



Internet Gaming/Internet Sports Betting

TECHNICAL SECURITY STANDARDS (CONTROLS) QUESTIONNAIRE
--

General Instructions and Definitions:

1. This questionnaire is designed to capture information relevant to the adoption, implementation, and maintenance of technical security standards (controls) by an internet gaming/sports betting operator and its internet gaming/internet sports betting platform provider, as required in the following administrative rules:
 - a. Internet Gaming Rule: **R 432.639**
 - b. Internet Sports Betting Rule: **R 432.739**
2. This questionnaire must be completed by an internet gaming/sports betting operator and its internet gaming/internet sports betting platform provider and submitted to the Michigan Gaming Control Board (board) with each internet gaming platform and/or internet sports betting platform submission.
3. An internet gaming/sports betting operator may complete a single questionnaire for multiple platforms, including one or both of its internet gaming platforms and its internet sports betting platform, but only if they are provided by the same internet gaming/internet sports betting platform provider.
4. This questionnaire must be completed in its entirety. Any items that are not applicable may be answered with "N/A" or left blank.
5. If information or documentation requested in this questionnaire has already been provided to the board (in an internal control system submission, for example), the information or documentation does not need to be restated or provided again. Instead, provide a reference to where the requested information or documentation can be found.
6. If multiple internet gaming/internet sports betting platforms are included in a single questionnaire, responses must differentiate those applications, software, hardware, technologies, or procedures which are unique to each platform. If an application, software, hardware, technology, or procedure is common to multiple platforms, then identify it accordingly.
7. Provide as much detail as possible for each platform covered in this questionnaire. Include the name of each specific platform, version number, and other uniquely identifying information.
8. Be sure to identify those services, processes, functions, or controls being provided by a third party such as data center services, cloud services, security, etc.
9. Provide copies of relevant audits, certifications, and other attestations for each platform or any third party providing services related to each platform.
10. If a service, process, function, or control has not yet been implemented, describe how you intend to implement or comply with the service, process, function, or control.

11. Definitions:

- a. "Internet Gaming Platform" means all hardware, software, firmware, communications technology, and other equipment as defined in Internet Gaming Rule **R 432.611(m)**.
- b. "Internet Sports Betting Platform" means all hardware, software, firmware, communications technology, and other equipment as defined in Internet Sports Betting Rule **R 432.711(i)**.
- c. "Third Party" means a person other than an internet gaming/sports betting operator or internet gaming/internet sports betting platform provider, including an internet gaming/sports betting supplier, vendor, or other third-party service provider.

1. Information Security Policy

- a. Provide a copy of your information security policy governing the internet gaming/internet sports betting platform and related data.
- b. How often is it reviewed and updated by management.
- c. Does your information security policy delineate the responsibilities of the internet gaming/sports betting operator, internet gaming/internet sports betting platform provider, and all third parties responsible for the operation, service, or maintenance of the internet gaming/internet sports betting platform (e.g., data center or cloud service providers)?
- d. Have you submitted to the board a copy of your internal control systems incorporating the technical and security standards (controls) for each applicable platform per the specific referenced administrative rule:
 - i. Internet Gaming Rule: **R 432.639**
 - ii. Internet Sports Betting Rule: **R 432.739**
- e. If not already submitted, provide a copy of the technical security standards (controls) for each applicable platform per the administrative rules listed above.

2. Internet Gaming/Internet Sports Betting Platform IT Security Audits

- a. Is the internet gaming/internet sports betting platform in compliance with any of the following standards for information security management:
 - i. SOC 2, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, PCI, NIST, Fedramp, World Lottery Association Security Controls, or similar standards.
- b. Describe the process to audit the internet gaming/internet sports betting platform at all locations where sensitive information or critical components are accessed, processed, transmitted, or stored.
- c. Explain how the audit process involves third-party data centers or cloud service providers (if applicable).
- d. Provide a copy of the full report for each of the most recent IT security audits performed on your internet gaming/internet sports betting platform, including audits performed for third parties such as data centers or cloud service providers.
- e. Provide copies of any other reports, certifications, or attestations regarding the IT security controls for your internet gaming/internet sports betting platform, including reports, certifications, or attestations prepared by or for third parties such as data centers or cloud service providers.

3. Location of Servers for Internet Gaming/Internet Sports Betting Platform

- a. Provide detailed information regarding the planned physical location of the servers, storage devices, network communication devices, and all other components of the internet gaming/internet sports betting platform. Include those housed in or by data centers and cloud service providers.

- b. Where will servers storing operating system recovery and platform data back-ups be located?
- c. Where will servers storing replicated platform data or an enterprise data warehouse be located?

4. Physical Security Controls of IT Assets

- a. Will you be using a data center or cloud service provider to house the IT assets of the internet gaming/internet sports betting platform? Provide the name of the data center or cloud service provider.
- b. Describe how the IT assets of the internet gaming/internet sports betting platform will be housed in a secure manner in order to prevent unauthorized physical access and damage from environmental factors, natural disasters, and fire.
- c. Provide details regarding physical security controls such as fencing, secure doors, mantraps, badge readers, PIN pads, biometrics, keys, etc.
- d. Describe what happens if a door is forced open to a secured area.
- e. How is physical access to the facility housing internet gaming/internet sports betting platform equipment granted, tracked, and monitored to ensure only appropriate and authorized personnel have access?
- f. Describe how entry into the IT room housing internet gaming/internet sports betting platform equipment is logged and how long these records are retained.
- g. How are unauthorized access events detected, logged, and investigated?
- h. If using a data center or cloud service provider to house internet gaming/internet sports betting platform equipment, would data center or cloud service provider staff have physical access to this equipment? Please explain.
- i. Describe the procedures for requesting data center or cloud service provider staff to service, install, or in any other way access your IT equipment for the internet gaming/internet sports betting platform. Include in your response:
 - i. How long any service requests with the data center or cloud service provider are retained.
 - ii. A list of typical tasks that data center or cloud service provider staff might be expected to perform on your behalf.

5. Camera Surveillance of Internet Gaming/Internet Sports Betting Platform Equipment

- a. Describe how surveillance coverage is used to protect the IT assets of the internet gaming/internet sports betting platform.
- b. How long is surveillance footage retained until deleted?
- c. Are all entrance and exit points covered by surveillance?
- d. Is the IT room housing internet gaming/internet sports betting platform equipment covered by surveillance?
- e. Is the surveillance system backed up? If yes, where and for how long?

6. Logical Access Control

- a. Describe how employee access to the critical components of the internet gaming/internet sports betting platform is secured against unauthorized access through the use of authentication credentials such as passwords, digital certificates, PINs, biometrics, multi-factor authentication, and other methods.
- b. Where passwords are used as an authentication credential for critical components of the internet gaming/internet sports betting platform, describe the password management processes and controls in place to enforce such items as password complexity, forced password changes, failed log-in attempts, etc.

- c. Describe the request management process to grant access to the critical components of the internet gaming/internet sports betting platform for employees. Be sure to include the names of any applications used to record, grant, and track user access to the internet gaming/internet sports betting platform.
- d. How long are records regarding access to the internet gaming/internet sports betting platform retained?
- e. Describe the process to review user accounts to ensure that each employee's access to the internet gaming/internet sports betting platform is appropriate and maintains segregation of duties.
- f. How often is the above review conducted and by whom?
- g. Describe the process for removing user account access to the internet gaming/internet sports betting platform when an employee transfers to a new position or their employment is terminated?
- h. Is the process for granting logical access different for third parties?
- i. Describe how all attempts, successful and unsuccessful, to log into the critical components of the internet gaming/internet sports betting platform are recorded in a secured log.
- j. Are utility programs which are capable of overriding application or operating systems controls used in your operating environment? If so, how are they regulated and implemented to prevent unauthorized use?
- k. If using a data center or cloud service provider to house internet gaming/sports betting platform equipment, would data center or cloud service provider staff have logical access to this equipment? Please explain.

7. Asset Management

- a. Do you have an acceptable use policy regarding the use of IT assets for the critical components of the internet gaming/internet sports betting platform? How are employees trained on this policy? Attach a copy of the policy.
- b. Describe your processes for ensuring an accurate inventory of all critical components of the internet gaming/internet sports betting platform in which all IT assets are accounted for and have a designated owner or management official that is responsible for each IT asset.
- c. Describe the procedures to ensure each designated IT asset owner or management official properly classifies information and IT assets in terms of criticality, sensitivity, and value.
- d. Describe your processes for the removal of old IT assets and the adding of new IT assets to the internet gaming/internet sports betting platform.
- e. How often are inventories conducted on all critical components of the internet gaming/internet sports betting platform?
- f. Describe the processes to decommission hardware components, storage media, removable memory devices, and other media are disposed of securely to prevent unauthorized access to data.

8. Communication Standards

- a. Describe the controls that are in place to ensure the integrity and confidentiality of all individual and authorized participant communications and ensure the proper identification of the sender and receiver of all communications.
- b. Does the internet gaming/internet sports betting platform perform communications across a public or third-party network? If so, describe how the platform either encrypts the data packets or utilizes a secure communications protocol to ensure the integrity and confidentiality of the transmission.

- c. Describe in detail the secure method utilized by the internet gaming/internet sports betting platform in regard to communications that contain internet wagering/internet sports betting account numbers, user identification, passwords or PINs, individual or authorized participant data, sensitive information, wagers or results, financial information, or individual or authorized participant transaction information.
- d. Describe how the internet gaming/internet sports betting platform ensures secure communications between individual or authorized participant devices and the platform.

9. IT Security Assessments and Penetration Testing

Security Assessment

- a. How often are IT security assessments performed on the internet gaming/internet sports betting platform?
- b. Provide a copy of the results of the most recent vulnerability assessment performed on the internet gaming/internet sports betting platform.
- c. Describe the procedures, process, and tools used to perform an IT security assessment to identify and evaluate potential vulnerabilities which may put the security and operational integrity of the internet gaming/internet sports betting platform at risk, including but not limited to:
 - i. Port scanning.
 - ii. Identification of devices, operating systems, protocols, and services in use.
 - iii. Web scanning using an HTTP and HTTPS vulnerability scanner.
 - iv. Missing OS and application patches and improperly configured software and services.
 - v. Outdated versions of operating systems and third-party applications.
 - vi. External vulnerabilities, including all external facing servers and network resources from which sensitive information may be obtained.
 - vii. Internal vulnerabilities, including all internal facing servers and network resources from which sensitive information may be obtained.

Penetration Testing

- d. Describe how IT penetration testing is used on internal, external, and wireless networks to test if potential vulnerabilities are susceptible to exploitation.
- e. Describe how IT penetration testing is used to identify and test potential vulnerabilities in applications using both authenticated and unauthenticated scans.
- f. Describe how the results of assessments are reviewed by management for corrective action and remediation of identified vulnerabilities.
- g. Provide a copy of the results of the most recent IT penetration test performed on the internet gaming/internet sports betting platform.

10. Network Cyber Security of Internet Gaming/Internet Sports Betting Platform

- a. Describe how the internet gaming/internet sports betting platform network security controls will authenticate all users on the network. Attach a network diagram showing firewalls, routers, NIDs, servers, and other relevant components of the internet gaming/internet sports betting platform.
- b. Describe how the internet gaming/internet sports betting platform network security controls will encrypt all network management communications.
- c. Describe the redundant features of the network so that the failure of a single router, server, or any other device does not result in a denial of service.
- d. Describe how network intrusion detection (NIDs) or network intrusion prevention (NIPs) devices and solutions are deployed throughout the network and monitor all communication to detect or prevent malicious attacks or unauthorized access, including but not limited to:

- a. Distributed Denial of Service DDOS attacks.
- b. Shellcode from traversing the network.
- c. Spoofing attacks
- d. Man-in-the-Middle attacks
- e. Describe how NIDs, NIPs, or other devices and technologies are deployed on your WLAN network to scan and detect any unauthorized or rogue devices or access points and disable them.
- f. Do you have applications or software tools which are able to maintain a log of all wireless access for at least 90 days, including information on the wireless devices involved which can be reconciled to an inventory of all networking devices on the internet gaming/internet sports betting platform?
- g. Describe the process for reviewing the WLAN controls and procedures to ensure security and integrity.
- h. Describe how anti-virus scanning solutions are deployed on critical components of the internet gaming/internet sports betting platform, including the name of the products used.
- i. Describe the procedures that ensure all changes to the networking infrastructure are logged.
- j. Are stateless protocols such as UDP (user datagram protocol) used in the transmission of sensitive data? If yes, how are they deployed in order to ensure data security?
- k. Are virtualized environments deployed in your network and if so, are they deployed in a manner so that redundant systems are not using the same hypervisor as the primary system?
- l. Describe how all networking hubs, services, and connection ports are secured to prevent unauthorized access, including unused services and ports.
- m. Describe how network communication equipment (NCE) for the internet gaming/internet sports betting platform is constructed in a way as to resist physical damage to the hardware or corruption of the contained firmware/software by normal usage.
- n. Describe how network communication equipment (NCE) is physically secured from unauthorized access at all locations, including third-party data centers or cloud service providers.
- o. Describe how network communication equipment (NCE) is logically secured from unauthorized access at all locations, including third-party data centers or cloud service providers.
- p. Describe your procedures to investigate, document, and resolve malfunctions including:
 - a. Determination of the cause of the malfunction.
 - b. Review of relevant records, reports, logs, and surveillance records.
 - c. Repair or replacement of the critical components.

11. Remote Access

- a. Describe the process to grant, rescind, and record remote access to the internet gaming/internet sports betting platform by employees and third parties.
- b. Are records for requests to grant, modify, or disable remote user access retained electronically? If so, for how long?
- c. How is remote access controlled so that a remote user only has access to those applications, servers, or other IT resources necessary for them to perform their job? Be sure to include the name of any utility or application used to assign permissions.
- d. Describe how remote access to internet gaming/internet sports betting platform resources is achieved in a secure manner.
- e. Describe the processes and procedures used to manage third party or guest accounts used for remote access to internet gaming/internet sports betting platform components.
- f. Are third party or guest remote access accounts disabled when not in use?
- g. How are third party or guest remote access accounts restricted so that they may only access those applications, servers, and other network resources which they are authorized to support?

- h. Is the remote access application able to capture and log remote session information including log-in name, host IP addresses, port numbers, protocols, and MAC addresses?
- i. Is the remote access application able to capture and log the time, date, and duration of the remote access session?
- j. Is the remote access application able to capture and log the remote user activity, resources accessed, and changes made? Please describe.

12. Environmental Controls and Power Capabilities for the Internet Gaming/Internet Sports Betting Platform

- a. Describe the controls, tools, and processes deployed to protect the IT assets of the internet gaming/internet sports betting platform from electrical, environmental, and fire hazards. Identify where third parties such as data centers or cloud service providers are responsible for the controls or services.
- b. Is your IT room housing internet gaming/internet sports betting platform equipment compliant with any of the following standards: SOC 2, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, NIST, or PCI? Provide a copy of the report from the most recent audit performed.

Electrical

- c. What is the level of electrical redundancy provided for the IT assets of the internet gaming/internet sports betting platform? i.e. N, N+1, 2n, etc.
- d. How many generators does the facility housing internet gaming/internet sports betting platform equipment have?
- e. How long can these generators run at full load before requiring refueling?
- f. Do you have a service level agreement for fuel delivery services for generators? If so, what is it?
- g. How often are the generators serviced and tested?
- h. What is the service level agreement for emergency generator service?
- i. Is generator testing done under full load conditions?
- j. What is the level of UPS redundancy provided for the IT assets of the internet gaming/internet sports betting platform? i.e. N, N+1, 2n, etc.
- k. Are equipment racks and cages configured with redundant electrical power supplies, including redundant UPS and generator service?
- l. Does the electrical power capacity in the facility housing internet gaming/internet sports betting platform equipment allow for future increase of electrical needs?

Environmental/HVAC

- m. What level of redundancy does the facility housing internet gaming/internet sports betting platform equipment have for the HVAC system? i.e. N, N+1, N+2, etc.
- n. How many cooling units are in use in the facility housing internet gaming/internet sports betting platform equipment?
- o. Is there a service level agreement for emergency service? What is it?
- p. How often are the HVAC systems inspected and serviced?
- q. Does the facility housing internet gaming/internet sports betting platform equipment use a raised floor design?

Fire Detection and Suppression

- r. What sort of fire suppression system is deployed in the facility housing internet gaming/internet sports betting platform equipment? i.e. FM 200, water system, dry pipe, etc.
- s. Is there a service level agreement for emergency service? What is it?
- t. How are staff trained in the use of manual fire suppression systems, alarms, extinguishers, etc.?

- u. How are smoke detectors deployed in the facility housing internet gaming/internet sports betting platform equipment to account for venting and air circulation factors?

13. Business Continuity and Disaster Recovery Planning

- a. Do you have a business continuity and disaster recovery plan in place? Provide a copy of this plan.
- b. Describe how your business continuity and disaster recovery plan will recover internet gaming/internet sports betting operations if it is rendered inoperable.
- c. Does your disaster recovery plan include a site for recovery which is separated from the production site?
- d. How does your method of storing individual or authorized participant, wagering, and other platform data minimize loss in the event of a disaster? Describe this process.
- e. Does your disaster recovery plan contain detailed steps or metrics required to re-establish internet gaming/internet sports betting operations? Please describe.
- f. How often is the business continuity and disaster recovery plan reviewed for appropriateness and tested?
- g. Does your disaster recovery plan include contingencies for incidents related to natural disasters, man-made events, civil unrest, and cyber-attacks?

14. Use of Third-Party Services

- a. Identify and explain how any third-party services are implemented into your internet gaming/internet sports betting platform, including but not limited to geolocation services, patron loyalty programs, financial services, identity verification services, cloud services, virtualization services, and data center services.
- b. Provide copies of the most recent compliance audit completed for any third-party entity providing any of the above services, including such audits as:
 - i. SOC 2, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, PCI, NIST, Fedramp, or World Lottery Association Security Controls.
- c. Describe how the security and responsibilities of third-party services within the internet gaming/internet sports betting platform are defined and documented.
- d. Describe the policies and procedures for managing and monitoring third-party services to ensure adherence to relevant security requirements, including but not limited to:
 - i. Agreements involving accessing, processing, communicating, or managing the internet gaming/internet sports betting platform and its components.
 - ii. Process for the regular review of services, reports, and records provided by third parties.
 - iii. Process for managing changes to the provisions of third-party service agreements, including security policies, procedures, and controls.
 - iv. Access rights of third-party service providers to the internet gaming/internet sports betting platform including granting, modifying, or disabling due to termination or job change.
- e. Are the services, reports, records, or SLAs provided by a third party monitored and reviewed by management on a routine basis? If so, how often?

15. Internet Gaming/Internet Sports Betting Platform Data: Integrity, Data Backup and Recovery Process

- a. Describe your procedures and controls for securing the data for the critical components of the internet gaming/internet sports betting platform, including accounting, reporting, significant event, and other sensitive data, against alteration, tampering, or unauthorized access.
- b. How are data handling methods implemented to achieve input validation and rejection of corrupted data?

- c. Describe how encryption or other equivalent security measures are used to secure data files and directories of the internet gaming/internet sports betting platform.
- d. If data encryption is not used, describe those processes used to restrict users from accessing the content of data files and directories based upon segregation of duties or responsibilities and how this access is monitored and recorded.
- e. Describe how production databases containing internet gaming/internet sports betting platform data are separated on the network from servers hosting user interfaces.
- f. Describe how supervised access controls are used to restrict the alteration of any accounting, reporting, or significant event data and how system logging captures the following information regarding any changes to data:
 - i. Unique ID number for the alteration.
 - ii. Data element altered.
 - iii. Data element value prior to alteration.
 - iv. Data element value after alteration.
 - v. Time/date of the alteration.
 - vi. Personnel that performed alteration (user identification).
- g. Describe the backup process including the frequency of full, incremental system backups.
- h. Describe how audit logs, databases, and all other internet gaming/internet sports betting platform data is stored to protect integrity and availability of the data in the event of a failure.
- i. How are redundant platform components or data copies used for backups and restoration so that a single failure of any portion of the internet gaming/internet sports betting platform would not result in loss or corruption of data?
- j. Describe the procedures, processes, and location for storing the backup copies or backup media of the internet gaming/internet sports betting platform in a physically separate location from the location housing the servers and data which are being backed up.
- k. Describe how this separate location is secured to prevent unauthorized access and provide adequate protection to prevent the permanent loss of any data. Include in your response any use of third-party entities such as data centers, cloud service providers, or a secured storage facility.
- l. Describe your procedures and processes, in the event of a complete and unrecoverable failure of the internet gaming/internet sports betting platform, to restore operations from the last backup point and fully recover all systems and data including, but not limited to:
 - i. All information specified under the board's administrative rules, technical standards and bulletins, and internal controls of the internet gaming/sports betting operator and internet gaming/internet sports betting platform provider.
 - ii. Current encryption keys.
 - iii. All other parameters, modifications, reconfigurations, additions, merges, deletions, adjustments, and parameter changes of the internet gaming/internet sports betting platform.

16. Domain Name Service (DNS) Requirements

- a. Do you employ a primary as well as a secondary DNS server?
- b. Describe how you have secured the primary DNS server and the secondary DNS servers so that they are both logically and physically separated from one another.
- c. Describe the controls to ensure logical and physical access to the DNS servers is restricted to authorized staff.
- d. Explain how zone transfers to arbitrary hosts will be disallowed.
- e. Explain how a registry lock will be implemented to ensure any requests to change DNS servers will need to be verified manually.

- f. Describe the method to prevent cache poisoning on the DNS servers.

17. Cryptographic Controls

- a. Describe how policies, controls, and technologies are developed and deployed to protect sensitive information of the internet gaming/internet sports betting platform, including but not limited to the following:
 - i. How individual, authorized participant, or sensitive internet gaming/internet sports betting platform data is encrypted if it travels across a network with lower level of trust.
 - ii. Explain the message authentication technique used for data which must be authenticated.
 - iii. What organization issues the security certificate used for authentication?
 - iv. Describe the process and procedures to periodically review encryption algorithms to ensure they are effective and, if need be, replaced or updated.

18. Encryption Key Management

- a. Describe your procedures for obtaining, generating, storing, and revoking encryption keys.
- b. Describe your procedures for changing existing encryption keysets.
- c. What is the process for recovering data which has been encrypted with a revoked or expired encryption key after the encryption key becomes invalid?

19. Firewall Implementation

- a. Describe how firewalls are deployed and implemented in such a way as to secure communications traffic to and from the internet gaming/internet sports betting platform network.
- b. Does a firewall exist at the boundary of any dissimilar security domains?
- c. Describe the controls in place to ensure no device on the same broadcast domain as the platform host may establish a network path which bypasses the firewall.
- d. Are all redundant network paths configured in such a way as to require the connection to pass through at least one application level firewall?
- e. Describe the procedures to ensure only firewall related applications have been installed on the firewall.
- f. Describe the controls to ensure only authorized system administrator accounts may be present on the firewall.
- g. Describe the controls to reject all connections except those which have been specifically approved.
- h. Describe how firewalls are configured to reject connections from destinations which cannot reside on the network from which the message originated.
- i. Is the firewall application able to maintain an audit log to capture such events as:
 - i. Configuration changes to the firewall.
 - ii. Successful and unsuccessful connection attempts through the firewall.
 - iii. Source and destination IP addresses, port numbers, protocols, and where possible MAC addresses.
- j. Will the firewall application disable all communications and generate an error if the audit log becomes full?
- k. Describe the process to review the firewall configuration and rules to ensure the operating condition of the firewall and the effectiveness of the rule sets.
 - i. Is the process conducted for all internal and external firewalls?
 - ii. How often is this review conducted?

20. Internet Gaming/Internet Sports Betting Platform Change Control Procedures

- a. Describe the change control process to ensure that only authorized versions of all hardware, software, and internet games are implemented into the production environment.
- b. Describe your version control processes to ensure all software, source code, and hardware implemented for the production environment are appropriate and authorized.
- c. How does your change control management process record additions, modifications, or updates, including:
 - i. Date of the installation, removal, or modification.
 - ii. Details for the reason or nature of hardware upgrades/repairs, new software, software updates, etc.
 - iii. Description of procedures or reviews required prior to implementing the change, modification, or introduction of new software or hardware.
 - iv. The identity of the individual performing the installation or modification.
- d. Describe the procedures and controls to ensure separation of duties between system developers, change authorizers, implementation staff, and testers.
- e. Describe procedures to ensure system documentation is updated as a result of all changes to the production environment.

21. Internet Gaming/Internet Sports Betting Platform Patch Management

- a. Describe your processes related to patch management of software and operating systems.
- b. Describe the procedures and processes to ensure operating system and application patches are tested prior to deployment into the production environment.
- c. Describe the procedures and processes to ensure required or recommended operating system and application patches are identified and applied in a timely manner.