PUBLIC AND PRIVATE SECTOR TEMPLATE
CYBER SECURITY PRODUCT REVIEW AS-IS | TO-BE PROCESS CAPTURE
Story-Boarding and Planning Phase

REMAINING ISSUES TO SOLVE

ISSUES TO SOLVE
A) EASY HAND OFF WITHIN CYBER
b) MCDONALDS MENU – FOR EASE OF EXPLANAINTION TO OUR CUSTOMER
c) SHOW STOPPERS FULLY IDENTIFIED
D) MINIMUM QUALIFICATIONS – IF A MIX OF MATRIX ITEMS ARE MISSING KILL IT
e) NOTE 339 admin accounts reduced to 39 during this process creation
f) HOW TO REMOVE / REVIEW NON-SANCTIONED APPS
G) PCARD LOGIC – IF THEN ELSE (WHO HAS THEM / RULES GOVERNING
H) BID PROCESS SPAWNS REVIEW- NOT BAKED IN
I) PROCUREMENT reQUESTS CAN ALSO TRIGGER REVIEW
J) SOLIDIFY CYBER HANDLING OF REVIEW PROCESS
K) SUGGEST AREAS TO SDMS TO STRENGTHEN THEIR PROCESS
L) CLOUD APPS EASIEST TO CIRCUMMVENT SYSTEM__ FIX

- Provide software or hardware to County;
- Connect to the County network;
- Provide services over a network (i.e., cloud-based services, etc.)
- Access or store County department or agency data.

PRODUCT IDENTIFIED FOR PURCHASE

EXTERNAL PROCESS

DEPARTMENT NEED

PRODUCT UPGRADE OR REPLACE

K

A.1 RQS SDM
Requests primarily originate through SDMs, although users also directly ask for reviews on occasion

A.2
Requests from the Licensing department's users may not always include management approval

A.3 SDM
Upon receiving the req, the SDM conducts prequalification, which involves reviewing existing tools that may fulfill the req. While there is no formal list available, there is a partial list documented in SNOW.

A.4 RQS SDM
After establishing that the tool is not present in our environment, the SDM initiates the search for a suitable product to fulfill the req. The requestor also has the option to specify a particular product if desired

A.5
At this stage, the SDM dispatches the relevant NIST-based cybersecurity questionnaire to the vendor to verify that all criteria are met

A.6
The SDM creates a SNOW ticket and dispatches it to the relevant teams: Network, Server, Cyber, EIS, and Desktop.

A.7
Upon receiving the questionnaire, tasks are generated for approvals

A.8
Teams review the questionaire, conducting a detailed exam of the form and researching the background of the org providing the product. As a result of this process, new meetings may be initiated for various reasons, including reviewing exceptions.

A.9
Approval or denial is the central aspect of this process and must be managed to prioritize effective decision-making for the security posture of HC, rather than focusing on assigning blame.

A.10
Upon approval, the SDM provides the research package to the requestor, who subsequently submits the product for procurement.

A.11
If denied or if any of the teams reject the product, detailed information is provided to outline corrective measures. Once verification is completed that the issue has been mitigated, approval may be granted.

THINK TANK AREA T1

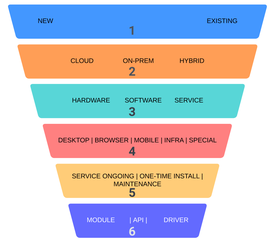
A

INITIAL INQUIRY AND EVALUATION

- M1 Utilize the R1 matrix to initiate scoping and assess the level of effort required. Guideline only
- M2 Utilize the R2 matrix to evaluate the overall health of the potential partner entity.
- M3 Incorporate R3 matrix elements into the investigation of the target product.
- M4 Utilize the R4 matrix to identify compliance and other relevant factors. This stage serves as a structured tool to explore certifications, thereby enhancing scrutiny of areas for investigation. The underlying idea is that certifications such as SOC 2 validate that an accredited body has assessed the organization's environment as "secure" for enterprise computing. While not a universal solution, certifications efficiently tackle and satisfy aspects outlined in our initial questionnaire. Vigilance is continuous, continuously improving our decision-making process.
- M5 To ensure compliance with our organizational standards and to optimize service delivery, we maintain a policy of working *exclusively with *local
- M6 Types of sensitive data to ensure all types are taken into account when validating for approval.

B

OBJECTIVE IS TO EXPERTLY VET PRODUCTS COMING INTO THE ENTERPRISE



C

ATTEMPT COMPLEXITY MATRIX

No existing data, use matrix approach starting from scratch	Existing applications have a source to begin investigating viability in the enterprise
	Product will be hosted, on-prem, or both. Level of complexity rises if not a pure cloud engagement.
Hardware can be straight forward if it does not need network access and connectivity.	
Browser and Mobile can be straightforward as it implies cloud based or non-network attached.	Desktop, infrastructure, and special items infer life in the environment and will have reliance on firewall, encryption, authentication, versions – and more…
Contract details and access to our systems is the research focal point	
Is it possible to gain access to the underlying server or database through the API endpoints? Does the API disclose any sensitive information? Can an attacker see other user's data?	
DETAIL ARTIFACTS THAT BELONG IN THE DIRECTORY USING THE FOLLOWING NAMING CONVENTION: 1. VENDOR QUESTIONAIRRES 2. PO / QUOTES / SOM COMMS 3. ALL COMMUNICATION PERTAINING TO INTERVIEWS AND DATA COLLECTION METHODS TO ARRIVE AT CONCLUSION 4. STATEMENT OF REASON WHY ACCEPTED OR DENIED	ISSUE IDENTIFICATION CYBER SOLVES FOR AUTHENTICATION METHODS ENCRPTION ABILITY TO AUDIT FW PORTS NEEDED FOR OPERATION <Get K's Least common denominators>

NOTES FOR PERIMETER G

Written problem statement on what business problem this product solves.

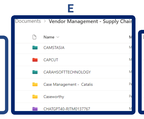
Write a clear definition of what the product does

1 through 6 must be defined on the way in - this will cut down on turn around time and risk. Format will make it easier for users to understand their product and what theyre asking for
DEFINE CONE OF SILENCE ENTIES FROM PERIMETER

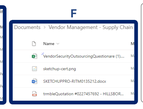
D

PRODUCT FOLDER COLOR CODE
- APPROVED
- IN FLIGHT | INCOMP
- DENIED
- PENDING HIGHER APPROVAL

E



F



THREE-VALUED LOGIC T2

WRONG		RIGHT
No SAML		Supports SAML
No MFA		Multi-Factor Authentication
No User and Data Audit Trail		Has User and Data Audit Trail
No User Authentication		Has User Authentication
Abnormal Firewall Permissions		Normal Firewall Permissions
M6 No Data Classification		Has Data Classification M6
M1 Companies Tier D and Below		Economically Viable A or B M1
M2 Better Business Bureau rating = F		Better Business Bureau rating = A M2
M2 Does Not Comply With SEC Reporting		Complies With SEC Reporting NUB M2
M2 Breached | Hacked multiple times	TIER C	Breach Free | Never been Hacked M2
M2 Controversial Entaglements		No Controversial Entaglements M2
M3 No Business Justification		Clear and Concise Business Justification M3
M3 No Questionairre		Properly Filed Questionairre M3
M4 No Legal Certifications		Legal Certifications - Retention | Ownership M4
M4 No Compliance Certifications		Compliance Certifications M4
M5 Sanctioned		Free and Clear M5

Above illustrates three-valued logic, encompassing absolute right, absolute wrong, and maybe also recognized as Engineering logic. The examples delineate, on a gradient scale, the most correct and incorrect scenarios. Although no products are flawlessly perfect, the objective is to lean more towards correctness than incorrectness when assessing eligibility for the enterprise.

DATA TYPES T3 M6

- PII • **Personal Identifiable Information (PII)**: Information that can be used to identify a specific individual, such as name, social security number, date of birth, etc.
- PHI • **Protected Health Information (PHI)**: Health-related information that is protected under HIPAA (Health Insurance Portability and Accountability Act) in the United States.
- FI • **Financial Information**: Data related to financial transactions, banking details, credit card information, etc.
- IP • **Intellectual Property**: Trade secrets, patents, copyrights, and other proprietary information.
- CR • **Credentials**: Usernames, passwords, security questions and answers, authentication tokens, etc.
- SC • **Sensitive Corporate Data**: Strategic plans, internal communications, customer lists, etc.
- LCI • **Legal and Compliance Information**: Information subject to legal privilege or compliance regulations.
- GD • **Geolocation Data**: Information that can identify the geographical location of an individual or device.

FIREWALL SCORING T4

<1%	Trusted Network to DMZ	YES
80%	Internal Out	YES
10%	DMZ to External	YES
9%	External to DMZ	NO
<1%	External to Internal	NO
<1%	DMZ to DMZ	NO

PRODUCT REQUEST TYPES T5

A	Cloud Based Level of Effort and Complexity Easy - Normally the same day	70
B	ON-Premise - Server Based Level of Effort and Complexity High - 2 days to 1 month	
C	HYBRID- Both Cloud and On-Premise Level of Effort and Complexity High - 2 days to 1 month	
D	Desktop Application Level of Effort and Complexity High - 2 days to 1 month	
E	PLUG-INS | API | BOLT-ONs Level of Effort and Complexity Medium - Normally 1 to 3 days	
F	GENERAL OFFICE EQUIPMENT - Overhead projectors, Phones, other peripheals Level of Effort and Complexity Medium - Normally 1 to 3 days	
E	SPECIALIZED HARDWARE - Ligowave Level of Effort and Complexity High - 2 days to 1 month	

Escrow code (proper language to highlight insolvency or disagreement on secure coding)
Source Code reviewed and meet SSDLC standards, recent pentest with results

Plugins dont necessarily need a questionnarre
Develop type Mcdonalds menue of recurring items and develop criteria based on each

What is broken in generation 1 | pre-ARM
1. storage is inconsistent and lacks all data necessary to review
2. 2. There is no tracking data - ticket number etc...
3. No catagorization Cloud | on-prem | desktop | etc...

M1

ITEM	AREA TO BE ADDRESSED	ECONOMIC QUALIFICATION SCORING
A	**Tier A: Large-Cap Corporations**	These are the largest and most established corporations with the highest market capitalizations.Typically, large-cap companies have market caps exceeding $10 billion. They are often industry leaders with extensive global operations and diversified revenue streams. Examples of large-cap corporations include Apple Inc. (AAPL), Microsoft Corporation (MSFT), and Amazon.com Inc. (AMZN).
B	**Tier B: Mid-Cap Corporations**	Mid-cap corporations are smaller in size compared to large-cap companies but still substantial in market capitalization. Mid-cap companies generally have market caps between $2 billion and $10 billion. They may exhibit strong growth potential and offer investors opportunities for capital appreciation. Examples of mid-cap corporations include Zoom Video Communications Inc. (ZM), Square Inc. (SQ), and DocuSign Inc. (DOCU).
C	**Tier C: Small-Cap Corporations**	Small-cap corporations are relatively smaller companies with lower market capitalizations compared to large-cap and mid-cap companies. Small-cap companies typically have market caps below $2 billion. They may be younger, less established firms with higher growth prospects but also higher volatility. Examples of small-cap corporations include Etsy Inc. (ETSY), Twilio Inc. (TWLO), and Peloton Interactive Inc. (PTON).
D	**Tier D: Low-Cap Startups, Mom-n-Pop , Dirt Floor (lol)**	Low-cap corporations are newcomers, fewer employees and no real way to quanitfy future succesds Low-cap companies typically have market caps well below $2 billion. They are not established firms with out an ability to project viability, and possess risk Examples of small-cap corporations Cyberfox, IAT software

M2

ITEM	AREA TO BE ADDRESSED	BUSINESS INTELLIGENCE AND BACKGROUND SCORING
A	**Rank Market Segments**	Start by defining the market segments or industries that align with your enterprise product solution. industry verticals, company size, geographic location, and target demographics.
B	**Segmentation by Company Size**	Conduct research to understand current trends, challenges, and opportunities in the enterprise market. Identify which market segments are experiencing growth, demand, or innovation in terms of product adoption. (are they likely to go out of business)
C	**Assess Budget and Resources**	Evaluate the budget and resources available to different tiers of companies. Understand the typical budget constraints of companies in each tier. This will help determine the affordability and willingness to invest in enterprise software solutions.
D	**LEGAL Issue**	LEXUS/NEXXUS SCAN
E	**Have the been Breached**	https://haveibeenpwned.com/PwnedWebsites | https://www.gearbrain.com/data-breach-cybersecurity-latest-hacks-2633724298.html | https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ | https://privacyrights.org/data-breaches | https://electric.ai/blog/recent-big-data-breaches
F	**Recon: BBB | Legal | Financial Sound**	Create defintion
	Reputation and Reviews	https://www.trustpilot.com/search?query=bonfire
	IN USE AT OTHER GOVERNMENT AGENCIES	Are any Florida or other government agencies successfully using the product MORE TO COME –

M3

ITEM	AREA TO BE ADDRESSED	ENTERPRISE | BUSINESS QUALIFICATION
A	**Business Case: General Information:**	Vendor name, contact information, and point of contact. Product name and version.
B	**Product Overview: What Problem Does this Solve**	Description of the software solution and its intended purpose. Supported platforms and operating systems.
C	**Security Features**	Encryption capabilities (e.g., data encryption in transit and at rest). Access controls and authentication mechanisms. Audit logging and monitoring features.
D	**Data Protection**	Data handling practices and data privacy protections. Data retention policies and data disposal procedures. Measures to protect against data breaches and unauthorized access.
E	**Vulnerability Management**	Procedures for identifying, assessing, and remediating security vulnerabilities. Patch management processes and frequency of security updates. Integration with vulnerability scanning tools and threat intelligence feeds.
F	**Incident Response:**	Incident response procedures and protocols. Notification process for security incidents or breaches. Support and assistance provided in the event of a security incident.
G	**Third-Party Security**	Security practices and controls implemented by third-party vendors or subcontractors. Assurance of supply chain security and vendor risk management.
H	**Compliance and Certifications**	Evidence of compliance with industry standards and certifications (e.g., SOC 2, PCI DSS). Documentation of regulatory compliance in relevant jurisdictions.
I	**Security Testing and Assurance**	Results of security assessments, penetration tests, or code reviews. Independent security certifications or audits conducted by third-party assessors.
J	**Support and Maintenance**	Availability of technical support and customer service. Maintenance and update schedules. End-of-life support and product retirement policies.
K	**Contractual and Legal Considerations**	Terms and conditions of the vendor's software license agreement. Liability and indemnification clauses related to security incidents. Data ownership and intellectual property rights.
L	**Additional Documentation:**	Copies of security policies, procedures, and documentation. References or case studies demonstrating successful implementations.
M	**CYBER INSURANCE**	Proof of Cyber Insurance - secondary claims or those over $1m,
N	**FIRE WALL PORTS NECESSARY**	
O	**SERVICE ACCOUNTS NEEDED**	By evaluating the responses to these questions, organizations can assess the security capabilities and reliability of a vendor's software solution and make informed decisions about its suitability for their needs.
P	**ELEVATED PRIVILEDGES TO RUN**	

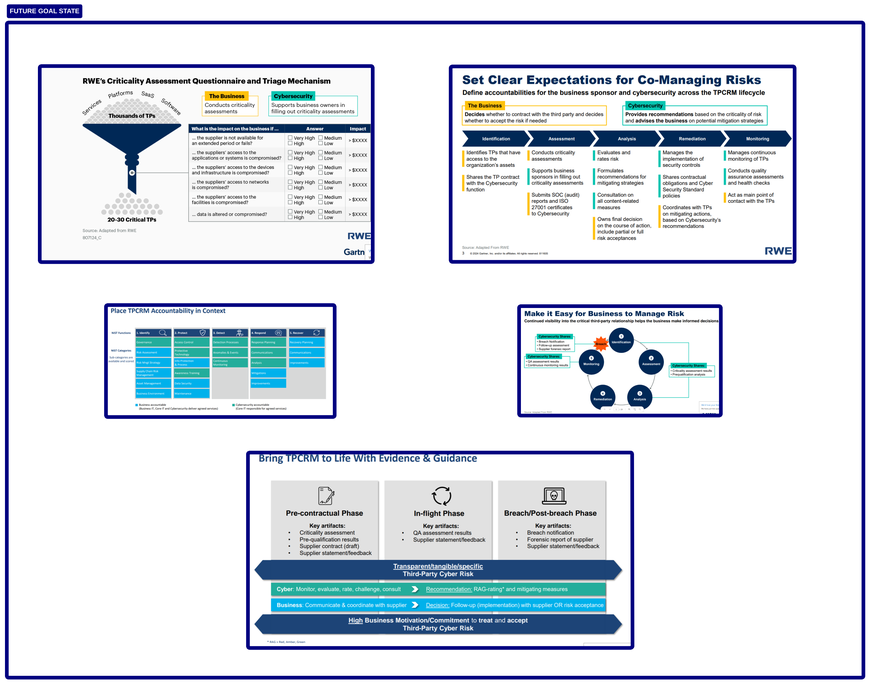
M4

ITEM	AREA TO BE ADDRESSED	COMPLIANCE CERTIFICATIONS HELD
A	**ISO 27001 & 02**	This certification validates that the cloud vendor follows international standards for information security management systems (ISMS). It ensures that the vendor has implemented robust security controls to protect data. **<Legal>**
B	**ISO 27002 & 01**	Together, the two standards provide a comprehensive starting point for an organization to establish risk-awareness and identify potential threats and vulnerabilities. **<Legal>**
C	**ISO 27018**	the international standard for protecting personal information in cloud storage. The term for the personal data it covers is Personally Identifiable Information or PII. ISO 27018 is a code of practice for public cloud service providers. **<Legal>**
D	**ISO 27017**	globally recognised framework that, when implemented, will effectively reduce the likelihood of data breaches and increase customer trust by demonstrating your commitment to information security techniques **<Legal>**
E	**SOC 1**	aims to control objectives within a SOC 1 process area and documents internal controls relevant to an audit of a user entity's financial statements. **<Legal>**
F	**SOC 2 Type II**	SOC 2 Type II certification confirms that the cloud vendor has adequate controls in place to safeguard customer data and ensure the security, availability, processing integrity, confidentiality, and privacy of the systems. **<Legal>**
G	**SOC 3**	an auditing procedure developed by the American Institute of Certified Public Accountants (AICPA) to demonstrate the strength of a service organization's internal controls over cloud and data center security **<Legal>**
H	**SOX (Sarbanes Oxley)**	the act of adhering to the financial reporting, information security and auditing requirements of the Sarbanes-Oxley (SOX) Act, a US law that aims to prevent corporate fraud. **<Legal>**
I	**SP 800-53**	provides a list of controls that support the development of secure and resilient federal information systems. These controls are the operational, technical, and management standards and guidelines information systems use to maintain confidentiality, integrity, and availability
J	**Industry-specific certifications:**	Depending on your industry, there may be additional certifications relevant to your organization's needs. For example, financial institutions may require compliance with regulations such as FINRA, FFIEC, or Basel III.
K	**GAAP**	sets out to standardize the classifications, assumptions and procedures used in accounting in industries across the US. The purpose is to provide clear, consistent and comparable information on organizations financials.
L	**Privacy Shield**	The EU Privacy Shield framework was developed by the U.S. and European Union to safeguard private data transmission between the two continents. The privacy shield agreement sets standards for both employee and customer data transfers, as well as any use of third party vendors
M	**COBIT**	is an IT governance framework for businesses wanting to implement, monitor and improve IT management best practices. COBIT is the acronym for Control Objectives for Information and Related Technologies.
N	**COPPA**	The Children's Online Privacy Protection Act (COPPA) includes a provision enabling industry groups or others to submit for Commission approval self-regulatory guidelines that implement the protections of the Commission's final Rule.
O	**HIPAA/HITECH (for healthcare)**	If your organization deals with sensitive healthcare data, ensure that the cloud vendor is compliant with Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) regulations. **<Legal>**
P	**GDPR (for handling EU data):**	If your organization operates within the European Union or handles EU citizen data, ensure that the cloud vendor complies with the General Data Protection Regulation (GDPR) requirements for data protection and privacy. **<Legal>**
Q	**FedRAMP (for government agencies)**	If your organization is a government agency or deals with government data, ensure that the cloud vendor has achieved Federal Risk and Authorization Management Program (FedRAMP) compliance, demonstrating adherence to rigorous security standards.
R	**PCI DSS (for payment card data):**	If your organization processes payment card transactions, ensure that the cloud vendor complies with Payment Card Industry Data Security Standard (PCI DSS) requirements for protecting cardholder data. **<Legal>**
S	**CSA STAR Certification:**	The Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) Certification is a comprehensive, third-party assessment of the security posture of cloud service providers.
T	**ITAR (for defense-related data)**	If your organization deals with defense-related data subject to International Traffic in Arms Regulations (ITAR), ensure that the cloud vendor complies with ITAR requirements for handling such sensitive information.
U	**CJIS (for law enforcement data):**	If your organization deals with criminal justice information, ensure that the cloud vendor complies with Criminal Justice Information Services (CJIS) Security Policy requirements.
V	**FINRA**	qualification you can earn from the Financial Industry Regulatory Authority (FINRA) to become a financial specialist such as a: Broker. Investment
W	**FISMA**	defines a framework of guidelines and security standards to protect government information and operations **<Legal>**
X	**SSAE 18**	is an auditing standard for service organizations. It is required by many industries and organization for vendors that provide them services. The examinations and audits of these Standards are known as SOC reports
Y	**ISAE 3402**	ISAE 3402 is a third party (mainly suppliers) assurance mechanism in the form of SOC (Service Organisation Controls). There are three kinds of SOC reports: SOC1 report - Relates to assurance on controls that could impact financial statements. SOC2 report - Relates to assurance on IT controls
Z	**HITRUST CSF**	HITRUST created and maintains the Common Security Framework (CSF), a certifiable framework to help healthcare organizations and their providers demonstrate their security and compliance in a consistent and streamlined manner.
AA	**Safe Harbor**	The term "safe harbor" means that through law, you're protected from a penalty when conditions are met. While the term applies to many areas of law, a major application of it is in taxation. Safe harbor can be applied to estimated taxes giving you some leeway in how much you need to pay.
BB	**GLBA**	The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data

M5

ITEM	AREA TO BE ADDRESSED	OFFSHORE DUE DILIGENCE
A	**DOMESTIC**	To ensure compliance with our organizational standards and to optimize service delivery, we maintain a policy of working *exclusively with *local or domestic companies. This approach enables us to uphold high cybersecurity and operational standards, maintain effective communication, and promote collaboration while supporting our local economy and workforce. This policy also aligns with our commitment to quality and efficiency in safe and secure service delivery.
B	**CANADA**	To ensure compliance with our organizational standards and to optimize service delivery, we maintain a policy of working *exclusively with *local or domestic companies. This approach enables us to uphold high cybersecurity and operational standards, maintain effective communication, and promote collaboration while supporting our local economy and workforce. This policy also aligns with our commitment to quality and efficiency in safe and secure service delivery.
C	**BUSINESS FRIENDLY COUNTRIES**	Exceptions to this policy may be examined on a case-by-case basis, subject to rigorous evaluation and approval by Cyber Security management. Such exceptions may be granted based on compelling business reasons that demonstrate clear benefits to our organization, including but not limited to specialized expertise not available locally or unique capabilities that significantly enhance project outcomes. Any exceptions granted will be documented and reviewed periodically to ensure ongoing alignment with our organizational goals and values.
D	**SANCTIONED OR WARNING COUNTRIES**	**Office of Foreign Assets Control** https://ofac.treasury.gov/sanctions-programs-and-country-information/sanctions-related-to-significant-malicious-cyber-enabled-activities https://ofac.treasury.gov/sanctions-programs-and-country-information https://www.treasury.gov/ofac/downloads/ssi/ssilist.pdf https://sanctionssearch.ofac.treas.gov/ **US Department of State** https://www.state.gov/economic-sanctions-programs/ https://www.state.gov/russia-business-advisory/

FUTURE GOAL STATE



CYBER CAPTURE PROCESS

INTERNAL CYBER PROCESS

S.1
APPROVAL RECIEVED THROUGH SNOW

S.2
NAVIGATE TO IIO / Vendore Management - Supply Chain Directory. Create a directory with the product name. This is ground zero where all related research will be stored.

PRODUCT FOLDER COLOR CODE
- APPROVED
- IN FLIGHT | INCOMP
- DENIED
- PENDING HIGHER APPROVAL

S.3
Create a word Document for research notes. Use the naming convention ProductName-RITM#

S.4
Most cases the RITM wll contain information about the product at a high level. Things such-as cloud , on-prem, mobile

S.5
RITM should also contain the Security questioniarre in most instances. Beging with reviewing the questionairre and then procede to evaluate the product using matrices R0 through R4

S.6
The goal of the preliminary research is using three value logic. scale. Absolute right maybe , and absolute wrong. The goal is to be closest to absolute right

S.7
ENTER PRODUCT INTO MICROSOFT APPLICATION RISK ASSESMENT https://security.microsoft.com/cloudapps/discovery

S.8
BEGIN PREQUALIFICATION RESEARCH | LOOK FOR QUCK HITS

S.9
USE T0 through T6 in conjunction with Security Questionairre. Some instances vendors won't supply this information. That is why the

S.10
Pre-qualification tops the hierarchy, offering vital insights for cyber-technical analysis. It greatly streamlines decision-making and clarifies our rationale to the requesting organization.

S.11
In some cases, further qualifications are needed, possibly requiring additional clarification from the requester. It's essential to verify that no other product in the environment can accomplish the same objective.

S.12
Further qualifications may entail contacting the vendor to address remaining cybersecurity concerns.

S.13
After addressing all security concerns, update the Word document mentioned in S3 and navigate to the RITM in SNOW and click 'approve'.

S.14
Before making the Determination check the SDM CS score as an additional measure for bringing new products into the environment.

S.15
If the score is higher additional scrutiny would be required. In the form of looking where the application may be stored and refer to the latest VS scan for Criticals and Highs. This would enhance overall posture if the environment score must be at a C-level or higher