZ has incident response policies and procedures in place that includes an escalation plan based on the nature and severity of the incident to senior management, the board of directors and external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties as necessary.	Inspected XYZ's documented incident response policies and procedures and determined that it includes escalation tree and communication plans depending on the nature of the incident, including escalation to senior management, the board of directors and external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties as necessary.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	<p>XYZ has made available contact email and phone numbers on its website and customer portal to customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, including anonymous third-party administered whistle-blower hotlines. Management monitors customer and workforce member complaints reported via the hotlines, emails and phones.</p>	<p>Inspected XYZ's customer portal and websites and determined that contact email and phone numbers are available to customers and external users on the customer portal and websites.</p> <p>Inspected XYZ's website and test dialed the hotline number provided and determined that an anonymous third-party administered hotline is available.</p> <p>For a selection of customer and workforce member complaints logged via the third-party administered hotline, inspected the related documentation and determined that personnel who violated the code of business conduct were sanctioned as per the policy.</p>	No exceptions noted.
	<p>The Legal, Compliance, and Internal Audit departments meets with the board of directors quarterly to provide relevant information resulting from assessments conducted by internal and external parties. In addition, any significant information</p>	<p>For a selection of quarters and the year, inspected the quarterly and annual board meeting minutes and determined that the Legal, Compliance and Internal Audit departments presents an executive summary of all external and internal</p>	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	security related findings noted as part of XYZ's financial audits are communicated by the external auditor to the Audit Committee during quarterly and annual meetings.	audit findings for the quarter including copies of the audit reports to the Board, and that significant information security related findings noted by the external auditors were also communicated by the external auditor to the Audit Committee.	
	XYZ posts a description of its system, system boundaries, and system processes that include infrastructure, software, people, processes and procedures, and data on its intranet for internal users and on the internet for external users.	Inspected XYZ's intranet and internet descriptions of XYZ's system, system boundaries, and system processes and determined that the description addressed infrastructure, software, people, processes and procedures, and data for the in-scope technology and locations.	No exceptions noted.
	XYZ's security commitments are communicated to external users, as appropriate. Agreements are established with service providers and business partners (governments or managed care providers and transportation providers) that include clearly defined terms, conditions, and responsibilities for	Inspected XYZ's customer portal and websites and determined that documented responsibilities as it relates to security commitments and responsibilities are available to external personnel. For a selection of agreements with the service providers and business partners, inspected the	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	service providers and business partners.	agreements and determined that the agreement outlined XYZ's requirements, including terms, conditions, and responsibilities for the service providers and business partners.	
Risk Assessment			
CC3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	XYZ management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the board of directors. The objectives incorporate the service commitments and system requirements of the MT services and TMS. Assessed risks are reviewed quarterly to identify changes in underlying threats or in the environment that would require an update to assessed risks.	Inspected the annual risk assessment documentation to determine whether the risk assessment process included consideration of the MT service commitments and TMS system requirements. Inspected documentation for two of the three quarterly reviews of the risk assessment to determine whether the reviews included evaluation of identified changes in laws and regulations and changes to contractual commitments.	No exceptions noted.
	XYZ subscribes to an external reporting service that identifies changes to laws and regulations relating to MT services for the jurisdictions in which it operates. Reported changes are	Obtained the monthly reports of changes in laws and regulations received from the external reporting service. For a sample of changes reported, obtained the evaluation	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	evaluated by personnel within the General Counsel's Office for their impact and the evaluations are communicated to senior management and are incorporated into the risk assessment and review process.	of the changes by General Counsel Office personnel and the communication of the evaluation to senior management to determine whether the changes assessed for their impact on the TMS system. Inspected documentation of the use of the evaluation in the subsequent annual risk assessment and quarterly risk assessment reviews.	
	Contracts personnel within the General Counsel's Office maintain a database of contract terms and commitments. Updates of or modifications to standard contractual terms and commitments are approved by the Chief Operating Officer prior to contract approval. Updates and modifications to contractual terms and commitments are incorporated into the risk assessment and review process.	<p>For a sample of updates to standard contract terms and new contracts with terms that differed from the standard contractual terms, inspected the entry in the contract terms and commitments databased to determine whether the changes were recorded completely and accurately.</p> <p>For a sample of changes to the contract terms and commitments database, inspected documentation of the Chief Operating Officer's approval of the change prior to contract execution.</p> <p>For a sample of changes to the contract terms and</p>	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		commitments database, Inspected documentation of the consideration of the change in the subsequent annual risk assessment and quarterly risk assessment reviews.	
CC3.2 The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Monthly, XYZ's Security Steering Committee meets to discuss strategy and operations, financial results, risk considerations, and other factors critical to the business.	Inspected a sample of minutes from monthly Security Steering Committee meetings to determine whether organizational strategy and operations, financial results and risk considerations critical to the business were discussed.	No exceptions noted.
	A quarterly risk assessment is performed to identify risks arising from external and internal sources and the effectiveness of these controls are shared with executive management and the audit committee.	Inspected the annual risk assessment to determine whether risks arising from external and internal sources and effectiveness of controls to mitigate those risks were identified and communicated.	No exceptions noted.
	An overview of the annual risk assessment is presented to the audit committee as well as used to help establish the annual audit plan.	Inspected a sample of minutes and meeting agendas from the audit committee meetings to determine whether an overview of the risk assessment was communicated.	No exceptions noted.
	The information security team assess and	Inspected a sample of minutes and meeting	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	responds to security risks on an ongoing basis through regular management meetings with IT personnel, reviewing and acting upon security event logs, performing vulnerability assessments, and conducting a formal annual IT risk assessment in conjunction with the company-wide risk assessment.	agendas from monthly information security team meetings to determine whether security risks and vulnerabilities were identified, assessed, and analyzed by management.	
	XYZ has a defined information classification scheme for the labeling and handling of data. XYZ classifies data into four levels: public, internal use, confidential, and protected.	Inspected the data classification policy to determine whether there is a documented classification scheme for labeling and handling data. For a sample of data files and databases, obtain the relevant data dictionary and compared the data classification per the contents of the data dictionary, the data classification scheme, and the data classification of the file/database.	No exceptions noted.
	XYZ conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services.	Inspected the annual risk assessment and a sample of completed vendor questionnaires during the calendar year to determine whether an organizational	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		assessment of risk was performed prior to the acquisition or outsourcing of dedicated information security services.	
	<p>A company-wide risk assessment is performed annually by management and includes the following:</p> <ul style="list-style-type: none"> <i>a.</i> Determining business objectives, entity, subsidiary, division, operating unit, and functional levels. <i>b.</i> Evaluating the effect of environmental, regulatory, and technological changes on XYZ's system security <i>c.</i> Involving appropriate levels of management. <i>d.</i> Analyzing risks associated with the threats <i>e.</i> Identifying threats to operations, including security threats, using information technology asset records <i>f.</i> Identifying threats to operations, including threats from 	Inspected the annual risk assessment documentation to determine whether they included the significant aspects of operations.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	<p>vendors, business partners, and other parties.</p> <p><i>g.</i> Determining a risk mitigation strategy</p>		
CC3.3 The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Management conducts a periodic fraud risk assessment to identify the various ways that fraud and misconduct can occur, including how management might engage in inappropriate actions, and maintains documentation of this assessment.	Inspected the fraud risk assessment documentation to determine whether management periodically evaluated and assessed the various ways fraud and misconduct can occur and that documentation of the assessment was maintained.	No exceptions noted.
	The board, audit committee and management review the XYZ's compensation and performance evaluation programs annually to identify potential incentives and pressures for employees to commit fraud.	Inspected the fraud risk assessment documentation to determine whether compensation and performance evaluation programs were reviewed annually by the board, audit committee and management.	No exceptions noted.
	XYZ has established measures to protect against unauthorized and willful acquisition, use, or disposal of assets.	Inspected the fraud risk assessment documentation and internal audit plan to determine whether measures were established to protect against unauthorized and unwell acquisition, use or disposal of assets.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	Management uses information technology tools including security systems, fraud detection and monitoring systems, and incident tracking systems to identify and manage fraud risk.	Inspected the fraud risk assessment documentation to determine whether management considered threats and vulnerabilities from the use of IT and access to information.	No exceptions noted.
CC3.4 The entity identifies and assesses changes that could significantly impact the system of internal control.	<p>XYZ, through its ongoing an annual risk assessment process, evaluates changes in:</p> <ul style="list-style-type: none"> a. the regulatory, economic, and physical environment in which XYZ operates. b. the business environment, including industry, competitors, regulatory environment, and consumers. c. the potential impact of new business lines, dramatically altered business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies. d. the management and respective attitudes and philosophies on the 	<p>Inspected the annual risk assessment documentation to determine that management identified the need for new controls to address risks that were not adequately addressed by existing controls.</p> <p>Inspected a sample of system change requests to determine that management followed the change management process for new controls identified.</p>	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	<p>system of internal control.</p> <p>e. XYZ's systems and changes in the technology environment.</p> <p>f. vendor and business partner relationships.</p>		
Monitoring Activities			
CC4.1 The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The internal audit department performs periodic audits to include information security assessments.	Inspected the internal audit plan for the calendar year and noted it included information security assessments.	No exceptions noted.
	Internal audit annual plans include a risk analysis of all significant operating and reporting areas of XYZ as a means to prioritize audit efforts for the year.	Inspected the internal audit plan and risk analysis documentation and noted that the significant operating and reporting areas of XYZ were assessed to prioritize audit efforts for the year.	No exceptions noted.
	XYZ developed, documented, and maintained a baseline configuration of the internal control system.	Inspected the baseline configuration documentation and noted that the design and current state of the internal control system	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		was used to establish a baseline for ongoing and separate evaluations.	
	XYZ provides training, as well as annual performance reviews, for internal audit personnel.	Obtained the dates of and attendance sheets for the annual training, as well as the annual performance reviews for internal audit personnel. Determined whether employees had signed the attendance sheet for training sessions and updates on the specified dates.	No exceptions noted.
	On a quarterly basis, internal audit performs an assessment of the audit plan and scope to identify potential changes impacting XYZ's risk profile.	Inspected the quarterly internal audit plan assessment and noted that the internal audit plan and scope was assessed to identify potential changes impacting XYZ's risk profile.	No exceptions noted.
	An internal audit department exists that is independent of management.	Inspected the organizational chart of XYZ noting the organizational chart described functional areas and reporting structures within functional areas and that reporting hierarchies were defined and appropriately segregated.	No exceptions noted.
	Internal audit personnel perform audit procedures	Inspected internal audit methodology and	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	using a formal methodology, document their procedures and results in working papers, and prepare an audit report summarizing the procedures performed and the findings from those procedures.	ascertained that the methodology, including requirements for planning, execution, and reporting, and based on standards established by a professional organization. For an XYZ internal audit, inspected documentation and ascertained that the documentation complied with the defined methodology.	
	Internal audit developed audit programs that include a mix of manual and automated controls, as well as preventive and detective controls, to mitigate risks identified during the risk assessment process.	Inspected a sample of audit programs during the calendar year to determine whether control activities to mitigate identified risks included a mix of manual, automated, detective and preventive controls.	No exceptions noted.
	Internal audit developed audit programs that include various levels of management.	Inspected a sample of audit programs during the calendar year to determine whether control activities applied various levels of management.	No exceptions noted.
	The XYZ's Security Steering Committee reviews reports from regulators or other third parties to determine whether they indicate	Inspected a sample of minutes from quarterly Security Steering Committee meetings to determine whether regulatory or other third-party reports were	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	possible deficiencies in internal control.	reviewed for possible internal control deficiencies.	
CC4.2 The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Complete reports of deficiencies in internal control from internal and external sources are provided to the board and audit committee. The board and audit committee work with management to suggest appropriate remediation and follow up to ensure that proper controls have been established.	Inspected minutes from the annual board meeting and audit reports to determine whether deficiencies in internal control and external sources were reported to the board and audit committee.	No exceptions noted.
	XYZ has established a practice that requires all deficiencies rated as serious threats to be reported to senior management and to the board or audit committee.	Inspected minutes from the annual board meeting to determine whether the audit committee reported deficiencies rated as serious threats were reported to the board.	No exceptions noted.
	The board and/or audit committee track the status of all deficiencies that have been rated as a serious threat to the organization until satisfactorily resolved.	Inspected the deficiency tracking matrix to determine whether deficiencies rated as serious threats to the organization were tracked to resolution by the board and/or audit committee.	No exceptions noted.
Control Activities			

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
CC5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	As part of its annual risk assessment, management linked the identified risks to controls that have been designed and operated to address them. When the need for new controls is identified, management develops the requirements for the new controls and uses the change management process to implement them.	Obtained and inspected the annual risk assessment documentation to determine that new controls were implemented for any risks not adequately addressed by existing controls. Inspected a sample of system change requests to determine that the change management process was followed.	No exceptions noted.
	As part of the risk assessment, management assessed the environment, complexity, nature and scope of its operations when developing control activities to mitigate the risks.	Obtained and inspected the risk assessment documentation to determine whether management assessed the environment, complexity, nature and scope of its operations when developing control activities to mitigate the risks	No exceptions noted.
	When management identifies the need for new controls, management considers a mix of control activities, included both manual and automated controls and preventive and detective controls.	Obtained and inspected the risk assessment documentation to determine whether management considered a mix of control activities to mitigate the identified risks.	No exceptions noted.
	XYZ has designed application-enforced	Inspected the access control policy to	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	segregation of duties to define what privileges are assigned to users within applications.	determine whether application controls were designed to enforce segregation of duties to users within applications.	
CC5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives.	As part of the IT strategic plan, strategic IT risks affecting the organization and recommended courses of action are identified and discussed.	Inspected the annual IT strategic plan documentation to determine whether IT risk affecting the organization and recommended courses of action were identified and discussed.	No exceptions noted.
	Management developed a list of control activities to manage the technology infrastructure risks identified during the annual risk assessment process.	Inspected the risk assessment, internal audit plan and audit program for the calendar year to determine whether management developed and implemented control activities over the technology infrastructure.	No exceptions noted.
	Management developed a list of control activities to manage the security access management risks identified during the annual risk assessment process.	Inspected the risk assessment, internal audit plan and audit program for the calendar year to determine whether management developed and implemented control activities designed to restrict technology access rights to authorized users commensurate with their job responsibilities and	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		protect corporate assets from external threats.	
	XYZ employs organization-defined tailored acquisition strategies and procurement methods for the purchase, development, and maintenance of information systems, system components, or information system services from technology suppliers.	Inspected the procurement policy manual to determine whether management employed acquisition strategies and procurement methods for the purchase, development, and maintenance of information systems, system components, or information system services from technology suppliers.	No exceptions noted.
CC5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	<p>XYZ's policy and procedure manuals address controls over significant aspects of operations. Policy sections include</p> <ul style="list-style-type: none"> <i>a.</i> security requirements for authorized users; <i>b.</i> data classification and associated protection, access rights, retention, and destruction requirements; <i>c.</i> risk assessment; <i>d.</i> access protection requirements; 	Inspected the policy and procedure manuals to determine whether they included section headings that addressed controls over the significant aspects of system operations.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	<p><i>e.</i> user provisioning and deprovisioning;</p> <p><i>f.</i> responsibility and accountability for security;</p> <p><i>g.</i> responsibility and accountability for system changes and maintenance;</p> <p><i>h.</i> change management;</p> <p><i>i.</i> complaint intake and resolution;</p> <p><i>j.</i> security and other incidents identification, response and mitigation;</p> <p><i>k.</i> security training;</p> <p><i>l.</i> handling of exceptions and situations not specifically addressed in policies;</p> <p><i>m.</i> commitment and requirement identification and compliance measurement; and</p> <p><i>n.</i> information sharing and disclosure.</p>		
	The XYZ's Security Steering Committee is charged with establishing, maintaining, and enforcing the overall	Inspected a sample of minutes from quarterly Security Steering Committee meetings to determine whether the	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	security policies and procedures.	committee was charged with establishing, maintaining, and enforcing the overall security policies and procedures.	
	Monthly service level assessments are performed by the functional heads of each department. These assessments include evaluation of the operation of key controls.	Inspected a sample of minutes from monthly departmental and management committee meetings to determine whether the evaluation of the operation of key controls were performed by department heads.	No exceptions noted.
	Assessments are reviewed at monthly departmental meetings and require the development of corrective action plans for control weaknesses.	Inspected a sample of minutes from monthly departmental and management committee meetings to determine whether the corrective action plans for control weaknesses were reviewed by department heads and the management committee.	No exceptions noted.
	XYZ has written job descriptions specifying the responsibilities and the academic and professional requirements for key job positions. Human resources personnel screen internal and external job applicant qualifications	For a sample of positions, inspected written job descriptions to determine whether the job descriptions included responsibilities and academic and professional requirements. For a sample of employees, inquired of	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	<p>based on the defined requirements within the job description. Transcripts are obtained to evidence educational attainment, and job references are checked to validate experience.</p>	<p>the employees about their understanding of their job responsibilities, academic qualifications, and professional certifications and compared their responses for consistency to the documented responsibilities, and academic and professional requirements documented in the job description applicable to their position.</p> <p>For a sample of new employees and employees who have transferred internally, inspected the personnel file to determine whether transcripts were obtained, and job references were checked.</p>	
	<p>XYZ's policy and procedure manuals are reviewed annually by the CIO, Vice President of Operations, and the Security Officer for consistency with the organization's risk mitigation strategy and updated as necessary for changes in the strategy.</p>	<p>Inspected the policy and procedure manuals to ascertain whether policies and procedures had been updated for changes in the risk mitigation strategy. Inspected documentation of the annual review of the policy and procedures manuals by the CIO, Vice President of</p>	<p>No exceptions noted.</p>

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		Operations, and the Security Officer.	
<i>Logical and Physical Access</i>			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The service organization monitors all system components through an automated management interface to log, track, and maintain all inventory components.	Inspected the automated inventory management tool to determine that the tool is in place to monitor the system components. Inspected information system inventory records from the inventory management tool to determine that the tool was providing necessary information to manage assets.	No exceptions noted.
	XYZ permits remote access to production systems by authorized employees only with multi-factor authentication (MFA) over encrypted virtual private network (VPN) connection.	Observed a remote login session to determine that MFA VPN was required to access the production network.	No exceptions noted.
	In-scope system components require unique username and passwords (or authorized SSH keys) prior to authenticating users.	Inspected login attempts to determine that the in-scope system components required authentication measures for users.	No exceptions noted.
	End user and server workload network traffic	Inspected the network diagram and configurations to determine that customer	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	is segmented to support isolation.	environments and data are segmented.	
	Management performs a quarterly access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected access review documentation for sample of quarters to determine that an access review was performed for in-scope system components and that tickets were created to remove inappropriate access.	No exceptions noted.
	A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel. SSL certificates are used at the entry-point firewalls to information assets to establish access control rules.	Inspected the data classification policy to determine that procedures existed around classifying and protecting confidential information. Inspected the SSL certificates for verification, issuance, signature algorithm, and validity date.	No exceptions noted.
	Passwords for in-scope system components are configured according to the XYZ's policy, which (a) requires eight-character minimum and 90-day password changes; (b) is complexity enabled; and (c) locks users out of the system after five invalid attempts.	Inspected in-scope system components to determine that passwords were configured according to company policy.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	The configuration management policy requires that all system changes undergo formal documentation, review, and authorization.	Inspected the configuration management policy to determine that all changes to the system are to be configuration controlled, approved, and a risk analysis is performed.	No exceptions noted.
	Databases housing sensitive customer data are encrypted at rest.	Inspected database configurations to determine that databases were encrypted at rest.	No exceptions noted.
	Encryption keys used by integrated services are encrypted themselves with a unique master key.	Inspected the configuration for the encryption process to determine that encryption activities use an acceptable cryptographic algorithm.	No exceptions noted.
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are	Access to in-scope system components requires a documented access request form and manager approval prior to access being provisioned.	Inspected access requests forms for a sample of new hires that received access to the in-scope system components to determine that an access provisioning request was approved prior to access being provisioned.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
removed when user access is no longer authorized.			
	A termination checklist is completed and access is revoked for employees within 24 hours as part of the termination process.	<p>Inspected a listing of terminated employees and compared the listing to the active user listing to determine that terminated employees did not retain access to the in-scope system and platforms after their separation.</p> <p>Inspected termination tickets for a sample of terminated employees during the review period to determine that access was revoked within 24 hours as a part of the termination process.</p>	No exceptions noted.
	Management performs a quarterly access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected access review documentation for sample of quarters to determine that an access review was performed for in-scope system components and that tickets were created to remove inappropriate access.	No exceptions noted.
CC6.3 The entity authorizes, modifies, or removes access to data, software,	Asset owners periodically review access to ensure continued appropriateness.	Interviewed asset owners and inspected documentation to determine that appropriate procedures	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		are in place to remove or modify application access as needed.	
	A termination checklist is completed and access is revoked for employees within 24 hours as part of the termination process.	Inspected a listing of terminated employees and compared the listing to the active user listing to determine that terminated employees did not retain access to the in-scope system and platforms after their separation. Termination tickets for a sample of terminated employees during the review period to determine that access was revoked within 24 hours as a part of the termination process.	No exceptions noted.
	XYZ establishes and administers privileged user accounts in accordance with a role-based access scheme that	Inspected the access control policy to determine that the role-based access scheme was employed to organize	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	organizes information system and network privileges into roles.	information system and network privileges into roles.	
	XYZ tracks and monitors privileged role assignments on a continuous basis through automated mechanisms.	Tested a sample of the automated mechanisms and their configuration settings, alerts, and reports to determine that the mechanisms are operating as intended.	No exceptions noted.
CC6.4 The entity restricts physical access to facilities and protected information assets (for XYZ, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Access to the data centers requires a documented access request form and manager approval prior to access being provisioned.	Inspected access requests forms for a sample of new hires that received access to the data centers to determine that an access provisioning request was approved prior to access being provisioned.	No exceptions noted.
	A termination checklist is completed and access is revoked for employees within 24 hours as part of the termination process.	Inspected a listing of terminated employees and compared the listing to the active user listing to determine that terminated employees did not retain access to the data centers after their separation. Termination tickets for a sample of terminated employees during the	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		review period to determine that access was revoked within 24 hours as a part of the termination process.	
	Access to the data centers is reviewed quarterly by management.	Inspected a sample of physical access reviews completed by management to determine that physical access to the data centers was reviewed on a quarterly basis.	No exceptions noted.
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Formal data retention and disposal procedures are in place to guide the secure disposal of the company's and customers' data.	Inspected data retention and disposal procedures to determine that they were in place.	No exceptions noted.
	Prior to removal from company facilities, all digital media is completely degaussed and sanitized to remove any data and software.	Examined media sanitization records for an agreed-upon sample of digital information system media to be sanitized to determine that measures are being	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		applied to sanitize digital media prior to disposal.	
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	System firewalls are configured to limit unnecessary ports, protocols and services. The only ports open into the environment are defined.	Inspected the firewall configurations and rulesets employed within the environment to determine that the permit rules aligned with the specified networking protocols permitted for inbound network traffic.	No exceptions noted.
	The company has deployed Transport Layer Security (TLS) for transmission of confidential and/or sensitive information over public networks.	Inspected TLS settings to determine that transmission of confidential and/or sensitive information over public networks was encrypted.	No exceptions noted.
	XYZ permits remote access to production systems by authorized employees only with multi-factor authentication (MFA) over encrypted virtual private network (VPN) connection.	Observed a remote login session to determine that MFA VPN was required to access the production network.	No exceptions noted.
	Intrusion detection systems are used to provide continuous monitoring of the XYZ's network and prevention of potential security breaches.	Inspected intrusion detection system configurations to determine that continuous monitoring of the XYZ's network and early prevention of potential security breaches were in place.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The information system restricts the ability of users to transmit, move, or remove system information to other information systems or networks.	Inspected the system and communications protection policy and procedures and associated system configuration settings to determine that the information system restricts the ability of users to transmit, move, or remove system information.	No exceptions noted.
	Secure file transfer protocols (SFTP) are deployed for transmission of confidential and/or sensitive information over public networks.	Inspected SFTP configurations to determine that SFTP was used for the transmission of confidential and/or sensitive information over public networks.	No exceptions noted.
	Removable media to be used for customer or system data is encrypted and sanitized prior to connecting such devices to the information system.	Inspected the information system media protection policy and procedures and media sanitization records to determine that removable media is encrypted and sanitized prior to use.	No exceptions noted.
	Mobile device access to production systems is permitted by authorized devices only with multi-factor authentication	Observed a remote login session to determine that MFA VPN was required to	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	(MFA) over encrypted virtual private network (VPN) connection.	access the production network. Inspected the MFA VPN configurations to determine whether user identification numbers, names, and passwords are required. Observed an employee attempt to access the system through the VPN software and ascertained that user identification numbers, names, and passwords are required to gain access.	
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Only authorized system administrators are able to install software on system devices. Unauthorized use or installation of software is explicitly covered in the employee handbook and Rules of Behavior.	Inspected the rules of behavior and the employee handbook and verified that the policies prohibit installation of software by users, and installation is limited to system administrators.	No exceptions noted.
	The security center monitoring system logs and alerts system administrators of software installation or attempted software installation.	Inspected documentation describing the current configuration settings for a sample of the automated mechanisms to determine that these mechanisms are configured as required. Tested the automated mechanisms and their	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		configuration settings by creating a simulated unauthorized installation to determine that these mechanisms are operating as intended.	
	Formally documented change management procedures (including emergency procedures) are in place to govern the modification and maintenance of production systems and address security and availability requirements.	Inspected the change management procedures to determine that procedures were in place to govern the modification and maintenance of production systems and addressed security and availability requirements.	No exceptions noted.
	Anti-malware technology is deployed for environments commonly susceptible to malicious attack. This software is used to scan assets prior to being placed into production.	Inspected screenshots of anti-malware software configurations (virus definition update, scan schedule, notifications, and evidence that software is deployed on all servers) to determine that anti-virus was updated routinely, logged, and installed on all production servers.	No exceptions noted.
	Logging and monitoring software is used to collect data from system infrastructure components and endpoint systems and used to monitor system performance, potential security threats and vulnerabilities, resource	Inspected installed software inventory for use of logging and monitoring software. For a sample of logging and monitoring software from the inventory, obtained the operations log for a sample date from each sample item selected to	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	utilization, and to detect unusual system activity or service requests.	determine whether the monitoring software was operational.	
<i>System Operations</i>			
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Baseline configurations are retained within the configuration manager tool for roll back capability anytime an approved configuration change is made. Baseline configurations are reviewed and updated annually, when required due to reviews and system changes, and anytime integral system components are added.	Inspected the configuration manager tool to determine that baseline configurations are retained and up to date for applicable system changes.	No exceptions noted.
	An IT infrastructure monitoring tool is utilized to monitor IT infrastructure availability and performance and generates alerts when specific predefined thresholds are met.	Inspected IT infrastructure monitoring tool configurations and an XYZ notification to determine that IT infrastructure monitoring tools were utilized to monitor IT infrastructure availability and performance and generated alerts when specific predefined thresholds were met.	No exceptions noted.
	XYZ utilizes a configuration monitoring tool that notifies	Inspected alert configurations settings and an XYZ alert to	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	management of changes to production system.	determine that a configuration monitoring tool monitored and alerted management of changes to production.	
	Automated mechanisms are used to continuously detect the addition of unauthorized components/devices into the system. The configuration monitoring tool logs all changes in status to network switch ports. Any attempt to insert or install a component immediately sends an alert to the monitoring tool and creates a ticket.	Inspected configuration settings for the monitoring tool and an XYZ alert to determine that a configuration monitoring tool monitored and alerted management of any unauthorized components.	No exceptions noted.
	Internal and external network vulnerability scans are performed quarterly. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected internal and external vulnerability scans for a sample of quarters to determine that internal and external vulnerability scans were performed quarterly and remediation plans were developed to remediate all critical and high vulnerabilities.	No exceptions noted.
CC7.2 The entity monitors system components and the operation of those components for anomalies that	User entities are provided with instructions for communicating potential security breaches to the information security team.	Inspected the instructions provided to user entities to determine whether they include protocols for	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		communicating potential security breaches.	
	When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures.	Inspected the written incident management procedures to determine whether the procedures include a process for handling the security incident.	No exceptions noted.
	Security incidents are reported to the help desk and tracked through to resolution. Incidents that may affect security compliance are reported to the security compliance officer.	<p>Selected a sample of security incidents logged in the incident tracking system and inspected documentation to determine whether the incident was tracked within a help desk ticket until resolution.</p> <p>Inspected a sample of security incidents logged in the incident tracking system and associated communications to the</p>	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		security officer that may affect security compliance to determine whether the incidents were reported to the security officer.	
	Intrusion detection systems are used to provide continuous monitoring of the XYZ's network and prevention of potential security breaches.	Inspected intrusion detection system configurations to determine that continuous monitoring of the XYZ's network and early prevention of potential security breaches were in place.	No exceptions noted.
	All incidents related to security are logged, tracked, and communicated to affected parties by management until resolved.	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No exceptions noted.
	A risk assessment is performed on at least an annual basis. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments, policies, and procedures are	Inspected the most recent risk assessment to determine that threats and changes were formally identified and assessed on an annual basis.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	identified and the risks are formally assessed.		
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	<p>XYZ has developed security incident response policies and procedures that are communicated to authorized users.</p> <p>A risk assessment is performed on at least an annual basis. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments, policies, and procedures are identified and the risks are formally assessed.</p>	<p>Inspected incident response policies and procedures to determine that an incident response plan was documented and communicated to authorized users.</p> <p>Inspected the most recent risk assessment to determine that threats and changes were formally identified and assessed on an annual basis.</p>	No exceptions noted.
	All incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved.	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No exceptions noted.
	A technician or administrator responsible for security incident tickets follows a process of analyzing the security	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	incident. The process begins with detailing what specific attack occurred, which system(s) were affected and what happened during the attack. Next the root cause is determined and the event is given a classification to assign the level of impact of the event. The impact level is based on guidelines detailed in the procedures.	authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Management has established defined roles and responsibilities to oversee implementation of information security policies including incident response.	Inspected security policies to determine the company has established defined roles and responsibilities to oversee implementation of the incident response plan.	No exceptions noted.
	After an incident has been confirmed, specific personnel are engaged in the containment process to reduce the magnitude of the incident.	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by authorized personnel, threats are mitigated,	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	
	The containment phase ensures that all other interconnections to the system were not affected by the security incident.	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No exceptions noted.
	An assessment of the incident response to better handle future incidents is performed through analysis after-action reports or the mitigation of exploited vulnerabilities to prevent similar incidents in the future.	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No exceptions noted.
	Daily incremental and weekly full backups are configured for the databases.	Observed backup configuration to determine that daily incremental and weekly full backups were	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		configured for the databases.	
	All incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved.	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No exceptions noted.
	Internal and external network vulnerability scans are performed quarterly. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected internal and external vulnerability scans for a sample of quarters to determine that internal and external vulnerability scans were performed quarterly and remediation plans were developed to remediate all critical and high vulnerabilities.	No exceptions noted.
	A risk assessment is performed on at least an annual basis. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments, policies, and procedures are identified and the risks are formally assessed.	Inspected the most recent risk assessment to determine that threats and changes were formally identified and assessed on an annual basis.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	XYZ incorporates lessons learned from ongoing incident response activities into incident response procedures accordingly. If changes are required, necessary changes are made to the policy and procedures and redistributed according to all responsible organizations and key personnel.	Inspected the incident response plan to determine that the document has been reviewed and revised every year and changes were incorporated from prior incidents and associated lessons learned.	No exceptions noted.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.	Software updates related to flaw remediation are tested for effectiveness and potential side effects on the system before installation. All software updates and patches are tested by creating a virtual instance of the environment and running the tests associated with the software update and/or patch. An ability to rollback is implemented during software updates and/or patching.	Inspected the configuration management policy to determine that all changes including patches/updates are configuration controlled through virtual instance testing and rollback capability. Inspected a sample of patch updates to determine that patches were tested in accordance with the configuration management policy prior to being placed into production.	No exceptions noted.
	All incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved.	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by authorized personnel, threats are mitigated,	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	
	A technician or administrator responsible for security incident tickets follows a process of analyzing the security incident. The process begins with detailing what specific attack occurred, which system(s) were affected and what happened during the attack. Next the root cause is determined and the event is given a classification to assign the level of impact of the event. The impact level is based on guidelines detailed in the procedures.	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No exceptions noted.
	An assessment of the incident response to better handle future incidents is performed through analysis after-action reports or the mitigation of exploited vulnerabilities to prevent similar incidents in the future.	Inspected a sample of IT security incident tickets to determine that an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		after-action report was prepared.	
	XYZ incorporates lessons learned from ongoing incident response activities into incident response procedures accordingly. If changes are required, necessary changes are made to the policy and procedures and redistributed according to all responsible organizations and key personnel.	Inspected the incident response plan to determine that the document has been reviewed and revised every year and changes were incorporated from prior incidents and associated lessons learned.	No exceptions noted.
	Annual testing of the incident response plan is performed using tabletop exercises and simulations to ensure the incident response procedures are up-to-date and accurate. When updating the incident response plan, lessons learned from tabletop exercises are used to implement changes to reflect effective procedures when handling incidents.	Inspected documentation for the most recent incident response plan review to determine that the plan was tested within the past year, and that drills conducted to imitate incidents were resolved and service availability was restored. Inspected the incident response plan for revision because of the testing performed.	No exceptions noted.
	XYZ has a formalized security and systems development methodology that includes project planning, design, testing, implementation, maintenance, and	Inspected the security and systems methodology policy to determine whether it includes project planning, design, testing, implementation, maintenance, and	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	disposal or decommissioning.	disposal or decommissioning.	
	Security administration team approval of changes is required prior to implementation.	Inspected change documentation from system-generated list of system changes to determine whether the changes were approved by security administration prior to implementation.	No exceptions noted.
<i>Change Management</i>			
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	XYZ has adopted a formal systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology requirements.	Inspected the systems development life cycle (SDLC) methodology to determine that it governed the development, acquisition, implementation, and maintenance of computerized information systems and related technology requirements.	No exceptions noted.
	XYZ's software and infrastructure change management process requires that change requests are: <ul style="list-style-type: none"> • Authorized • Formally documented 	Inspected a sample of change requests to determine that changes were: <ul style="list-style-type: none"> • Authorized • Formally documented 	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	<ul style="list-style-type: none"> • Tested prior to migration to production • Reviewed and approved 	<ul style="list-style-type: none"> • Tested prior to migration to production • Reviewed and approved • Tracked through completion 	
	Formally documented change management procedures (including emergency procedures) are in place to govern the modification and maintenance of production systems and address security and availability requirements.	Inspected the change management procedures to determine that procedures were in place to govern the modification and maintenance of production systems and addressed security and availability requirements.	No exceptions noted.
	XYZ requires all changes, including maintenance activities, to be documented in the help desk application and tracked from initiation through deployment and validation.	<p>Inspected a sample of change requests to determine that changes were:</p> <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Reviewed and approved • Tracked through completion 	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	Internal and external network vulnerability scans are performed quarterly. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected internal and external vulnerability scans for a sample of quarters to determine that internal and external vulnerability scans were performed quarterly and remediation plans were developed to remediate all critical and high vulnerabilities.	No exceptions noted.
	Baseline configurations are retained within the configuration manager tool for roll back capability anytime an approved configuration change is made. Baseline configurations are reviewed and updated annually, when required due to reviews and system changes, and anytime integral system components are added.	Inspected the configuration manager tool to determine that baseline configurations are retained and up to date for applicable system changes.	No exceptions noted.
	XYZ maintains a documented change management and patch management process.	Inspected the change and patch management policies to determine whether there are documented policies and procedures.	No exceptions noted.
	Servers are reviewed monthly by the security administration team to determine if required vendor security patches have been applied by comparing patches	For a sample of months, inspected management's server review documentation to determine whether the security administration team had completed the	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	applied per system configuration reports to the vendor's list of current patches released.	review of the patches applied to the vendor's list of current patches released. For any missing patches identified, inspected the change request created by the security administration team and the change record to ascertain that the identified patches were applied.	
	XYZ contracts with third parties to conduct monthly security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management. Management develops a plan of action for each recommendation and follows up on open recommendations monthly.	For a sample of months, inspected the security review and vulnerability assessment reports to determine whether the assessments were performed, communicated, and addressed by management.	No exceptions noted.
	XYZ prepares a root cause analysis for high severity incidents. Based on the root cause analysis, change requests are prepared, and XYZ's risk management process and relevant risk management data is updated to reflect the	Inspected the root cause analysis for high severity incidents to determine whether the risk management process and relevant risk management data was updated to reflect the planned incident response.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	planned incident response.		
	XYZ maintains a formally documented change management process. Changes to hardware, operating system, and system software are authorized, tested (when applicable), and approved by appropriate personnel prior to implementation.	<p>Inspected the change management policy for hardware, operating system, and system software to determine whether procedures are formally documented, including procedures over authorization, testing (when applicable), and approval prior to implementation.</p> <p>Inspected change documentation from system-generated list of system changes to determine whether the changes were authorized, tested, and approved prior to implementation.</p>	No exceptions noted.
	Changes to system infrastructure and software are developed and tested in a separate development or test environment before implementation. Additionally, developers do not have the ability to migrate changes into production environments.	<p>Inspected documentation of the system infrastructure architecture to determine whether a separate development or test environment existed from the production environment.</p> <p>Inspected the access list to the change management tools to determine whether access to migrate changes to production</p>	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		<p>was appropriate based on job responsibilities and that developers did not have the ability to migrate changes into production.</p> <p>Inspected change documentation from system-generated list of system changes to determine whether the changes were authorized, tested, and approved prior to implementation.</p>	
	Emergency changes follow the standard change management process but at an accelerated timeline. Prior to initiating an emergency change, all necessary approvals are obtained and documented.	Inspected change documentation from system-generated list of program changes for a sample of emergency changes to determine whether the changes were approved.	No exceptions noted.
<i>Risk Mitigation</i>			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. Inspected	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	<p>A risk assessment is performed on at least an annual basis. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments, policies, and procedures are identified and the risks are formally assessed.</p> <p>The risk management program includes the use of insurance to minimize the financial impact of any loss events.</p>	the most recent risk assessment to determine that threats and changes were formally identified and assessed on an annual basis.	
CC9.2 The entity assesses and manages risks associated with vendors and business partners.	The risk management program includes the use of insurance to minimize the financial impact of any loss events.	Inspected the risk management policy to determine that the program includes cyber insurance for potential loss events.	No exceptions noted.
	Formal information sharing agreements are in place with related parties and vendors. These agreements include the scope of services and security commitments applicable to that entity.	Inspected contracts for a sample of new vendors added during the audit period to determine that agreements included scope of services and security commitments.	No exceptions noted.
	A vendor risk assessment is performed for all vendors on an annual basis that have access to confidential data or	Inspected vendor risk assessment documentation for a sample of vendors to determine that a risk	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	impact the security of the system.	assessment was performed within the past year.	
	Management has established defined roles and responsibilities to oversee implementation of information security policies.	Inspected security policies to determine XYZ has established defined roles and responsibilities to oversee implementation of information security policies.	No exceptions noted.
	XYZ has documented and communicated security policies that define the information security rules and requirements for the service environment.	Inspected the security policies to determine that they address applicable information security requirements including communication of service issues. Observed the XYZ's intranet to determine that security policies are published and communicated to employees and relevant third parties.	No exceptions noted.
	An annual risk assessment is performed by management and includes the following: a. Determining business objectives, entity, subsidiary, division, operating unit, and functional levels b. Evaluating the effect of environmental,	Inspected the annual risk assessment documentation to determine whether they included the significant aspects of operations.	No exceptions noted.

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
	<p>regulatory, and technological changes on the TMS system security</p> <p>c. Involving appropriate levels of management.</p> <p>d. Analyzing risks associated with the threats</p> <p>e. Identifying threats to operations, including security threats, using information technology asset records</p> <p>f. Identifying threats to operations, including threats from vendors, business partners, and other parties</p> <p>g. Determining a risk mitigation strategy</p>		
	<p>XYZ has clauses in its agreements with vendors and business partners to terminate relationships when necessary. Vendor and business partner access is removed upon termination through a termination checklist and access is revoked within 24 hours as part of the termination process.</p>	<p>Inspected a listing of terminated vendors and compared the vendor employee listing to the active user listing to determine that terminated vendor employees did not retain access to the in-scope system and platforms after their separation.</p> <p>Inspected termination tickets for a sample of terminated vendors</p>	<p>No exceptions noted.</p>

<i>Trust Services Criteria for the Security Category</i>	<i>Description of XYZ Service Organization's Controls</i>	<i>Service Auditor's Tests of Controls</i>	<i>Results of Service Auditor's Tests of Controls</i>
		during the review period to determine that vendor employee access was revoked within 24 hours as a part of the termination process.	

Section 5—Other Information Provided by Example Service Organization That Is Not Covered by the Service Auditor's Report

Note to Readers: *The service organization may wish to attach to the description of the service organization's system, or include in a document containing the service auditor's report, information in addition to its description. The following are examples of such information:*

- *Future plans for new systems*
- *Other services provided by the service organization that are not included in the scope of the engagement*
- *Qualitative information, such as marketing claims, that may not be objectively measurable*
- *Responses from management to deviations identified by the service auditor when such responses have not been subject to procedures by the service auditor*

For brevity, an example is not provided.