Sub-Category	Control Objective
Asset Management	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
Asset Management	
Asset Management	
Asset Management	
Asset Management	
Asset Management	
Business Environment	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
Business Environment	
Business Environment	
Business Environment	
Business Environment	

Governance	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
Governance	
Governance	
Governance	
Risk Assessment	The organization understands the cybersecurity risk to organizational operations, organizational assets, and individuals.
Risk Assessment	
Risk Assessment	
Risk Assessment	
Risk Assessment	
Risk Assessment	
Risk Management Strategy	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
Risk Management Strategy	
Risk Management Strategy	

Control description
Physical devices and systems within the organization are inventoried.
Software platforms and applications within the organization are inventoried.
Organizational communication and data flows are mapped.
External information systems are catalogued.
Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality and business value.
Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established.
The organization's role in the supply chain is identified and communicated.
The organization's place in critical infrastructure and its industry sector is identified and communicated.
Priorities for organizational mission, objectives and activities are established and communicated.
Dependencies and critical functions for delivery of critical services are established.
Resilience requirements to support delivery of critical services are established.

Organizational information security policy is established.
Information security roles and responsibilities are coordinated and aligned with internal roles and external partners.
Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.
Governance and risk management processes address cybersecurity risk.
Asset vulnerabilities are identified and documented.
Threat and vulnerability information is received from information sharing forums and sources.
Threats, both internal and external, are identified and documented.
Potential business impacts and likelihoods are identified.
Threats, vulnerabilities, likelihoods and impacts are used to determine risk.
Risk responses are identified and prioritized.
Risk management processes are established, managed and agreed to by organizational stakeholders.
Organizational risk tolerance is determined and clearly expressed.
The organization's determination of risk tolerance is informed by its role in critical infrastructure.

Questions to ask	Pass/Fail
1. Do you have an up to date CMDB or asset inventory of all physical (hardware) devices? 2. How do you perform periodic review on the CMDB to ensure that it's accurate and up to date?	Pass
1. Do you have an up to date CMDB or asset inventory of all software assets such as critical applications? 2. How do you perform periodic review on the CMDB to ensure that it's accurate and up to date?	Fail
1. Do you have clear, up to date, network diagrams - including the cloud environment?	Pass
1. Does your CMDB include Software-as-a-Service (SaaS) instances catalogued and classified as per sensitivity and criticality? 2. Do you have an up to date inventory of all third party suppliers?	Fail
1. Are assets in the CMDB classified based on sensitivity and criticality?	Fail
1. Are cyber security roles and responsibilities defined? 2. Is there a clear information security policy outlining roles and responsibilities for cyber security (including third party suppliers)?	Fail
1. Does the organisation have clear documentation outlining their role within their own supply chain when it comes to cyber security?	Fail
1. Is this organisation considered 'critical infrastructure'?	N/A
1. Does the organisation have a clear business strategy and mission statement?	Pass
1. Does the organisation have key critical services and applications inventoried and classified? 2. Does the organisation have business continuity plans and disaster recovery plans for key critical services?	Fail
1. Determine if the organization's business continuity and disaster recovery plans support resilience of critical services.	Pass

1. Does the organisation have an information security policy?	**Fail**
1. Have information security roles and responsibilities been documented and communicated with internal and external stakeholders?	**Fail**
1. Are the organisation's legal and regulatory responsibilities from an information security point of view well documented?	**Fail**
1. Does the organisation have mature processes and procedures to manage cyber security risks? 2. Does the board have oversight of information security issues?	**Fail**
1. Are vulnerability scans conducted and vulnerabilities analysed and documented?	**Fail**
1. Does vulnerability management program include subscriptions to threat intelligence sources?	**Fail**
1. Have cyber security threat assessments been conducted? 2. Have threat actors been identified, assessed, and documented?	**Fail**
1. Do cyber security risk assessments include business impact and likelihood?	**Fail**
1. Does the risk assessment process identify threats, vulnerabilities, likelihood and potential damage?	**Fail**
1. Are recommendations/outcomes of the risk assessment process prioritised based on criticality and impact?	**Fail**
1. Has the risk management process been endorsed by senior management?	**Fail**
1. Has the organization defined and approved a cyber risk appetite statement?	**Fail**
1. If the organisation is considered critical infrastructure, does the cyber risk tolerance take this into consideration?	**N/A**

Comments
IT team has spreadsheet with laptop serial numbers, models, and warranty details. Needs periodic reviews.
Office365 and SaaS applications are not catalogued in CMDB. Software assets should be added to CMDB and classified per sensitivity and criticality.
IT team has up to date network diagrams including cloud environment.
SaaS applications (Office365, Horizon Labs) and third-party suppliers are not inventoried or classified.
No asset classification program in place. Assets need to be classified based on criticality and sensitivity.
Cybersecurity roles and responsibilities haven't been defined. Currently assigned to IT team without clear delineation. No information security policy exists.
Oscorp does not have a process to manage cyber security supplier risk. Third-party suppliers not mapped or classified.
Oscorp is not a critical infrastructure organisation.
CEO has clear business strategy for the business.
While BC/DR plans exist, critical assets and services are not inventoried and classified. Need clear list of key critical assets.
IT team conducts regular disaster recovery testing, has clear documented business continuity plans, and takes regular tested backups.

Only generic IT policy exists. No formal information security policy in place.
Information security roles and responsibilities have not been defined or communicated. Currently ad-hoc assignment to IT team.
Legal and regulatory cybersecurity requirements are not documented or managed.
Cyber security risks are not documented. Board has no visibility over cyber security risks. Only financial risk is managed.
Qualys scanner exists but used ad-hoc. Large number of high/severe vulnerabilities reported. No formal vulnerability management program.
No cyber security function to subscribe to and monitor threat intelligence sources.
No cyber security threat assessments conducted. Threat actors not identified.
No cyber security risk assessment process in place.
No cyber security risk assessment process exists.
No risk assessment process to generate prioritized recommendations.
No cyber security risk management process exists. Only financial risk is managed.
No cyber risk appetite or tolerance defined.
Oscorp is not a critical infrastructure organisation.