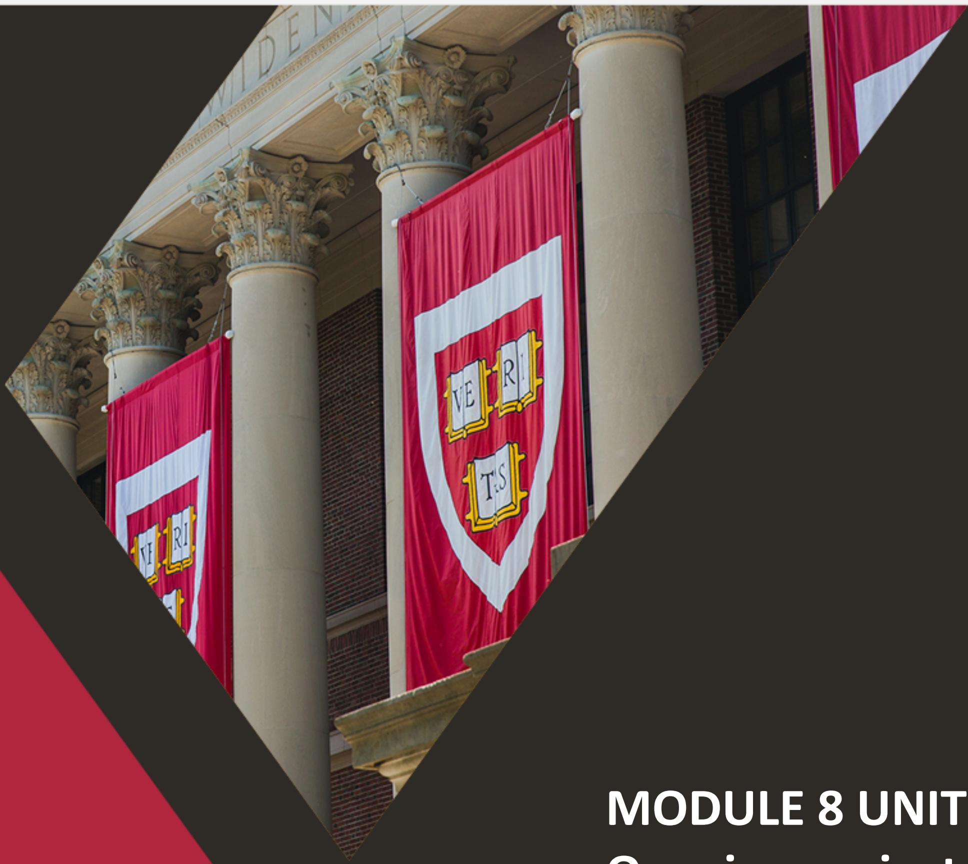
HARVARD
Office of the Vice Provost for Advances in Learning



MODULE 8 UNIT 2
Ongoing project

HARX CYB Module 8 Unit 2 Ongoing project

Learning outcome:
LO5: Develop a cyber risk mitigation strategy specific to your organization.

Name: Aniya Adair

1. Instructions and guidelines (Read carefully)

Instructions

1. Insert your name and surname in the space provided above, as well as in the **file name.** Save the file as: **First name Surname M8 U2 Ongoing project** – **e.g.** **Zadie Smith M8 U2 Ongoing project**. **NB:** *Please ensure that you use the name that appears in your student profile on the Online Campus.*
2. Write all your answers in this document. There is an instruction that says, "Start writing here" under each question. Please type your answer there.
3. Submit your assignment in **Microsoft Word only**. No other file types will be accepted.
4. Do **not delete the plagiarism declaration** or the **assignment instructions and guidelines**. They must remain in your assignment when you submit.

PLEASE NOTE: **Plagiarism cases will be investigated in line with the Terms and Conditions for Students.**

IMPORTANT NOTICE: Please ensure that you have checked your course calendar for the due date for this assignment.

Guidelines

1. Make sure that you have carefully read and fully understood the questions before answering them. Answer the questions fully but concisely and as directly as possible. Follow all specific instructions for individual questions (e. g. "list", "in point form").
2. Answer all questions in your own words. Do not copy any text from the notes, readings or other sources. **The assignment must be your own work only.**

Plagiarism declaration

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.

2. This assignment is my own work.
3. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as their own work.

4. I acknowledge that copying someone else's assignment (or part of it) is wrong and declare that my assignments are my own work.

2. Brief

This module focused on the importance of risk mitigation and the value companies can derive from implementing a risk mitigation strategy to improve organizational resilience and manage risks effectively. This assignment requires you to complete a cyber risk mitigation strategy for your organization.

As the notes made clear, a risk mitigation strategy helps an organization prioritize its risks so it can allocate resources efficiently. This final submission is an opportunity for you to reflect and condense all the knowledge you have gained over the duration of the course by incorporating feedback from your previous ongoing project submissions into a consolidated cyber risk mitigation strategy.
If you are completing your ongoing project on Sony, you are required to create a risk mitigation strategy that the organization should have followed in light of the 2014 hack.

Note:
All ongoing project submissions throughout the course need to focus on the same organization. Or, if you choose to focus on the case study of Sony, you will need to complete all your submissions on Sony.
It is highly recommended that you avoid disclosing any confidential information in your assignments. Although you are encouraged to draw on real-world experience during the course, you are urged to use pseudonyms (false names) and alter any sensitive details or data where necessary. You are responsible for ensuring that you do not disclose any information that is protected by confidentiality undertakings; all information is treated in accordance with our privacy policy.
Please read Section 4 of the Honor Code in the Orientation Module course handbook for more guidance.

Note:

- The published word count in each assignment is for satisfactory work – it is the amount of detail, analysis and nuance needed for a satisfactory score according to the rubric. If you exceed the published word count, you will not be penalized. The extra work can improve your grade – up to and including an exceptional score. Your grade is not dependent on the number of words you write. The word count is simply a benchmark for an average level of detail, analysis and nuance, and additional detail and nuance is needed to surpass a Satisfactory grade.

- You must not only include overall organizational context, but per-question context as well. This context allows the reader to understand what the organization does and which sector it is part of, as well as why each question is important to the organization.

3. Risk mitigation strategy

Introduction

Write a brief paragraph in which you provide a high-level overview of your organization's need for a risk mitigation strategy.

(Write approximately 150 words)

Start writing here:

Information is an essential asset to VMW's and its day-to-day business operations. As an application virtualization enterprise that has and continues to experience tremendous cloud computing sector growth, VMW's information assets must be adequately protected. For the purpose of VMW's risk mitigation strategy, information assets have been defined as 'any information with value to VMW regardless of the format or the means by which it is shared; information sssets exist in many forms, including but not limited to printed or written materials stored and transmitted electronically, shown in presentations, or spoken in conversation'. Information assets include automated and manual systems including those managed or hosted by third parties on behalf of VMW.

VMW's need for a risk mitigation strategy is based on its mission to achieve *information security:* protecting information assets in order to assure business continuity while minimizing risk and augmenting business opportunities. The VMW Security and Resiliency team, led by the CISO under the executive umbrella of the VMW Chief Digital Transformation Officer, manages the enforcement, development, and maintenance of information security policies and standards to ensure VMW's information assets are preserved in a secure and compliant environment according to business and risk objectives.

Vision

Outline your organization's vision of what implementing a risk mitigation strategy will ideally achieve.

(Write approximately 150 words)

Start writing here:

"VMware, a global leader in cloud infrastructure and business mobility, accelerates our customers' digital transformation journey by enabling enterprises to master a software-defined approach to business and IT. With VMware solutions, organizations are

creating exceptional experiences by mobilizing everything, responding faster to opportunities with modern data and apps hosted across hybrid clouds, and safeguarding customer trust with a defense-in-depth approach to cybersecurity." [1]

VMW's risk mitigation strategy aims to achieve its stated mission via information security and compliance. Security compliance will be achieved through implementing controls that leverage a technological infrastructure. These controls should be established, implemented, monitored, reviewed, and continually improved, to ensure security and business objectives are realized. VMW is committed to protecting the integrity, confidentiality, and reliability of all VMW information assets from unauthorized disclosure, removal, acquisition, modification, or destruction. VMW's information security risk mitigation program and its related information security policies and standards (ISSPs) are the foundation for achieving security compliance across all levels of the organization starting with employees and managers, and spreading out to engineering architecture, customers, independent contractors, and other 3rd party vendors. VMW will also achieve an enterprise-wide cybersecurity culture by integrating its risk mitigation strategy into each functional business unit whether technical or non-technical.

Strategic Goals and Objectives

List at least four strategic goals your organization must achieve to reduce its risks to an acceptable level. List at least two objectives under each strategic goal that explain what must be done to achieve the strategic goal.

> **Note:** A thorough risk mitigation strategy should include associated action plans and milestones, but you are not required to detail these for the purposes of this submission.

(Write approximately 450 words)

Start writing here:

Strategic Goal #1: Security Control Standardization and Automation

- To ensure confidentiality, integrity and availability of systems and PII, PHI, and PCI data, security controls must be implemented with uniformity and in a manner that minimizes exceptions and other non-standardizations.
    - Objective 1.1: Exceptions to security control standards will be actively monitored and managed by the appropriate resources
    - Objective 1.2: Security Controls will be automated whenever possible. Human judgement will not be relied upon by default. Security controls with significant manual requirements will not be implemented.
    - Objective 1.3: A Zero Trust approach (never trust, always verify) will be taken to prevent unauthorized access to VMW data, systems, and processes
        - Objective 1.3.1: Customers and employees must be authenticated and continuously validated [2]

Strategic Goal #2: Resiliency is an enterprise-wide priority

- The Security and Resiliency team is responsible for creating and updating ISSPs in conjunction with the constantly changing threat landscape and as technologies change. ISSPs should be established and documented correlating with the VMW EISP, covering each categories of enterprise security governance: Asset Management, Data Classification, Data Handling and Protection, Security Compliance, Third Party Risk Management, Data Backup, Computer and Network Management, Systems Access, Systems Development and Maintenance, Security Incident Management, Operations Security, Change Management, Vulnerability Management, Architecture, Platform and Application Cloud Security Standards, and Physical Environmental Security.

  - Objective 2.1: The Security and Resiliency team will conduct regular reviews of VMW Information Security Policies
    - Objective 2.1.1: Reviews will be a cross-functional effort with Human Resources and Privacy and Cybersecurity legal counsel
  - Objective 2.2: The Security and Resiliency team will develop recovery strategies in accordance with the VMW Business Impact Analysis of defined mission-critical assets
    - Objective 2.2.1: The Data Backup ISSP will include an officially documented Data Backup Schedule

Strategic Goal #3: Auditability and Accountability of Systems

- As a government Cloud Service Provider, VMW systems which host United States government information and data will be audit-enabled to comply with the FedRAMP Authorization Boundary for VMW's Cloud Service Offerings [3], as well as to achieve compliance with the Federal Information Processing Standards Publication (FIPS) 199 [4]
  - Objective 3.1: VMW Data Governance, Security Architecture, Risk Management and Privacy teams will mutually select events to be captured and provide the rationale behind each chosen event
    - Objective 3.1.1: Audit events will be reviewed and updated annually
  - Objective 3.2: Continuous audit records will be generated for specified audit events

Strategic Goal #4: Implementing Security by Design

- Security should be built into VMW architecture and systems during development, not after.
  - Objective 4.1: Architecture must follow the five pillars of Cyber Hygiene [5]: Patching (*regularly, using automated tools such as VMW Unified Endpoint Management* [6]); Multi-Factor Authentication (MFA) (*all internal and external access to VMW systems requires MFA*); Rule of Least Privilege *(controlling privileged access with a role-based structure);* Micro-segmentation (*creating multiple network layers using NSX* [7] *to increase automation and reduce need for 3rd party controls*); and Encryption (*ensuring all VMW devices and data in transit or at rest is encrypted*)
  - Objective 4.2: OWASP secure coding practices [8] must be used at all times

Metrics

List at least three metrics your organization will use to analyze the achievement of its goals/objectives. These metrics should be specific to the goals/objectives listed in the previous question.

(Write approximately 150 words)

Start writing here:

Strategic Goal	Objectives	Metric(s)
Security Control Standardization and Automation	Implementing uniform security controls across the org structure and at the customer level to ensure CIA of data (1.1, 1.2, 1.3, 1.3.1)	1. Effectiveness of implemented controls will be measured by the number of Data Loss alerts triggered per fiscal quarter ● Technical and operational metric logs for alerts will be collected via monitoring tools o Log source count o Alert handling response time o Control violations 2. Physical equipment used to generate, store, and archive cryptographic keys will be physically protected and monitored 24/7 ● Access to facilities storing cryptographic equipment will be tracked by badge scans. Only “restricted area” badges can scan into facilities. o Access attempts by other badge types will be recorded. 3. A trackable security control exception request mechanism will be implemented for case-by-case risk assessment 4. At minimum, all production systems, networks, approved 3rd party application integrations, infrastructure and endpoints are required to maintain the following standard controls: ● SSL certificate ● FIPS-validated cryptography solution, with AES-128 minimum ● Anti-malware software ● Firewalls with TCP/IP specific protocol o Asset management practices will be implemented to identify and inventory corporate-owned devices 5. All wireless networks (corporate, guest, and work from home) will log sign-on and sign-off events with credentials and IP address
Resiliency is an enterprise-wide priority	Creating, documenting and enforcement of ISSPs by the VMW Security and Resiliency team, focusing on resiliency and recovery (2.1, 2.1.1, 2.2, 2.2.1)	1. A Business Continuity Plan must be reviewed and updated every 12 months by the CEO and CISO 2. A business process recovery exercise must be completed by the Security and Resiliency team and VMW CSIRT team every 12 months simulating security incidents defined as ‘catastrophic’ 3. Business Continuity Plan contacts must be reviewed and updated quarterly

		4. Critical data store backup volume tests/reviews will be conducted monthly at random by the VMW Database Administration team to ensure data integrity ● Backup reviews will evaluate for ≥ 99% adherence to defined backup schedules: o Daily backups for records/fields that have been changed within previous 24 hours o Monthly backups of all data on the first day of each month o Quarterly backups of all data on the first day of each fiscal quarter
Auditability and Accountability of Systems	Compliance with FIPS and FedRamp standards as a US government Cloud Service Provider for systems hosting government data (3.1, 3.1.1, 3.2)	1. Auditability and compliance for FIPS will be evaluated against whether audit records are consistently generated (≥ 95%) on government data-hosting and processing systems; whether those logs are generated on a centralized platform; and whether audit logs include the each of the following data points: ● Event type ● Event timestamp ● Event source ● Identity of user ● Session and connection duration ● Authentication checks completed ● Data changes ● Successful or unsuccessful attempts to access, modify or delete defined security objects within the system of record 2. Audit Records must retain at least 12 consecutive months of searchable data for security incident investigations that might occur after-the-fact
Implementing Security by Design	Cyber Hygiene in Architecture and OWASP coding practices (4.1, 4.2)	1. Internal penetration testing will be conducted on 100% of development/architecture applications before production release ● 100% of penetration tests will be completed in ≤ 2 weeks (excluding weekends) from the start of the test ● 100% of CVSS [9] 'critical' vulnerabilities are to be fully remediated 2. **All** VMW platforms, applications and/or information infrastructure documented within the master register will have risk assessments performed biannually and assessment results uploaded to a central location, categorized by risk severity. 3. Time to deployment of critical patches is ≤ 24 hours from discovery of the critical vulnerability

Note:
Include refined versions of your previous submissions in the sections below. Where relevant, incorporate any feedback from your Tutor, as well as additional knowledge gained during the course to improve on your previous submissions.

Threat Actors and Methods of Attack

Integrate your submission from Module 2, in which you identified at least two threat actors to your organization and described methods of attack these actors could use. If you are using the Sony case, integrate the submission in which you identified the threat actor Sony faced in the 2014 hack and their method of attack, as well as at least one other threat actor Sony could face in the future and what method of attack they might use.

(Write approximately 550 words)

Start writing here:

Operating in the fast-growing, highly interconnected and completely online cloud computing sector brings a considerable amount of inherent vulnerability. According to a quantitative analysis published by consumer IT trends researcher Lionel Vailshery, half of corporate data is now stored in the cloud [10, 11]. This increased reliance on the cloud brings with it increased risk of data breaches, the stealing or ransoming sensitive of data or trade secrets, and DDoS attacks. Given the recent increase in destructive ransomware and malware attacks [12] (due in part to geopolitical turbulence), VMW must be vigilant in accounting for nation state or other state-sponsored threat actors in its enterprise cyber risk management strategy. VMW will keep abreast of the constantly changing threat landscape and keep in mind the role the organization's geographical diversity plays in managing risk, increasing its security posture in response to current events, such as updating and blacklisting emerging IoCs at the enterprise level using anti-malware software such as Carbon Black Cloud.

Nation state actors are launching attacks against enterprises at greater rate than any other target category [13] including defense, media and communications and governmental authorities. To combat an attack by potential state-sponsored threat actors, particularly those originating within Russia, VMW will comply with industry guidance from authorities—such as "Shields Up" from the Cybersecurity and Infrastructure Security Agency—as well as official directives/sanctions levied against geopolitical enemies by the United States government. Furthermore, as a federal contractor, it is paramount that VMW protect the and ensure the confidentiality, integrity and availability of all critical information and infrastructure, but especially systems that host, transmit and process US government data from Russian state reconnaissance in retaliation for suspending operations in the country following the Ukraine assault [14]. As a result of sanctions and suspending operations, VMW employees in Russia are affected in that their immediate employment has been ended. This paves the way for another threat and actor—insiders.

Disillusioned or disgruntled employees seeking retribution for a perceived wrong is a constant threat since confidential company information can be regularly accessed on the company intranet and through official corporate communications. Current and former employees with ongoing or previous access to sensitive, privileged information can become insider threat actors once they decide to end their professional relationship with the company.

Whether intentional or accidental, it is estimated that approximately 30% of organizational security breaches and incidents are caused by insiders [15]. To mitigate the business operational risk associated with insider threats and achieve Information Security, investment in in-house multi-factor authentication and strict adherence to the least-privilege access doctrine will be employed. It is important that VMW use an internal unified endpoint management solution be used to further reduce risk associated with 3rd party vendors. To mitigate insider threats on the frontend, VMW will continue to perform stringent background checks on all candidates before an offer of employment can be extended, as recommended by the NIST [16]. Background checks are to be proportional to role requirements and classification of the data an employee will have access to. Once hired, ongoing insider threat risk management in this area will take the form of role-based security training, workforce development programs to enhance employee satisfaction, and security awareness training (to be explained in further detail under section "Cybersecurity Governance"). Software tools and other means will also be used to regularly monitor or inspect users' endpoints. Training and development helps the organization aims to prevent disgruntlement and promote a culture of Information Security awareness. VMW Human Resources and IT Security Operations will implement robust de-authorization procedures for employees leaving the company.

Business Critical Assets

Integrate your submission from Module 3, in which you identified the assets that are most essential to your organization or Sony's ability to accomplish its mission. Describe what vulnerabilities there may be in the organization's systems, networks, and data that may put these assets at risk.

(Write approximately 550 words)

Start writing here:

Consistent, reliable access to VMW's proprietary technology stack is necessary for customers to perform their own critical transactions such as workforce management, software development, and secure information storage—the core of VMW's business. Therefore, VMW is committed to Information Security of its mission and business critical assets. VMW has many systems and tools it relies on to conduct business and deliver cloud services; however, business critical assets are defined as such due to the destructive impact to confidentiality, integrity, and availability if they were to be compromised. They can be divided into three broad categories.

- **Wireless Networks**: corporate, guest, and work from home network including the corresponding VPNs and firewalls and configurations
- **Company, Customer and Employee Data**: product source code, intellectual property, earnings, and corporate strategy; customer contract data such as dollar amounts, financial transaction details and account numbers; and employee login credentials, SSNs, and other PII
- **Endpoints**: physical servers; physical network devices including routers and switches; and cloud servers/applications

The ongoing COVID-19 pandemic has led to an explosion of remote work across the world. for VMW, it stretched the organization's already distributed workforce and the systems that support basic business continuity. VMW hiring efforts did not slow down due to the pandemic; with a growing workforce comes greater potential for certain network vulnerabilities as the Bring Your Own Device (or BYOD) program expanded to its largest participation since inception. BYOD's can serve as an entry point for unauthorized apps and ransomware that would disrupt operations. In the same way, employee home wireless networks are not professionally managed with the same level of security of the corporate network. While VMW will continue to use Virtual Private Networks (or VPNs) that require MFA, there have been instances where even those connections have been hijacked by state-sponsored threat actors [17].

Taking advantage of the pandemic and the newly increased ease of impersonating a remote colleague, cybercriminals have upped their phishing efforts almost 220% [18]. VMW remains vulnerable to this type of human error as a significant percentage of the workforce is remote and will remain so for the foreseeable future as the pandemic remains unpredictable—even while some offices in the US and Europe reopen.

It is imperative VMW works to minimize vulnerability to critical assets' CIA while undergoing its Digital Transformation to become the leading multi-cloud provider. As a Cloud Service Provider (CSP), VMW is responsible for the security of its cloud service offerings themselves (as opposed to customers, who are responsible for security of their instances/data *within* the cloud). Cloud infrastructure complexity is a vulnerability as VMW continues to scale its cloud-native offerings across platforms. Deploying completely error-free software code across several different operating systems takes a concerted engineering effort. Known application coding vulnerabilities—SQL Injection, Cross Site Scripting (XSS), buffer overflow, broken authentication, sensitive file disclosure—must be avoided with automated tools. Automation will also reduce the need for super user and admin account privileges for developers, reducing the risk of human error.

All teams under the umbrella of Security and Architecture Engineering must adhere to the robust Patch Management process for all vulnerabilities as they are discovered, particularly for vSphere and vCenter Server products. vSphere requires high usability as the virtualization platform; vCenter acts as the admin for vSphere servers. If one or both assets were to be hit with a DDoS attack or the data within them ransomed or lost, customers would be unable to access and manage their environments. VMW cannot afford the resulting legal and reputational risks as a result of unmitigated and unpatched vulnerabilities. There will always be the unknown (zero-day attacks) and the uncontrollable (customers refusing to upgrade legacy software to the latest version, which is a security threat), but implementing Information Security practices based on risk mitigation at the center will ensure VMW achieves its mission.

Cybersecurity Governance

Integrate the three questions from your submission in Module 4 in which you recommended a cybersecurity leadership plan, improvements to management processes, and a cybersecurity awareness training program.

(Write approximately 1,200 words)

Start writing here:

VMW is committed to conducting business ethically and in compliance with all federal, state and local laws, regulations and international standards. VMW's Governance Strategy therefore focuses on ensuring the organization achieves its mission of Information Security via protection of all business and mission critical Information Assets. The four pillars of this risk-based strategy are:

1. Establishing, maintaining and enforcing compliance of VMW's EISP and ISSPs
2. Continuous training and awareness
3. Continuous oversight and review of 3rd party SLAs and liaising with VMW Privacy and Cybersecurity legal to manage risk
4. Protection of critical information assets via Data Governance. Data Governance articulates VMW's approach to Data Protection as Identification, Development and Ongoing Maintenance. Data Governance works closely with sister-team Information Security to execute this approach.

VMW's governing structure is cross functional which reflects the org's interdepartmental, Zero Trust approach to Information Security. VMW's Office of the Chief Digital Transformation Officer is a new group within VMW responsible for leading the company's multi-cloud strategy [19] with the CEO. As part of the Office of the CDTO, and reporting directly to the CDTO specifically, is the Chief Security Officer. The CISO is the first security-focused executive role in the reporting structure. The VMW CISO is the leader of the company's dedicated Security and Resiliency department, whose mission is to be visible, responsive and effective in enabling VMW to deliver against strategic Information Security objectives by reducing the risk of security incidents and data breaches. The Security and Resiliency department provides specialized support and guidance to all orgs within the company, ensuring that assets and processes at all levels are secure. Security and Resiliency, and therefore the CISO, is accountable for managing cyber risk and implementing risk controls.

Diving deeper into the structure of the Office of the CDTO, this 'team' is made up of four separate but interconnected departments: Security Engineering, Architecture and Vulnerability Management, Physical Security, Governance, Risk, Compliance and Assurance, and finally Threat Management, all reporting to the CISO. Each department is responsible for a different risk mitigation aspect of enterprise wide Information Security:

- **Security Engineering, Architecture and Vulnerability Management**: Proactively manages risk to Information Assets by identifying and remediating security vulnerabilities in VMW systems to inform management of the security posture of the organization. This department is responsible for achieving the 'Security by Design' objective.
- **Physical Security**: Safeguards VMW facilities, staff and assets via tools such as building design, environmental controls, security systems, designated security personnel. The Physical Security department helps ensure Confidentiality, Integrity, and Availability of VMW cloud services and information assets.
- **Governance, Risk, Compliance and Assurance**: Maintains company values of transparency and accountability by addressing and enforcing the standards set forth in the EISP and ISSPs, as well as other standards and key decisions made by other internal VMW authorities related to cloud computing. The most pronounced responsibility of the department is maintaining compliance with the myriad laws,

regulations, policies, and standards which are applicable to cloud computing and by extension VMW. The team must continuously review and account for all legal requirements relating to markets, taxes, the environment, employee welfare, and international trade; however, cloud computing specifically introduces additional complexities of compliance given its borderless nature.

- **Threat Management**: Protects VMW from cyberthreats targeting the organization and its employees with continuous hands-on threat monitoring, identification, and response.

There is always room for improvements in the org structure. VMW would further benefit from including its Chief Information Officer under umbrella of Security and Resiliency. The CIO would work alongside the CISO, sharing responsibility for Confidentiality, Integrity, and Availability while also focusing on balancing the security risks in delivering IT solutions [22]. Current VMW CIO priorities focus on project delivery itself. Including this role in the Security and Resiliency department would further increase Information Security visibility within VMW's project management organization, which operates separately.

VMW employs several cybersecurity governance management practices to effectively execute three baseline Data Governance objectives:

1. **Strategic Direction** via a roadmap focused on risk mitigation and overall alignment of cybersecurity
2. **Commitment** via implementing and performing assessments. VMW Data Governance is committed to identifying gaps and facilitating remediation.
3. **Specific designation of responsibility for Information Security Management**: The VMW CISO, under the strategic direction the Chief Digital Transformation Officer (detailed below), is accountable for the management, enforcement, development and maintenance of Information Security, enterprise wide.

Management Practice	Details	Improvement Areas
Establishing an Enterprise Information Security Policy (EISP)	The EISP, ISSPs and SysSPs not only have executive sponsorship, but individual executive ownership as well. The Security and Resiliency team is responsible for creating and updating ISSPs and SysSPs. ISSPs and SysSPs covering each category of enterprise security governance have been established and documented correlating with the VMW EISP.	A detailed outline of an ongoing Security, Education, Training and Awareness program could be added at the EISP level to address the recent change in traditional vs remote workforce distributions and the risks associated with it.
Establishing Cybersecurity Culture	Each of the four central components of a strong company cybersecurity culture are enacted: 1. *Transparency:* VMW cybersecurity policy takes a "non-secrecy "approach. Exceptions to VMW Information Security policy can be granted on a case-by-case basis if there is sufficient justification (for example, an employee's personal mobile device operating system is not in compliance with the Mobile Device Management Policy's minimum requirements). A technical standards library, evaluated against CIS benchmarks [20]	While the management practices behind creating a cybersecurity culture are in place, there is not a specific cyberculture plan [21] in place outlining specific actions the organization can take to grow it.

	for critical applications, is available internally for VMW employees and externally for 3rd parties. Through the value of 'professional skepticism', employees are encouraged to report any suspected cybersecurity incident to the Security and Resiliency team. 2. Appropriate systems knowledge: All VMW employees are mandated to attend information annual trainings. Trainings are in-depth and foster a consensus that Information Security is everyone's responsibility. VMW employees are required to complete an initial Information Security training within their date of hire. There are different levels of trainings given, each commensurate with the employee's day to day role and exposure to critical Information Assets. 3. Compliance with policy and procedure: Functional managers are tasked with ensuring all direct reports are aware of their responsibility for Information Security. Managers also protect the Confidentiality, Integrity and Availability of VMW critical assets by managing authorization and deprovisioning of their reports' access to VMW systems. 4. Formal communications: VMW uses Slack and email as an official means of communicating security related announcement. Employees can also engage directly with cybersecurity and threat leadership in these instant messaging channels.	Additionally, continually engaging in a feedback loop with users will close any gaps employees may have that might prevent them from viewing cybersecurity as something that is intrinsic to their role, no matter what that role may be. Training frequency could be more regular to further increase risk mitigation (by continually developing knowledge, thus improving, human factors).
Budgeting and Resource Allocation	VMW does have a dedicated cybersecurity budget. Earnings calls are held once per quarter hosted by the CFO. Cash flow metrics are discussed at a very high level.	Generally, specifics of how budget allocations are calculated are not shared beyond corporate finance; however, VMW could consider hosting internal AMAs or town halls to review cybersecurity budgets and categories per business unit. Disseminating this information in an official but strictly confidential format also contributes to transparency and commitment to cyber defense. Reporting on metrics such dollars saved by preventing data breaches are tangible ways to prove ROI and effectiveness.
Reviewing 3rd Party Agreements	Governance leadership maintains an automated a 3rd party security risk questionnaire to remove the manual efforts of weighing trade-offs in risk. Governance leadership also frequently performs formal	Reduce reliance on questionnaires in evaluating risk acceptance. VMW should continue to create a

	assessments of the EISP's and ISSPs' alignment with VMW's core company mission.	structured framework for evaluating risk, similar to those of Microsoft and Adobe [24]
Talent Management	VMW aims to be a prime destination for cybersecurity talent and has a company-wide referral bonus program for all security and engineering roles. The program incentivizes current employees to leverage their professional networks to secure quality candidates. Each employee with at least one year of continuous employment is eligible for course, workshop or degree tuition reimbursement for 3rd party programs, trainings, conferences, etc. directly related to cybersecurity, risk management, and privacy. Eligibility requirements for employees with several years of consecutive service	VMW could consider adopting recruitment management practices in the NICCS Cybersecurity Workforce Development Toolkit [23]. VMW hiring managers from non-technical departments could be leveraged to prioritize an enterprise-wide talent recruiting initiative following the "Build" guidelines. Using the toolkit's trait profiled would assist in evaluating potential talent for the pipeline for non-technical recruiters. For current VMW employees that are interested in cybersecurity but don't have a technical background, company-sponsored training reimbursement program could be implemented for in-demand certifications such as CompTIA or GIAC. The cost of individual certifications is often much less than degree programs and are a faster way to upskill and prove competency.

Regarding improvements to the Security, Education, Training and Awareness program, new efforts should be undertaken to underscore the importance of Online Threat Awareness (phishing, malware and the pronounced human element of cyberattacks).

Using the same platform and delivery format as the annual security recertification, this new course would be required to be completed quarterly. The audience for the required course would be extended from only full-time employees to contractors and contingent workers with access to any VMW system. An on-the-job phishing awareness campaign in addition to the online course will simulate phishing attempts. Carefully created emails will be sent out to all corporate user accounts. The emails are live testing for employees to correctly identify a sophisticated phishing attempt and report it to the proper internal channels. The majority of the VMW workforce is remote and was previously distributed globally even before the pandemic; email and instant messaging are the primary methods of communicating with other employees and email is the primary method of communicating with customers/other external contacts. The CSO, and subsequently the Security and Resiliency team will oversee the content of the new Online Threat Awareness course and partner with the VP of Governance, Risk, Compliance and Assurance to operationalize the live phishing simulations, Data Analytics (falling under Governance, Risk Compliance and Assurance umbrella) will evaluate, measure and report on the awareness campaign's effectiveness.

Protective Technologies

In Module 5, you compiled a list of questions you would ask to understand the technologies implemented to protect your organization's critical systems, networks, and data. In this section, based on the questions you asked and by conducting any other additional research, identify technologies your organization can employ to protect its critical systems, networks, and data.

If you are using the Sony case, recommend protective technologies that could have addressed Sony's shortcomings in protecting their critical networks, systems, and data.

Note:
This question requires you to submit a paragraph consolidating the information you learned, and is not a resubmission of the questions you submitted in Module 5.

(Write approximately 650 words)

Start writing here:

VMW is a data virtualization company and primarily conducts business with its customers via cloud application building and hosting services; customers therefore rely on cloud infrastructure's Confidentiality, Integrity, and 100% Availability to conduct business.
To address the challenges the organization faces in keeping its IaaS network assets secured, the company will continue to use cutting edge tools and technologies for identity and access management such as multi-factor authentication and token authentication; computer network management such as private network services and IP address management; managed network security solutions such as firewalls and network segregation; and intrusion detection and protection systems (IDPS) such as Carbon Black Cloud (CBC).

As part of the VMW EISP, all VMW networks must firstly be designed to ensure Confidentiality, Integrity, and Availability. Network controls must then be effectively deployed and managed to protect Information Assets. Firewalls in particular are important since they are the first line of network defense. These configurations will be regularly reviewed and audited. Reviews will employ tools that scan and test for vulnerabilities, perform rule analysis, and evaluate integrity of the architecture. The Security and Resiliency team will be responsible for performing such reviews.

To manage firewall intrusion risk, the following firewall attributes and practices will be required at minimum:

- Only VMW approved access methods shall be used to connect to its networks and network services, keeping in line with the organization's Zero Trust to Information Security
- 'Default Deny' firewall configuration(s) will be applied
- Firewalls will be placed at *every* Internet connection
- All connections initiated from or destined to the Internet will pass through a firewall
- Network traffic with invalid source or destination addresses will be blocked
- inbound connections to VMware systems from the Internet will terminate in a De-Militarized Zone or DMZ

To protect PHI, PCI, and PII data, VMW will use tools and practices in line with recommendations from industry authorities such as NIST, ISO, and CIS such as Dynamic Data Masking [30] and de-identifying and re-identifying sensitive data records via algorithm (removing account numbers, SSNs, names, addresses, and any other attributes that could be used to identify an individual).

Identity and Access Management must be simple and secure; the goal is not to interfere with productivity to achieve Information Security. Minimum IAM standards to protect Confidentiality, Integrity, and Availability of critical data stores:

- federated single sign on (SSO) will be integrated with existing internal identity management platforms
- strong passwords, i.e. upper and lowercase letters, numbers, inclusion of a special character, minimum character length, are required to protect customers and employees
    - Temporary access keys will be used to eliminate the use of long-term credentials

Network Intrusion Detection and Prevention Systems (IDPS) will be used to monitor traffic for malicious activity. Active real-time monitoring capabilities will be used in particular to detect changes to privileged accounts. Compliance and Behavior Monitoring on VMW imaged devices is required to ensure conformity to security configuration standards. Carbon Black Cloud will be deployed enterprise wide. Proper event logging remains crucial for VMW not only for proper threat detection and response, but also for auditing accountability. Logging capabilities must be enabled and maintained specifically for Carbon Black AppControl [31] as this tool allows VMW to record user actions relevant to internal Information Security such as:

- application certificate approvals and usage
- file approvals and usage, sensor updates
- unapproved files or software
- application executions and user activity across VMW's networks
- denied or rejected firewall connections

To protect information hosted within the cloud:

- Risk assessments of all applications, servers, and data hosted will be performed
    - Privacy and Cybersecurity legal must review and sign off before going live
- Container and workload penetration testing will be done on a regular basis
- External IP addresses will be scanned on a regular basis by VMW
    - Logs and reports will be generated for review by Security Operations, Vulnerability Management and other team within Security and Resiliency

- Data leak and loss prevention tools will be employed to ensure compliance with PCI, Sarbanes-Oxley (SOX), and HIPAA

Legal Considerations

In Module 6, you compiled a list of questions you would direct towards an organization's senior management and general counsel in order to gauge the organization's legal risk mitigation strategy and the adequacy of their preparations. In this section, based on the questions you asked, and by conducting any other additional research, discuss the legal considerations your organization should take into account when compiling its risk mitigation strategy.

If you are using the Sony case, recommend steps that could have addressed Sony's shortcomings in protecting themselves from legal action.

> **Note:**
> This question requires you to submit a paragraph consolidating the information you learned, and is not a resubmission of the questions you submitted in Module 6.

(Write approximately 550 words)

Start writing here:

VMW customers, employees and applicants, contractors, and partners expect the company to demonstrate compliance with global privacy laws and uphold standard privacy practices in processing their personal data. Privacy laws around the world govern how VMW can process personal data. Privacy informs the company's overall risk strategy, as it is subject to over 100 privacy laws and regulations across the globe. VMW will use the European Union's General Data Protection Regulation, or GDPR, as an enterprise baseline standard for its data handling since there is no US equivalent currently. However, the VMW Privacy and Cybersecurity Legal Counsel will collaborate with Data Governance and Information Security Compliance to continuously monitor and assess new laws, regulations and trends as they emerge.

VMW will keep the following privacy basics at the focal point of its risk mitigation strategy:

- **Transparency in how personal user data is processed**. A Data Processing Agreement will be made to detail contractual obligations on behalf of VMW. VMW will only collect, hold, and use personal user data or information submitted by users to the product/service for processing only as instructed or authorized by the user and not for any other purpose.
- **Implementation of controls to safeguard and protect personal user data, in alignment with the EISP and overall company mission.** Confidentiality, Integrity, Availability, and overall Information Security must be always maintained. VMW solutions are architected with 'security by design' for compliance with existing legislation such as Payment Card Industry (PCI) Data Security Standards (DSS), Federal Information Security Management Act (FISMA), and the Health Insurance Portability and Accountability Act (HIPAA).
- **Implementation of data retention and deletion policies**. Personal data will be kept in a form that permits identification of the individual for no longer than is necessary,

and only for the purposes for which it was processed. Data retention standards will be built into the product; for example: retention period option cannot be ‘indefinite’.

- **Implementation of mechanisms that allow users to access and delete their data upon request**. Users have rights and choices to update, correct, withdraw, revoke consent, erase, restrict, or otherwise object to their data where VMW acts as a processor. Privacy Notices for each use case will be publicly available. Users will also be able to contact the Privacy team directly via the official company website.
    - *Note: VMW is legally bound to comply if subpoenaed by a government to access customer data and content. VMW will notify any customer of such a request in a timely manner. Additionally, the company operates several offices in Europe as well as contracts with several EU-based public and private companies. In the case of a GDPR subject rights request, VMW is a processor; there are direct compliance/accountability obligations placed on processors (keeping records of processing, reporting to the data controller, implementing adequate data security). Individual, contractual data handling terms will still apply.*
- **Timely notification of any suspected or confirmed data breaches.** VMW has a dedicated Security and Resiliency team led by the CISO. Breach Incident response procedures are documented and tested regularly to ensure that in a confirmed breach situation VMW can notify not only users but law enforcement, as well as prove that privacy measures were in place to significantly lower the risk of a security event. VMW would also transparently collaborate with sector-information sharing organizations in the event of an attack to share, learn and improve its security.

Incident Response Plan (not required)

Note:
The incident response plan is a central part of an organization’s cyber risk mitigation strategy. However, as you will not have an opportunity to revise your plan based on your Tutor’s feedback in time for Module 8, you are **not** required to integrate it into your final risk mitigation strategy. Please consult the grading breakdown in the Orientation Module course handbook for more information.

Bibliography

[1] Comparably. 2022. *VMware Mission, Vision & Values*. Available: https://www.comparably.com/companies/vmware/mission [2022, March 12].

[2] Raina, K. 2021. *Zero Trust Security Explained: Principles of the Zero Trust Model*. Available: www.crowdstrike.com/cybersecurity-101/zero-trust-security/ [2022, March 19].

[3] FedRAMP.gov. 2022. *A FEDRAMP AUTHORIZATION BOUNDARY.* Available: https://www.fedramp.gov/assets/resources/documents/CSP_A_FedRAMP_Authorization_Boundary_Guidance.pdf [2022, April 18].

[4] National Institute of Standards and Technology. 2004. *Standard for Security Categorization of Federal Information and Information Systems.* Available: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf [2022, April 18].

[5] Kerner, S. 2017. *VMware Outlines 5 Pillars of Cyber Hygiene.* Available: https://www.esecurityplanet.com/threats/vmware-outlines-pillars-of-cyber-hygiene/ [2022, April 18].

[6] VMware, Inc. 2022. *Workspace ONE Unified Endpoint Management.* Available: https://www.vmware.com/products/workspace-one/unified-endpoint-management.html [2022, April 18].

[7] VMware, Inc. 2022. *VMware NSX*. Available: https://www.vmware.com/products/nsx.html [2022, April 18].

[8] SecureCoding.com. 2021. *OWASP Secure Coding Checklist*. Available: https://www.securecoding.com/blog/owasp-secure-coding-checklist/ [2022, April 18].

[9] Balbix. 2022. *What are CVSS Scores*. Available: https://www.balbix.com/insights/understanding-cvss-scores/ [2022, April 18].

[10] Kesten, G. 2021. *What are the Top Cloud Computing Security Risks?* Available: https://www.mimecast.com/blog/cloud-computing-security-risks/#_edn1 [2022, March 4].

[11] Vailshery, L. 2022. *Share of corporate data stored in the cloud in organizations worldwide from 2015 to 2021.* Available: https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/ [2022, March 3].

[12] Cybersecurity & Infrastructure Security Agency. 2022. *Alert (AA22-040A) 2021 Trends Show Increased Globalized Threat of Ransomware*. Available: https://www.cisa.gov/uscert/ncas/alerts/aa22-040a [2022, April 18].

[13] Lapienytė, J. 2021. *We may be closer to cyberwar than ever before, study about nation-states concludes*. Available: https://cybernews.com/news/we-may-be-closer-to-cyberwar-than-ever-before-study-about-nation-states-concludes/ [2022, April 18].

[14] VMware Global Communications. 2022. *VMware Statement Regarding Ukraine.* Available: https://news.vmware.com/releases/vmware-statement-regarding-ukraine [2022, March 5].

[15] Global Data Systems, Inc. 2022. *The Insider Threat Problem and What You Can Do About It.* https://www.getgds.com/resources/blog/cybersecurity/the-insider-threat-problem-and-what-you-can-do-about-it#:~:text=But%20what%20many%20organizations%20overlook,follow%20best%20cyber%20security%20policies. [2022, April 18].

[16] Spencer, T. 2019. *How to Identify Your Company's Cybersecurity Risks.* Available: https://www.nist.gov/blogs/manufacturing-innovation-blog/how-identify-your-companys-cybersecurity-risks#:~:text=Background%20checks%20are%20essential%20to,Criminal%20background%20checks [2022, April 18].

[17] Lakshmanan, R. 2022. *FBI, CISA Warn of Russian Hackers Exploiting MFA and PrintNightmare Bug.* Available: https://thehackernews.com/2022/03/fbi-cisa-warn-of-russian-hackers.html [2022, April 18].

[18] F5, Inc. 2022. *Phishing Attacks Soar 2020% During COVID019 Peak as Cybercriminal Opportunism Intensifies*. Available: https://www.f5.com/company/news/features/phishing-attacks-soar-220--during-covid-19-peak-as-cybercriminal [2022, April 2022].

[19] Aguilar, B. 2020. *VMware Expands Leadership Team with New Information Technology and Digital Transformation Appointments*. Available: https://news.vmware.com/company/vmware-cio-cdto-news [2022, March 19].

[20] Mazzoli, R. 2021. *Center for Internet Security (CIS) Benchmarks*. Available: https://docs.microsoft.com/en-us/compliance/regulatory/offering-cis-benchmark [2022, March 20].

[21] Scholl, F. 2022. *The Path to Improved Cybersecurity Culture.* Available: https://quonline.quinnipiac.edu/blog/path-to-improved-cybersecurity-culture.php [2022, April 18].

[22] Nathans, D. 2015. *Designing and Building Security Operations Center.* Waltham, MA: Syngress, pp.85-100.

[23] US Department of Homeland Security. 2016. *Cybersecurity Workforce Development Toolkit How to Build a Strong Cybersecurity Workforce*. Available: https://niccs.cisa.gov/sites/default/files/documents/pdf/cybersecurity_workforce_development_toolkit.pdf?trackDocs=cybersecurity_workforce_development_toolkit.pdf [2022, March 20].

[24] Zhao, J. 2022. *Third-Party Risk Management: Best Practices for Protecting Your Business*. Available: https://hyperproof.io/resource/third-party-risk-management/ [2022, April 18].

[25] Adair, A. (2022) 'Aniya Adair M2 U3 Ongoing Project'. Harvard University. Unpublished essay.

[26] Adair, A. (2022) 'Aniya Adair M3 U3 Ongoing Project'. Harvard University. Unpublished essay.

[27] Adair, A. (2022) 'Aniya Adair M4 U3 Ongoing Project'. Harvard University. Unpublished essay.

[28] Adair, A. (2022) 'Aniya Adair M5 U3 Ongoing Project'. Harvard University. Unpublished essay.

[29] Adair, A. (2022) 'Aniya Adair M6 U3 Ongoing Project'. Harvard University. Unpublished essay.

[30] Yaseen, A. 2016. *Using Dynamic Masking in SQL Server 2016 to protect sensitive data.* Available: https://www.sqlshack.com/using-dynamic-data-masking-in-sql-server-2016-to-protect-sensitive-data/ [2022, April 18].

[31] Netsurion. 2022. *Carbon Black (Cb) Protection*. Available: https://www.netsurion.com/knowledge-packs/cb-protection [2022, April 18].

Your ongoing project submission will be graded according to the following rubric:

4. Rubric

	Very poor	Poor	Satisfactory	Very good	Exceptional
Adherence to the brief *All sections in the template are completed.*	No submission, or student fails to address any element of the brief. (0)	Some key elements are not addressed. Most information provided is irrelevant. (5.5)	Student has adhered to most of the brief. Sufficient information is provided and is mostly relevant. (7)	Student has adhered to almost all elements of the brief. Almost all information is provided and is relevant. (8.5)	Student has fully adhered to the brief. All information provided is comprehensive and relevant. (10)
Introduction and vision *Student has clearly outlined the need for their risk mitigation strategy, and what it aims to*	No submission. OR Student fails to clearly outline the need for the strategy or its long-term vision. There is no evidence that	Student shows an incomplete understanding of the need for their strategy, or its long-term vision.	Student demonstrates satisfactory understanding of the need for their strategy, and its long-term vision.	Student demonstrates a strong understanding of the need for their strategy, and its long-term vision. The	Student demonstrates a thorough and incisive understanding of the need for their strategy, and its long-term vision. The student has been able to

achieve by implementing the strategy. *Student has thought critically and incorporated learnings from the content.*	the student has used the content covered in the course to inform their response. (0)	There is some evidence that the student has engaged with the content covered in the course but this is not always accurately applied. (5.5)	The student has clearly engaged with the content covered in the course, but a more nuanced answer is required. (7)	answer shows a strong grasp of the content. (8.5)	critically apply their learning from the course. (10)
Strategic goals and objectives *Student has outlined at least four strategic goals that will reduce their organization's risks to an acceptable level. They have included at least two objectives that clearly explain what must be done to achieve each goal.* *Student has thought critically and incorporated learnings from the content.*	No submission. OR Student fails to clearly outline their strategy's goals and objectives. There is no evidence that the student has used the content covered in the course to inform their response. (0)	Student shows an incomplete understanding of their strategy's goals and objectives. There is some evidence that the student has engaged with the content covered in the course but this is not always accurately applied. (5.5)	Student demonstrates satisfactory understanding of their strategy's goals and objectives. The student has clearly engaged with the content covered in the course, but a more nuanced answer is required. (7)	Student demonstrates a strong understanding of their strategy's goals and objectives. The answer shows a strong grasp of the content. (8.5)	Student demonstrates a thorough and incisive understanding of their strategy's goals and objectives. The student has been able to critically apply their learning from the course. (10)

Metrics *The student has listed at least three metrics their organization could use to measure the achievement of their goals, and the metrics are specific to the goals/objectives identified.* *Student has thought critically and incorporated learnings from the content.*	No submission. OR Student fails to list three metrics their organization could use to measure cybersecurity. The metrics are not specific to the identified goals/objectives. There is no evidence that the student has used the content covered in the course to inform their response. (0)	Student shows an incomplete understanding of metrics their organization could use to measure its cybersecurity. The metrics lack relevance to the identified goals/objectives. There is some evidence that the student has engaged with the course content, but this is not always accurately applied. (5.5)	Student demonstrates satisfactory understanding of the metrics their organization could use to measure its cybersecurity and they are relevant to the goals and objectives identified. The student has clearly engaged with the course content but a more nuanced answer is required. (7)	Student demonstrates a strong understanding of the metrics their organization should use, and they are specific to the goals/objectives identified. The answer shows a strong grasp of the content. (8.5)	Student demonstrates a thorough and incisive understanding of the metrics their organization can use, and they are specific to the goals/objectives identified. The student has been able to critically apply their learning from the course. (10)
Cybersecurity threat actors *Student has identified at least two threat actors and described a scenario of an attack.* *In the case of Sony, student has accurately identified the threat actor and method of attack in the 2014 hack, as*	No submission. OR Student fails to list two threat actors that could attack their organization. They have not provided a possible method of an attack. There is no evidence that the student has used the course content to	Student shows an incomplete understanding of the threat actors who could attack their organization and the possible method of attack. There is some evidence that the student has engaged with the course	Student demonstrates satisfactory understanding of the threat actors who could attack their organization and the possible method of attack. The student has clearly engaged with the course	Student demonstrates a strong understanding of the threat actors who could attack their organization and the possible method of attack. The answer shows a strong	Student demonstrates a thorough and incisive understanding of the threat actors who could attack their organization and the possible method of attack. The student has been able to critically apply their learning from the course. (10)

well as one other potential threat actor. *Student has thought critically and incorporated learnings from the content and has applied this to their chosen organization.*	inform their response. (0)	content, but this is not always accurately applied. (5.5	content but a more nuanced answer is required. (7)	grasp of the content. (8.5)	
Business critical assets *Student has identified the assets that are most essential to their organization, and described vulnerabilities these assets may be exposed to.* *Student has thought critically and incorporated learnings from the content.*	No submission. OR Student fails to identify the assets that are critical to their organization and accurately describe how these assets are vulnerable. There is no evidence that the student has used the course content to inform their response. (0)	Student shows an incomplete understanding of their organization's critical assets, and how they are vulnerable. There is some evidence that the student has engaged with the course content but this is not always accurately applied. (5.5)	Student demonstrates satisfactory understanding of their organization's critical assets, and how they are vulnerable. The student has clearly engaged with the course content but a more nuanced answer is required. (7)	Student demonstrates a strong understanding of their organization's critical assets, and how they are vulnerable. The answer shows a strong grasp of the content. (8.5)	Student demonstrates a thorough and incisive understanding of their organization's critical assets, and how they are vulnerable. The student has been able to critically apply their learning from the course. (10)

Cybersecurity governance *Student has recommended cybersecurity leadership plan, improvements to management processes, and a cybersecurity awareness training program.* *Student has thought critically and incorporated learnings from the content.*	No submission. OR Student fails to recommend a cybersecurity leadership plan, improvements to management processes, and a cybersecurity awareness training program. There is no evidence that the student has used the course content to inform their response. (0)	Student shows an incomplete understanding of cybersecurity leadership plans, management processes, and cybersecurity awareness training programs. There is some evidence that the student has engaged with the course content but this is not always accurately applied. (5.5)	Student demonstrates satisfactory understanding of cybersecurity leadership plans, management processes, and cybersecurity awareness training programs. The student has clearly engaged with the course content but a more nuanced answer is required. (7)	Student demonstrates a strong understanding of cybersecurity leadership plans, management processes, and cybersecurity awareness training programs. The answer shows a strong grasp of the content. (8.5)	Student demonstrates a thorough and incisive understanding of cybersecurity leadership plans, management processes, and cybersecurity awareness training programs. The student has been able to critically apply their learning from the course. (10)
Protective technologies *Student has accurately identified protective technologies that are, or should be, implemented to enhance their organization's cybersecurity.* *Student has thought*	No submission. OR Student fails to identify protective technologies that are, or should be, implemented to enhance their organization's cybersecurity. There is no evidence that the student has used the course content to	Student shows an incomplete understanding of the necessary protective technologies that are, or should be, implemented to enhance their cybersecurity. There is some evidence that the student has engaged with the content	Student demonstrates satisfactory understanding of the technologies that are, or should be, implemented to enhance their cybersecurity. The student has clearly engaged with the course	Student demonstrates a strong understanding of the technologies that are, or should be, implemented to enhance their cybersecurity. The answer shows a strong grasp of the content. (8.5)	Student demonstrates a thorough and incisive understanding of the technologies that are, or should be, implemented to enhance their cybersecurity. The student has been able to critically apply their learning

critically and incorporated learnings from the content.	inform their response. (0)	covered in the course but this is not always accurately applied. (5.5)	content but a more nuanced answer is required. (7)		from the course. (10)
Legal considerations *Student has critically analyzed the legal considerations their organization should take into account.* *Student has thought critically and incorporated learnings from the content.*	No submission. OR Student fails to critically analyze the legal considerations their organization should take into account. There is no evidence that the student has used the course content to inform their response. (0)	Student shows an incomplete understanding of legal considerations that their organization should take into account. There is some evidence that the student has engaged with the course content but this is not always accurately applied. (5.5)	Student demonstrates satisfactory understanding of legal considerations that their organization should take into account. The student has clearly engaged with the course content but a more nuanced answer is required. (7)	Student demonstrates a strong understanding of the legal considerations their organization should take into account. The answer shows a strong grasp of the content. (8.5)	Student demonstrates a thorough and incisive understanding of the legal considerations their organization should take into account. The student has been able to critically apply their learning from the course. (10)
Application of course content to organizational context *The student has accurately applied the learnings from the course content to their own organization or*	No submission OR The student has not made use of their organization's unique organizational context and constraints to inform their response (0)	Student has demonstrated a limited understanding of their organization's unique context and constraints and context (5.5)	Student has demonstrated a satisfactory understanding of their organization's context and constraints, however a there is room for deeper engagement	There is clear evidence that the student has thought about their organization's unique context and constraints, and catered for this in their strategy accordingly. (8.5)	There is strong evidence that the student has understood and thought carefully about their organization's unique context and constraints, and has provided considered recommendations in their strategy accordingly. (10)

Sony's unique context.			with its nuances. (7)		
Organization of writing *Answer should be structured clearly and logically.*	No submission or complete lack of logical structure. (0)	Answer has some logical structure, but not enough to justify a passing grade. (5.5)	Answer is structured fairly well in terms of logic and clarity. (7)	Answer is structured very well in terms of logic and clarity. (8.5)	Answer is structured exceptionally well in terms of logic and clarity. (10)

Total: 110 points