**Asset Management**

Asset Management includes the data, personnel, devices, systems, and facilities that are identified and managed consistent with the organization’s risk strategy.

**2.2**

**Do you maintain an inventory of assets, such as systems, cloud instances, and/or software applications?**

Maintaining a current list of all system components will enable an organization to accurately and efficiently define the scope of their environment for implementing security controls. Without an inventory, some system components could be forgotten, and be inadvertently excluded from the organization’s scope boundaries and configuration standards.

Suggested artifacts:

* A written system inventory containing a list of hardware components, including a description of function/use for each, including virtual systems and/or cloud-based platforms.
* If '**NO**', a Justification is required.
* Snapshot of your cloud-based inventory

**\* Justify your answer below.**

Yes we do maintain an inventory of cloud instances and software applications. Our system is cloud based

Yes

Virtal data centres (gcloud) - All software runs from here

Private Network - Virtual data centres within private network

Separate MYSQL Data base - Store company information

**2.3**

**Do you maintain a listing of software applications?**

Maintaining a current list of all critical software applications enables an organization to accurately and efficiently define the scope of their environment for implementing security controls. Without an application inventory, some critical security services could be missed, and be inadvertently excluded from the organization’s scope boundaries and SDLC standards.

Suggested artifacts:

* A written inventory of critical applications, including a description of function/use for each.

**\* Justify your answer below.**

**Yes**

**GSUITES**

**MICROSOFT -**

**ADOBE - secure digital signature**

**SLACK PRO - communication**

**SENTRY - Logs and events of apps**

**ATLASSIAN - Version control system, task management. Store code base**

**AIRTABLE - Tracking tasks**

**XERO - financial tracking and reporting**

**2.4**

**Do you perform regular risk assessments on critical systems?**

A risk assessment enables an organization to identify threats and associated vulnerabilities with the potential to negatively impact your business. Examples of different risk considerations include cybercrime, web attacks, and malware.

Suggested artifacts:

* - all 5 TSC including specific security controls in the environment
* Internal risk assessments of critical systems based on common standards and guidelines, such as NIST 800-30<https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>

**\* Justify your answer below.**

**Yes**

**<need drive to upload security documents>**

**2.5**

**Do you have data flow diagrams for all confidential data and systems?**

Data-flows identify the location of all confidential data that is stored, processed, or transmitted within the network.

Network and system data-flow diagrams help an organization to understand and keep track of the scope of their environment, by showing how data flows across networks and between individual systems and devices.

Suggested Artifacts:

* Data Flow Diagram(s)
* Data Flow Topology
* Data Flow Description

**\* Justify your answer below.**

**Yes**

**We have** Data Flow Topology

Need Dataflow Diagram ()flow chart) and Description

**2.6**

**Are system components (e.g., hardware, devices, data, time, personnel, and software) classified according to criticality, regulations, and business value?**

**Information Security - Inventory and Classification of Assets**

3.1.2 Security Objectives and Types of Potential Losses

3.2 Impact Assessment FIPS 199 defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability).

**\* Justify your answer below.**

Without clearly defined security roles and responsibilities assigned, there could be inconsistent interaction with the security group, leading to unsecured implementation of technologies or use of outdated or unsecured technologies.

**2.8**

**Risk Management**

Performing regular risk assessments of critical system components ensures that the organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Identifying and addressing vulnerabilities in a timely manner reduces the likelihood of a vulnerability being exploited and potential compromise of a system component or cardholder data.

**2.10**

**Do your receive cyber threat intelligence from reputable vendors, forums, and sources?**

**Information Security - Security Operations**

It's critical that organizations keep up to date with new vulnerabilities that may impact their environment.

Sources for vulnerability information should be trustworthy and often include vendor websites, industry news groups, mailing list, or RSS feeds.

Once an organization identifies a vulnerability that could affect their environment, the risk that the vulnerability poses must be evaluated and ranked. The organization must therefore have a method in place to evaluate vulnerabilities on an ongoing basis and assign risk rankings to those vulnerabilities.

Management should establish defined processes and appropriate governance to facilitate the performance of security operations including Analysis of threat intelligence from external sources.

**\* Justify your answer below.**

**Yes.**

**Forums, News Groups. Learn of threats relevant to software and tech we use**

**Recommendation: Investigate use of a SIEM system**

**2.11**

**Are threats, both internal and external, identified and documented?**

**Information Security - Risk Mitigation**

Management should also obtain, analyze, and respond to information from various sources (e.g., Financial Services Information Sharing and Analysis Center [FS-ISAC]) on cyber threats and vulnerabilities that may affect the institution.

**\* Justify your answer below.**

**No. (They not but they can be)**

**2.12**

**Are potential business impacts and likelihoods identified?**

**Information Security - Information Security Program Management**

Management should integrate the information security program with the institution’s lines of business and support functions. An integrated program provides management the ability to assess the likelihood and potential damage to the institution from an incident, identify the root cause(s) of the incident, and implement controls to address identified issues.

**\* Justify your answer below.**

**No. (but can be)**

**2.13**

**Are threats, vulnerabilities, likelihoods, and impacts used to determine risk?**

**Information Security - Risk Identification**

Risk identification should produce groupings of threats,including significant cybersecurity threats.

**\* Justify your answer below.**

**Yes - to an extent (not comprehensive)**

**We maintain a risk register of software applications**

**2.14**

**Do you have a vulnerability and patch management program?**

**Vulnerability Management**

Security vulnerability and patch management processes are essential to securing the environment. Given the criticality of this function, please provide the following:

Required Artifacts:

* Policies and Procedures in place to identify new security vulnerabilities and associate a risk ranking to the vulnerability, such as "high", "medium", "low", and the timing requirements for remediation for each ranking.
* List of sources/vendors that patches are received from
* Evidence of patch application and assignment of risk rankings

**\* Justify your answer below.**

**No.**

* **Recommendation: Investigate use of a SIEM system**
* **Create policy**
* **Implementation plan**

**2.15**

**Do you have an Incident Response training program?**

**Incident Response**

Without a thorough security incident response plan that is properly disseminated, read, and understood by the parties responsible, confusion and lack of a unified response could create further downtime for the business, unnecessary public media exposure, as well as new legal liabilities.

Suggested Artifacts:

* Type of Learning Management System (LMS), such as internal intranet sites, COTS LMS, training emails, etc.
* Screenshots acceptable
* Incident Response training completion records for a representative sample of employees
* Evidence of third-party (service provider) integration with IRP, such as IR Playbooks, contracts, table-top exercises, etc.
* End-user IR training collateral

**\* Justify your answer below.**

**No.**[**Matthew Piper**](mailto:matthewp@khula.co.za) **Bamboo**

**2.16**

**Do you protect data and systems using Encryption?**

Proper encryption ensures the security of sensitive data in storage, and in transit by minimizing exposure.

**Do you have controls to protect data in motion and at rest using standard encryption technologies to prevent unauthorized access?**

Suggested artifacts:

· Organization’s policies and related documents that are relevant to their network security strategy.

**\* Justify your answer below.**

**Yes. Some.**

**Recommendation:**

* **need to implement encryption on sensitive tables**
* **Migrate DB to cloud**

**2.17**

**Do you have a Change Control program?**

Uncontrolled changes to assets can introduce unauthorized access and vulnerabilities. Therefore, controlling changes to critical assets is essential for information security (and high availability).

**Are sufficient logs available that provide information to support changes to sensitive configuration settings and files?**

Suggested artifacts:

· Organization’s policies and related documents that are relevant to their build and release process or change control process.

**\* Justify your answer below.**

**Kind of. We have git**

**Recommendations:**

* **Implement Config and Secret management**

**2.18**

**Data Minimization / Data Destruction**

Reducing the amount of sensitive data that persists in an environment also reduces that environment’s overall security risk profile, and the risk of non-compliance with applicable privacy laws.

**Will data be deleted/destructed once contract is terminated by the entity?**

Suggested artifacts:

· Organization’s policies and related documents that are relevant to their data handling, and retention strategy.

**\* Justify your answer below.**

Not all. We do not delete data.

* Most the data we are required to not delete, for extra functionality
* We only delete data when the user deletes the account, eventually.

**Access Control**

Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

**3.2**

**Are identities and credentials issued, managed, verified, revoked, and audited for authorized devices, users and processes?**

Malicious individuals often use vendor default settings, account names, and passwords to compromise operating system software, applications, and the systems on which they are installed. Because these default settings are often published and are well known in hacker communities, changing these settings will leave systems less vulnerable to attack. Even if a default account is not intended to be used, changing the default password to a strong unique password and then disabling the account will prevent a malicious individual from re-enabling the account and gaining access with the default password.

* By ensuring each user is uniquely identified—instead of using one ID for several employees—an organization can maintain individual responsibility for actions and an effective audit trail per employee. This will help speed issue resolution and containment when misuse or malicious intent occurs.
* If multiple users share the same authentication credentials (for example, user account and password), it becomes impossible to trace system access and activities to an individual. This in turn prevents an entity from assigning accountability for, or having effective logging of, an individual’s actions, since a given action could have been performed by anyone in the group that has knowledge of the authentication credentials.
* Personnel usage policies can either prohibit use of certain devices and other technologies if that is company policy, or provide guidance for personnel as to correct usage and implementation. If usage policies are not in place, personnel may use the technologies in violation of company policy, thereby allowing malicious individuals to gain access to critical systems and cardholder data.

**\* Justify your answer below.**

**Yes.**

* **DB admin user accounts**
* **We have Password policies (strong password usage enforced)**
* **Users also need to use strong password for platforms**

**3.3**

**Is physical access to assets managed and protected? <Branch Logic for Virtual Client Infrastructures>**

Without physical access controls, such as badge systems and door controls, unauthorized persons could potentially gain access to the facility to steal, disable, disrupt, or destroy critical systems and sensitive data. Identifying authorized visitors so they are easily distinguished from onsite personnel prevents unauthorized visitors from being granted access to areas. Controlling physical access to sensitive areas helps ensure that only authorized personnel with a legitimate business need are granted access.

* When personnel leave the organization, all physical access mechanisms should be returned or disabled promptly (as soon as possible) upon their departure, to ensure personnel cannot gain physical access to sensitive areas once their employment has ended.
* Controls for physically securing media are intended to prevent unauthorized persons from gaining access to sensitive data on any type of media. Sensitive data is susceptible to unauthorized viewing, copying, or scanning if it is unprotected while it is on removable or portable media, printed out, or left on someone’s desk.
* Personnel need to be aware of and following security policies and operational procedures for restricting physical access to sensitive data and critical systems on a continuous basis.

**\* Justify your answer below.**

**Yes.**

* **Physical access to office: office park with boom gate. Office door with keys.**
* **Laptops collected after employment ends**

**3.4**

**Do you have access controls polices that incorporate the principles of least privilege and separation of duties?**

Reducing the number of personnel with access to the production environment minimizes risk and helps ensure that access is limited to those individuals with a business need to know. The intent of this control is to separate development and test functions from production functions. For example, a developer may use an administrator-level account with elevated privileges in the development environment, and have a separate account with user-level access to the production environment.

**\* Justify your answer below.**

**Some.**

* **Access is granted depending on role. Eg. Only devs have access to IT infrastructure, Only Accounting personnel can access account information, HR to employment, etc.**

**3.5**

**Awareness and Training**

The organization’s personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

Kindof:

* Regular notifications on security risks like phishing.

**3.6**

**Do senior executives understand their roles and responsibilities from a IT security perspective?**

Without clearly defined security roles and responsibilities assigned, there could be inconsistent interaction with the security group, leading to unsecured implementation of technologies or use of outdated or unsecured technologies.

Each person or team with responsibilities for information security management should be clearly aware of their responsibilities and related tasks, through specific policy. Without this accountability, gaps in processes may open access into critical resources.

Entities should also consider transition and/or succession plans for key personnel to avoid potential gaps in security assignments, which could result in responsibilities not being assigned and therefore not performed.

**\* Justify your answer below.**

**Yes.**

* **Executives review security policies.**

**3.7**

**Do physical and cybersecurity personnel understand their roles and responsibilities?**

Without clearly defined security roles and responsibilities assigned, there could be inconsistent interaction with the security group, leading to unsecured implementation of technologies or use of outdated or unsecured technologies.

Each person or team with responsibilities for information security management should be clearly aware of their responsibilities and related tasks, through specific policy. Without this accountability, gaps in processes may open access into critical resources or sensitive data.

Entities should also consider transition and/or succession plans for key personnel to avoid potential gaps in security assignments, which could result in responsibilities not being assigned and therefore not performed.

**\* Justify your answer below.**

**Yes**

* **Need outline/example of security policies**
* **Should include a Security Roles and Responsibilities Matrix: Security Activity, Accountable (A),Responsible (R, Consulted (C), Informed (I)**

**3.8**

**Information Protection Processes and Procedures**

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets, including virtual and cloud-based deployments.

No.

* Need a Data Classification and Handling Policy

**3.9**

**Is a System Development Life Cycle to manage systems implemented?**

Without the inclusion of security during the requirements definition, design, analysis, and testing phases of software development, security vulnerabilities can be inadvertently or maliciously introduced into the production environment.

Without properly documented and implemented change controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur, or malicious code could be introduced.

Application developers should be properly trained to identify and resolve issues related to these (and other) common coding vulnerabilities. Having staff knowledgeable of secure coding guidelines should minimize the number of security vulnerabilities introduced through poor coding practices.

As industry-accepted secure coding practices change, organizational coding practices and developer training should likewise be updated to address new threats—for example, memory scraping attacks.

Public-facing web applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems. The following processes and technologies can support the secure SDLC process:

• Manual or automated vulnerability security assessment tools or methods review and/or test the application for vulnerabilities

• Web-application firewalls filter and block non-essential traffic at the application layer. Used in conjunction with a network-based firewall, a properly configured web-application firewall prevents application-layer attacks if applications are improperly coded or configured.

**\* Justify your answer below.**

**Yes.**

* **Industry best practices on security and coding standards are observed and implemented as needed.**
* **No automated security checks done.**
* **Network Firewalls configured**

**3.10**

**Are backups of information conducted, maintained, and tested?**

If stored in a non-secured facility, backups that contain sensitive data may easily be lost, stolen, or copied for malicious intent. Periodically reviewing the storage facility enables the organization to address identified security issues in a timely manner, minimizing the potential risk.

**\* Justify your answer below.**

**Yes.**

* **We make occasional DB backups**

**3.11**

**Are protection processes continuously improved?**

Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise systems and steal sensitive data from the sensitive data environment. The specific types of failures may vary depending on the function of the device and technology in use. Typical failures include a system ceasing to perform its security function or not functioning in its intended manner; for example, a firewall erasing all its rules or going offline.

Incorporating “lessons learned” into the incident response plan after an incident helps keep the plan current and able to react to emerging threats and security trends. Regularly confirming that security policies and procedures are being followed provides assurance that the expected controls are active and working as intended. The intent of these independent checks is to confirm whether security activities are being performed on an ongoing basis. These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, firewall reviews, etc.—to assist the entity’s preparation for its next assessment.

**\* Justify your answer below.**

**No.**

* **Nothing in place to detect security controls in place.**
* **Recommendations: Add some form of automatic security check on static code, and other security controls on the system.**

**3.12**

**Is effectiveness of protection technologies shared with appropriate parties?**

**Management - Monitoring and Reporting**

Financial institution management should ensure satisfactory monitoring and reporting of IT activities and risk. These practices should include the following:

* Developing metrics to measure performance, efficiency, and compliance with policy.
* Developing benchmarks for reviewing performance.
* Establishing and reviewing service level agreements (SLA) with critical third-party providers.
* Developing, implementing, and monitoring a process to measure IT compliance with established policies, standards, and practices.
* Evaluating the effectiveness of mitigation strategies and controls.
* Implementing a quality control or quality assurance program to monitor and test systems and applications.
* Implementing timely and effective reporting processes.

**\* Justify your answer below.**

**No SLAs with cyber security companies, only clients**

**3.13**

**Are response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) in place and managed?**

Implement incident response procedures in the event unauthorized wireless access points are detected.

Each person or team with responsibilities for information security management should be clearly aware of their responsibilities and related tasks, through specific policy. Without this accountability, gaps in processes may open access into critical resources or cardholder data.

Entities should also consider transition and/or succession plans for key personnel to avoid potential gaps in security assignments, which could result in responsibilities not being assigned and therefore not performed.

Each person or team with responsibilities for information security management should be clearly aware of their responsibilities and related tasks, through specific policy. Without this accountability, gaps in processes may open access into critical resources or cardholder data.

Entities should also consider transition and/or succession plans for key personnel to avoid potential gaps in security assignments, which could result in responsibilities not being assigned and therefore not performed.

**\* Justify your answer below.**

**Not really.**

* **For business continuity of the services, We have snapshots and backups of VMs (Virtual Machines) where our services run.**

**3.14**

**Is cybersecurity included in human resources practices (e.g., deprovisioning, personnel screening)?**

If an employee has left the company and still has access to the network via their user account, unnecessary or malicious access to sensitive data could occur—either by the former employee or by a malicious user who exploits the old and/or unused account. To prevent unauthorized access, user credentials and other authentication methods therefore need to be revoked promptly (as soon as possible) upon the employee’s departure.

Controlling physical access to sensitive areas helps ensure that only authorized personnel with a legitimate business need are granted access.

When personnel leave the organization, all physical access mechanisms should be returned or disabled promptly (as soon as possible) upon their departure, to ensure personnel cannot gain physical access to sensitive areas once their employment has ended.

Performing thorough background investigations prior to hiring potential personnel who are expected to be given access to sensitive data reduces the risk of unauthorized use of sensitive data by individuals with questionable or criminal backgrounds.

**\* Justify your answer below.**

Not really:

* There is personnel screening
* Access for IT resources are deprovisioned when employees leave

**Anomalies and Events**

Anomalous activity is detected in a timely manner and the potential impact of events is understood.

**4.2**

**Do you maintain a baseline of network operations and expected data flows for users and systems established and managed?**

Maintaining network and connectivity diagrams and data flow charts to ensure adequacy of layered controls and to facilitate more timely recovery and restoration of systems when incidents occur. Network diagrams describe how networks are configured, and identify the location of all network devices.

Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.

Data-flow diagrams identify the location of all data that is stored, processed, or transmitted within the network. Network and data-flow diagrams help an organization to understand and keep track of the scope of their environment, by showing how data flows across networks and between individual systems and devices.

A documented and implemented process for approving and testing all connections and changes to the firewalls and routers will help prevent security problems caused by misconfiguration of the network, router, or firewall. Without formal approval and testing of changes, records of the changes might not be updated, which could lead to inconsistencies between network documentation and the actual configuration.

**\* Justify your answer below.**

**4.3**

**Do you analyze detected events to understand attack targets and methods?**

Many breaches occur over days or months before being detected. Regular log reviews by personnel or automated means can identify and proactively address unauthorized access to the cardholder data environment. The log review process does not have to be manual. The use of log harvesting, parsing, and alerting tools can help facilitate the process by identifying log events that need to be reviewed.

Checking logs daily minimizes the amount of time and exposure of a potential breach. For example, notifications or alerts that identify suspicious or anomalous activities—as well as logs from critical system components, and logs from systems that perform security functions, such as firewalls, IDS/IPS, file-integrity monitoring (FIM) systems, etc. is necessary to identify potential issues. If exceptions and anomalies identified during the log-review process are not investigated, the entity may be unaware of unauthorized and potentially malicious activities that are occurring within their own network.

**\* Justify your answer below.**

**4.4**

**Do you collect and correlate event data from multiple sources and sensors?**

It is critical to have a process or system that links user access to system components accessed. This system generates audit logs and provides the ability to trace back suspicious activity to a specific user. These monitoring systems are designed to focus on potential risk to data, are critical in taking quick action to prevent a breach, and must be included in the incident-response processes. Many breaches occur over days or months before being detected. Regular log reviews by personnel or automated means can identify and proactively address unauthorized access to sensitive data. The log review process does not have to be manual. The use of log harvesting, parsing, and alerting tools can help facilitate the process by identifying log events that need to be reviewed.

**\* Justify your answer below.**

**4.5**

**Security Continuous Monitoring**

The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

**4.6**

**Do you monitor your network(s) to detect potential cybersecurity events?**

The use of tools to detect cybersecurity events and enforce perimeter protection include routers, firewalls, intrusion detection systems (IDS) and intrusion prevention systems, proxies, gateways, jump boxes, demilitarized zones, virtual private networks (VPN), virtual LANs (VLAN), log monitoring and network traffic inspecting systems, data loss prevention (DLP) systems, and access control lists.

Reviewing these logs daily minimizes the amount of time and exposure of a potential breach. For example, notifications or alerts that identify suspicious or anomalous activities—as well as logs from critical system components, and logs from systems that perform security functions, such as firewalls, IDS/IPS, file-integrity monitoring (FIM) systems, etc. is necessary to identify potential issues.

**\* Justify your answer below.**

**4.7**

**Do you perform monitoring for unauthorized personnel, connections, devices, and software?**

Examples of monitoring include:

* Unauthorized wireless devices. The size and complexity of a particular environment will dictate the appropriate tools and processes to be used to provide sufficient assurance that a rogue wireless access point has not been installed in the environment.
* Intrusion detection and/or intrusion prevention techniques (such as IDS/IPS) compare the traffic coming into the network with known “signatures” and/or behaviors of thousands of compromise types (hacker tools, Trojans, and other malware), and send alerts and/or stop the attempt as it happens.
* Change-detection solutions such as file-integrity monitoring (FIM) tools check for changes, additions, and deletions to critical files, and notify when such changes are detected.

These monitoring systems are designed to focus on potential risk to data, and are critical in taking quick action to prevent a breach. All of the monitoring systems must be included in the incident-response processes.

**\* Justify your answer below.**

**4.8**

**Do you perform vulnerability scans on your systems and networks?**

A vulnerability scan is a combination of automated or manual tools, techniques, and/or methods run against external and internal network devices and servers, designed to expose potential vulnerabilities that could be found and exploited by malicious individuals. Once these weaknesses are identified, the entity corrects them and repeats the scan until all vulnerabilities have been corrected. Identifying and addressing vulnerabilities in a timely manner reduces the likelihood of a vulnerability being exploited and potential compromise of a system component or sensitive data.

**\* Justify your answer below.**

**Response Planning**

Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.

**5.2**

**Do you have an incident response plan that is executed during or after an event?**

This is achieved by implementing an incident response program. The goal of incident response is to minimize damage to the institution and its customers in the event of a security incident.

A company's information security policy creates the roadmap for implementing security measures to protect its most valuable assets. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. Security threats and protection methods evolve rapidly. Without updating the security policy and incident response plan to reflect relevant changes, new protection measures to fight against these threats are not addressed.

**\* Justify your answer below.**

**5.3**

**Communications**

Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

**5.4**

**Do you ensure that all personnel aware of their roles and order of operations when a response (i.e.incident, disaster) is needed?**

This control is often shown in a RACI matrix (Responsible, Accountable, Consulted, Informed). A company's information security policy creates the roadmap for implementing security measures to protect its most valuable assets. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. Security threats and protection methods evolve rapidly. Without updating the security policy to reflect relevant changes, new protection measures to fight against these threats are not addressed.

**\* Justify your answer below.**