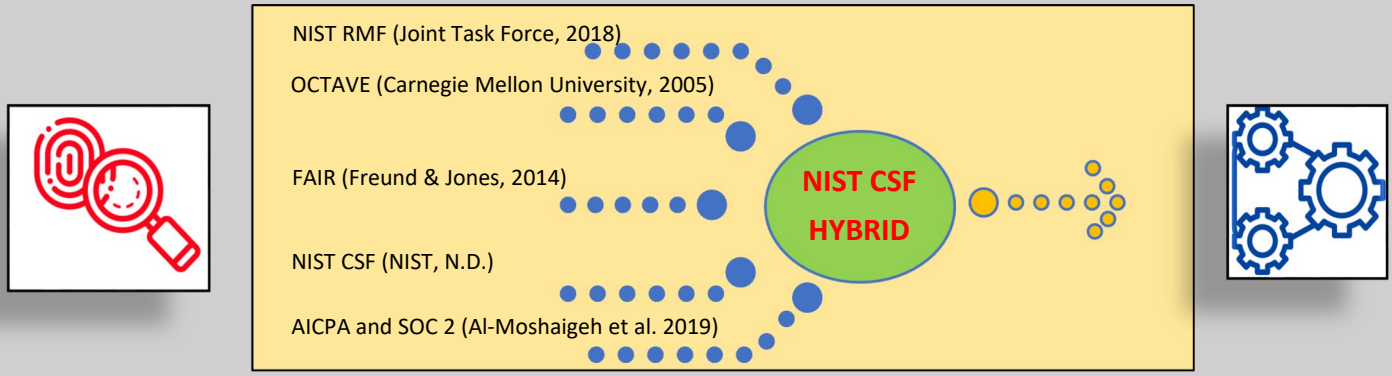
Risk assessment methodology: NIST Cyber Security Framework Hybrid Model



NIST Risk Management Framework:

+ Versatile and applied to most systems (Joint Task Force, 2018).
+ 6 step framework (Violino, 2021).
+ Comprehensive documentation and control catalogue.
- Mandated for US federal agencies requiring government assistance (Iorga & Karmel, 2020).
- Very prescriptive process.
- Less approachable documentation rarely used in private sector.

OCTAVE:

+ Flexible methodology.
+ Octave-S for smaller organisations and less complex (Tucker, 2018).
- Only qualitative.
- Reliant on individual knowledge of the company security practices and processes to classify risk to assets. (Santos, 2018).

Open FAIR:

+ Simplistic, quantifiable probabilities, scalability and business exposure analysis (Suloyeva et al., 2019).
+ Cost efficient (Linford, 2020).
+ Hybrid approach with Octave could be useful (Hanes et al., 2017).
- Insufficient reporting documentation.
- Limited risk management solutions (RSI Security, 2021).

NIST Cyber Security Framework:

+ Collaboration between US government and private sector (National Institute of Standards and Technology, 2018).
+ Uses common language and cost-effective on business needs (Benz & Chatterjee, 2020).
+ No additional regulatory requirements on businesses.
+ 5 step framework and catalogue of controls to support.
+ Opportunities for improvement within a context of a continuous and repeatable process.
+ Allows effective communication between internal and external stakeholders.
- Open interpretation to standards for protection, mitigation and response.
- Limited topic identification areas (Krumay et al., 2018).

AICPA and SOC 2:

+ Flexibility of controls with alignment to business operations.
+ Manages customer data on five core principles :security, availability, processing integrity, confidentiality and privacy. (OneTrust GRC, 2021).
- Audits at times do not operate as intended.
- Restrictions of how data may be share that can impact processes.

Learning Outcomes
Identify and analyse critically IT system risks and problems,
and identify appropriate methodologies, tools, and techniques to solve/mitigate them.

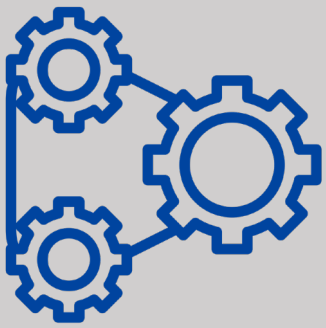
Select a risk assessment methodology

Justification of the framework

Supporting literature

NIST Cyber Security Framework Hybrid Model

The hybrid model incorporates NIST RMF to design or improve an existing program (Tracy, 2017)



+ Uses customised common language recommended for any organisation, size or degree of risk.
+ Cost-effective on business needs, flexible guidelines and voluntary usage.
+ No additional regulatory or audit requirements on businesses.
+ 7 step framework (Figure 1) integrating NIST RMF with three components [Core, Tiers and Profiles] (Tierney, 2021).
+ CSF can make RMF more robust.
+ Opportunities for improvement within a context of a continuous and repeatable process.
+ Allows effective communication between internal and external stakeholders.
+ Establish and maintain lifecycle risk management process.
+ Automation of processes to function the framework.
+ CSF functions link categories that manage security controls (Figure 2) such as COBIT 5, NIST SP 800-53 and ISO-27001 (Schall, 2017).
+ Prioritises most critical activities, identify mitigation strategies, evaluate tools and processes.
+ Measures the return of investment of cybersecurity investments and maturity controls.

- Limited topic areas as no identification of natural disasters, monetary aspects or organisation climate (Krumay et al., 2018).
- In risk identification, security roles and responsibilities has little coverage in the area of specific role definition.
- Vague wording leaves room for too much interpretation in protection and mitigation.
- Undefined standards therefore users not clearly respond to a detected threat with insufficient details on response actions to a breach (Dedeke & Masterson, 2019).

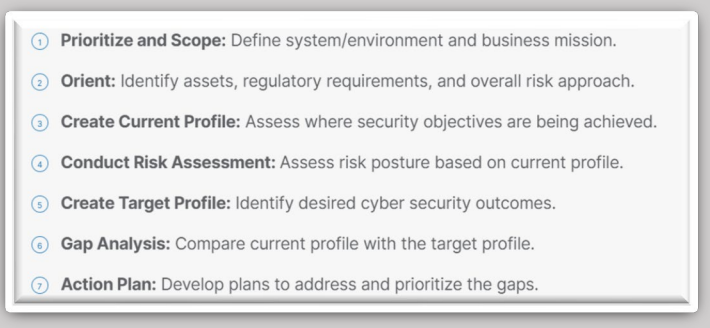


Figure 1: NIST Hybrid Model 7 Step Framework (Tracy, 2017)

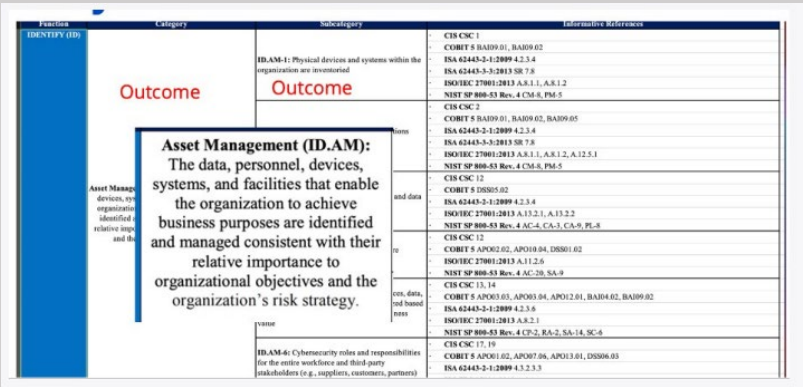
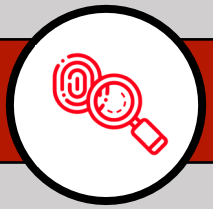
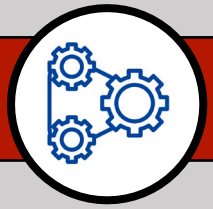


Figure 2: NIST CSF functions and security controls (Skeen, 2021)

Learning Outcomes
Identify and analyse critically IT system risks and problems, and identify appropriate methodologies, tools, and techniques to solve/mitigate them.



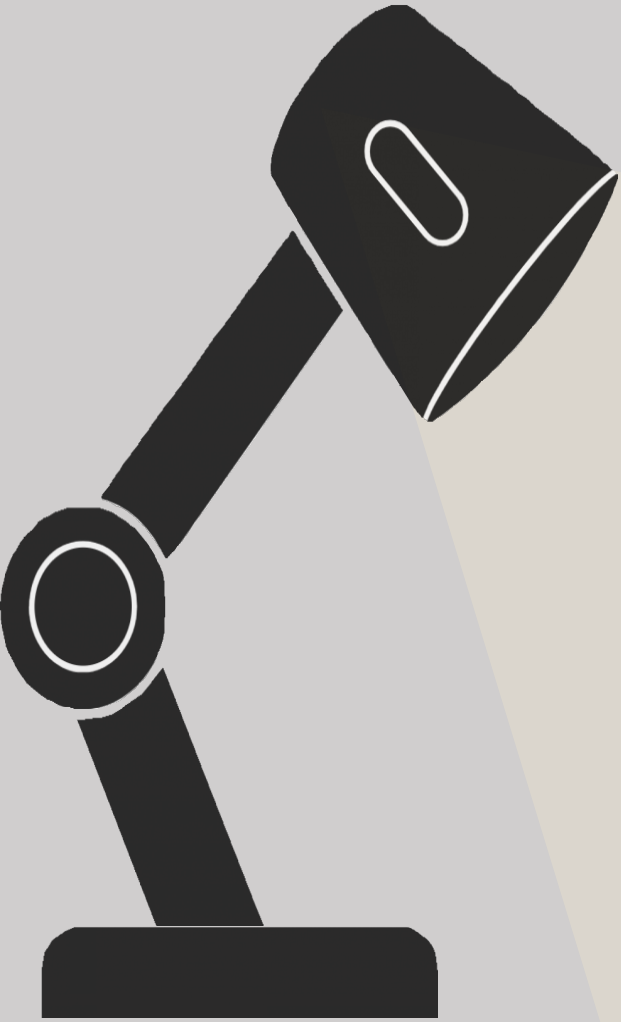
Select a risk assessment methodology

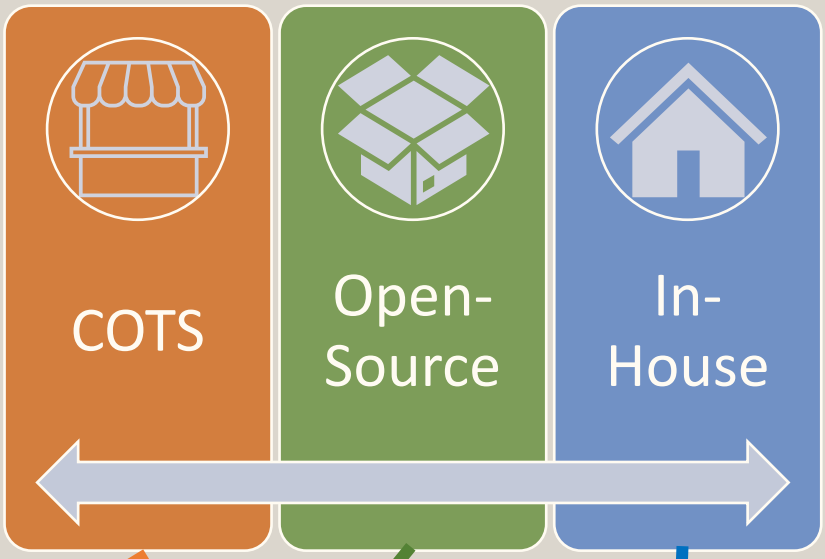


Justification of the framework

Supporting literature

SPOT LIGHT ON SHORTLIST OPTIONS





NIST CSF Hybrid

Open FAIR

Octave

Learning Outcomes
Identify and analyse critically IT system risks and problems,
and identify appropriate methodologies, tools, and techniques to solve/mitigate them.

Select a risk assessment methodology

Justification of the framework

Supporting literature

Risk No.	Risk	Potential Effect	Risk Assessment			Recommendation	Treatment
			Probability	Impact	Risk Level		
COTS (Commercial Off the Shelf) solution							
1	Inadequate support of COTS vendor	Inadequate service quality Security breaches and incidents Non-compliance with regulatory authority Financial loss and reputational damage	3	3	9	Transfer/ Reduce	1. Procure COTS products from well-known suppliers with support capabilities. 2. Contract should specify software escrow agreement
2	Process risk	Sustainability of application leading to service degradation	3	2	6	Mitigate	Adopt agile approach for solution delivery which will reduce time to delivery
3	SLAs not meeting agreed-on metrics	Not able to provide the agreed-on RTO and RPO	3	3	9	Mitigate	1. Establish metrics for monitoring SLAs. 2. Add indemnification clause for breach of SLA
4	Product obsolescence	Inadequate service quality Security breaches and incidents Financial loss and reputational damage Not able to meet organisations strategic objectives	3	3	9	Mitigate	Choose the subscription model. A monthly or yearly subscription model will address the risk of obsolescence
Open-Source solution supported by Internal IT department							
1	Software quality	Inadequate service quality Not able to meet strategic objectives	3	3	9	Mitigate	1.Train/upskill niche resrouces. 2. During the planning stage of the
2	Sustainability over longer time period	Inadequate service quality Security breaches and incidents Not able to meet organisations strategic objectives	3	3	9	Mitigate	Developers should check: 1.No of commits that shows level of activity 2. How many bugs are fixed in
3	Copyright infringement	Financial loss and reputational damage	3	3	9	Mitigate	Incorporate automated tools to track the usage of open source licenses
4	Software security risks	Security breaches and incidents Financial loss and reputational damage	3	4	12	Mitigate	1. Adopt a continuous vulnerability management approach using a mix of open source and commercial security tools 2. Conduct yearly vulnerability

In-house developed solution built by a student and supported by Internal IT department

1	Unrealistic estimated schedule	Not able to meet organisations strategic objectives	4	2	8	Mitigate	Transfer solution to internal IT dept for development.
2	Lack of adequate skill set	Not able to meet organisations strategic objectives Security breaches and incidents Inadequate service quality	4	3	12	Mitigate	Purchase COTS application and adopt agile methodology for quick deployment
3	Incomplete solution	Not able to meet organisations strategic objectives	2	3	6	Mitigate	Transfer solution to internal IT dept for development.
4	Lack of upper management involvement	Not able to meet organisations strategic objectives	2	3	6	Mitigate	Month/Quarterly progress meetings to review the progress and risks
5	Insufficient testing	Security breaches and incidents Inadequate service quality	3	4	12	Mitigate	1. Adopt a continuous vulnerability management approach using a mix of open source and commercial security tools

Table 1: Risk Register

The quantitative method uses numerical and statistical techniques to calculate the likelihood and impact of riskand is data-driven and produces statistically reliable results. Given the high degree of uncertainty and insufficient knowledge, a quantitative method will not yield a satisfactory result. Also, reliable historical data is not available for analysis to quantify risk. Qualitative analysis often reflects inputs of business units more accurately than quantitative analysis, and it also captures “soft” risks. Considering the above, we used the qualitative assessment method for risk assessment.

Impact Matrix					
	Negligle (1)	**Minor(2)**	**Major(3)**	**Extensive(4)**	**Catastrophic(5)**
Reputation	Contained to industry and insiders locally	Local media coverage and reputation impact	National media coverage and local criticism	Short term international media coverage and business impacting reputational damage	Long term (>1) international attention and lasting reputational damage
Financial	< $100K	< $500K	< $2M	< $5M	< $10M
Health & safety	Minor first aid	Medical treatment incident	Hospitalization/Lost Time Injury (LTI) of multiple persons	Fatal incident up to 5 people	Mass fatalities > 5

Table 2: Impact Matrix

Probability Matrix			
	Likelihood	**Frequency**	**Percentage Probability**
Very High (5)	Expected to occur in most circumstances	Can happen often in a year	75%+
High (4)	Likely to occur in many circumstances	Expected yearly	50-70%
Medium (3)	May occur but less likely than likely	Once every few years	21-49%
Low (2)	Can occur but unlikely	At least once in 5 years	6-20%
Very low (1)	May occur only in exceptional circumstances	Once in 10 years event	> 5%

Table 3: Probability Matrix

Risk Matrix					
	Negligle (1)	**Minor(2)**	**Major(3)**	**Extensive(4)**	**Catastrophic(5)**
Very High (5)	Medium	Medium	High	Very High	Very High
High (4)	Low	Medium	High	Very High	Very High
Medium (3)	Low	Medium	Medium	High	Very High
Low (2)	Low	Low	Medium	High	Very High
Very low (1)	Low	Low	Medium	Medium	High

Table 4: Risk Matrix

Based on the risk appetite, financial appetite and risk assessment conducted, we recommend procuring the COTS application

Disaster Recovery Solution

Assumption

- ACME has eCommerce website for selling goods similar with the researched companies **(**CHX Products, N.D.).
- The COTS solution able to support clusters, containers, and cloud solution like Azure.

RPO/ RTO requirements

	Regions	RTO target	RPO target	Annual Cost	Recovery Action
Cloud Container Active Active	**2**	< 20 mins	< 1 mins	~40k (Figure 4)	Health check
Cloud Container Active Passive	**1**	> 4 hrs	> 15 mins	~28k (Figure 5)	Move Region Data migration Build container
Cloud Virtual machine (VM) Active Passive	**1**	> 12 hrs	> 1 hr	~20k (Figure 6)	Move Region Data migration Build VM

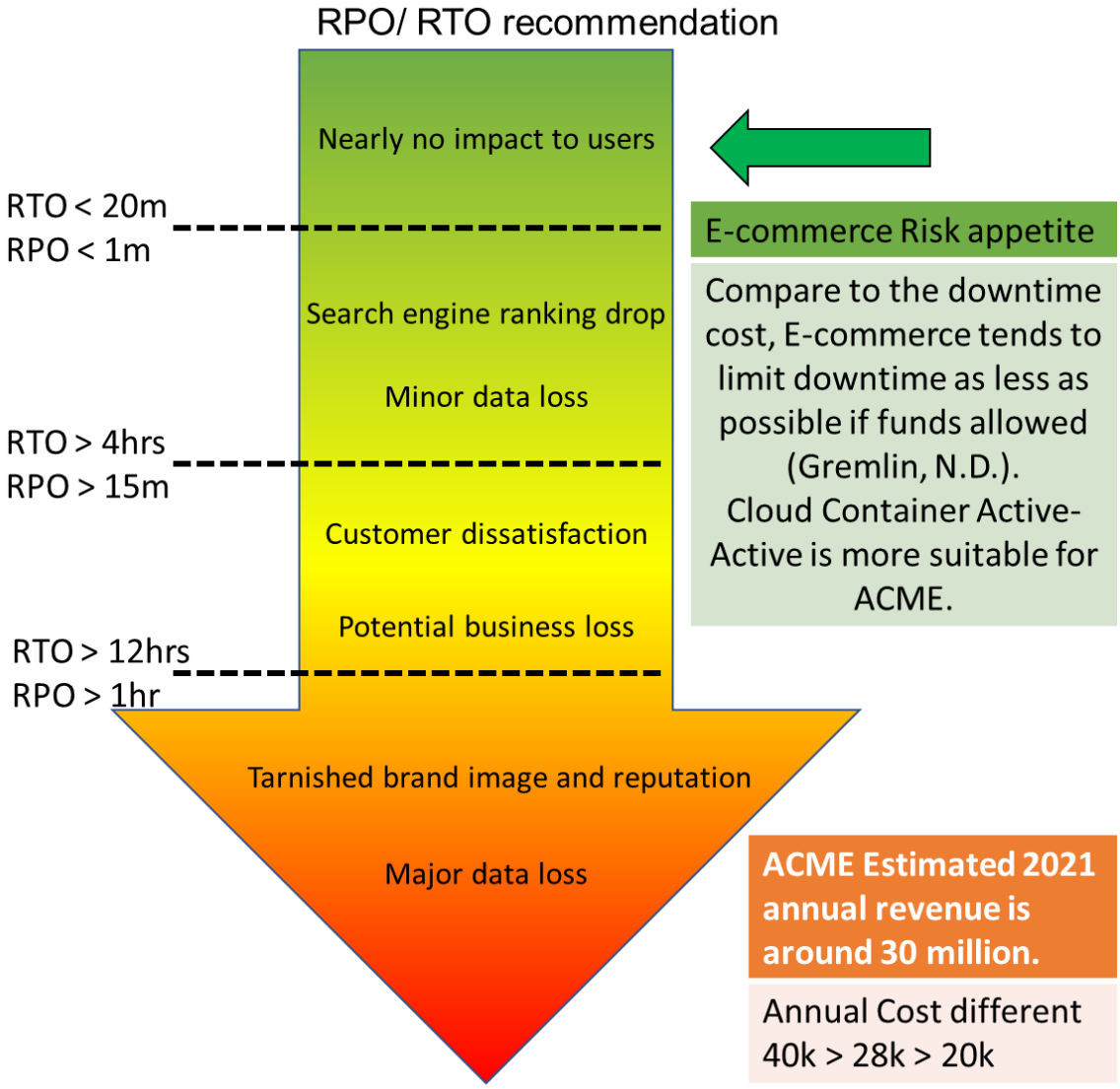


Figure 3: RPO/ RTO recommendation (Gremlin, N.D.)

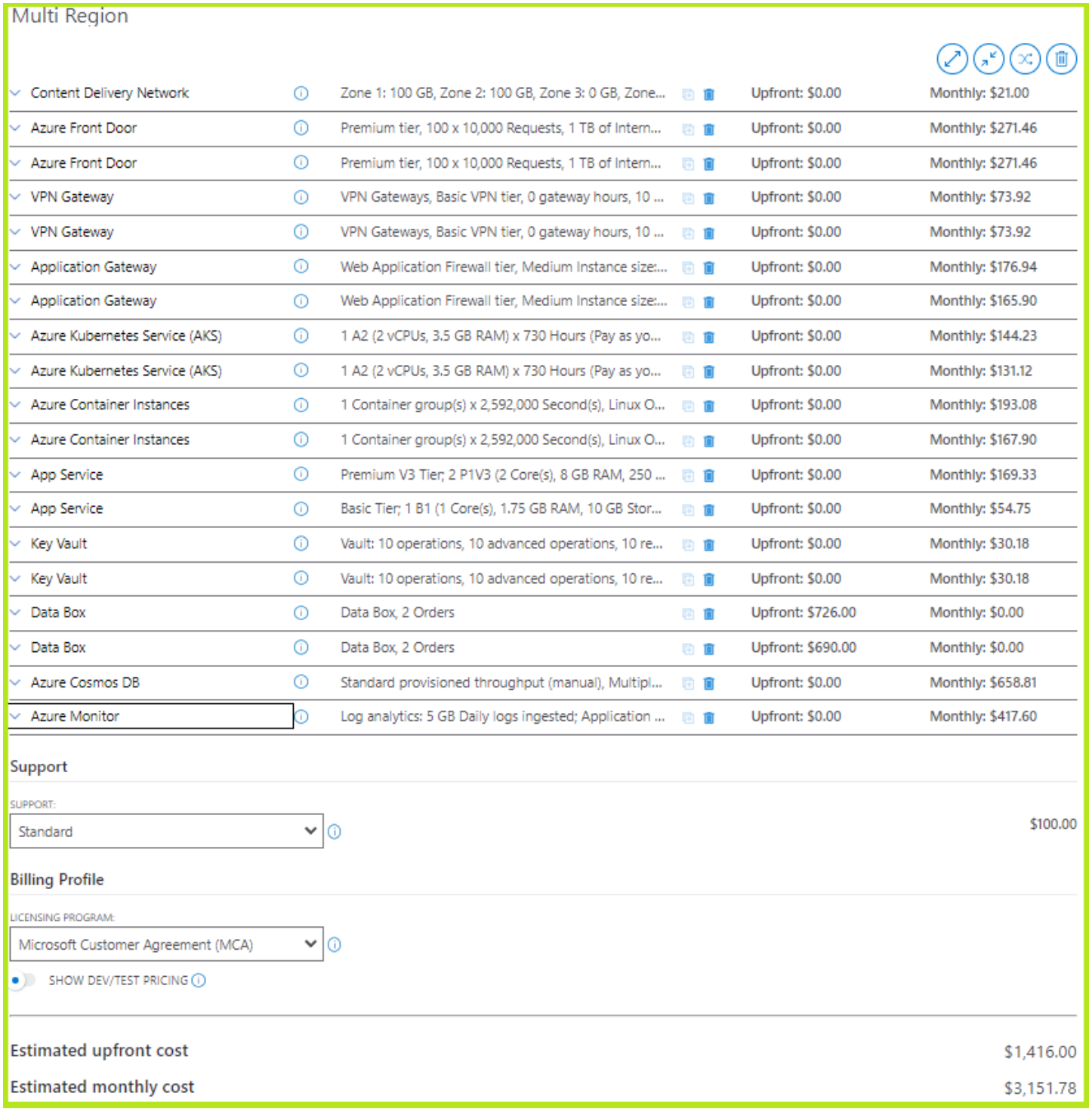


Figure 4: Multi Region, Annual cost: $1,416 + $3,151.78 x 12 = $39,237.36 (Azure, 2022)

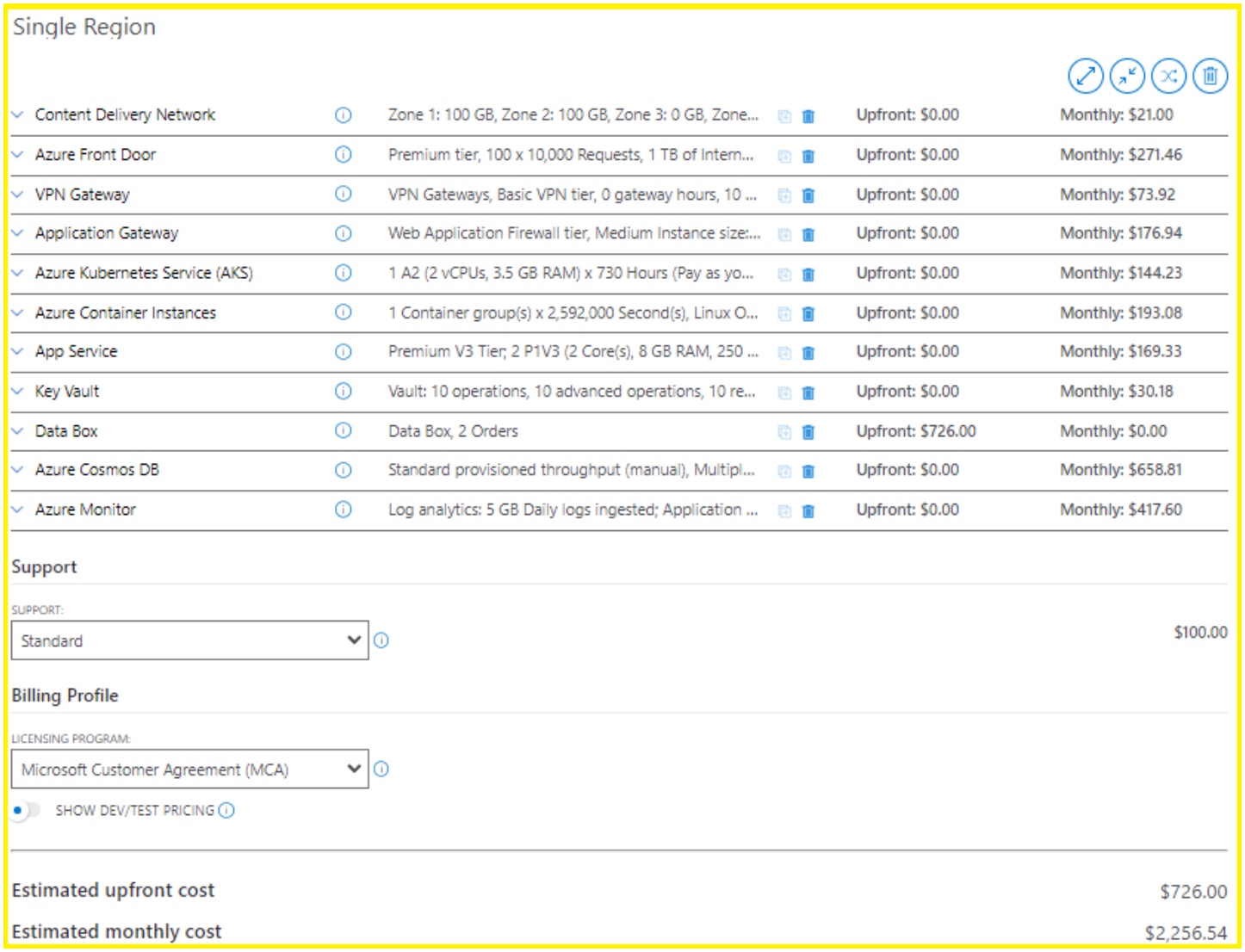


Figure 5: Single Region, Annual cost: $726 + $2,256.54 x 12 = $27,804.48 (Azure, 2022)

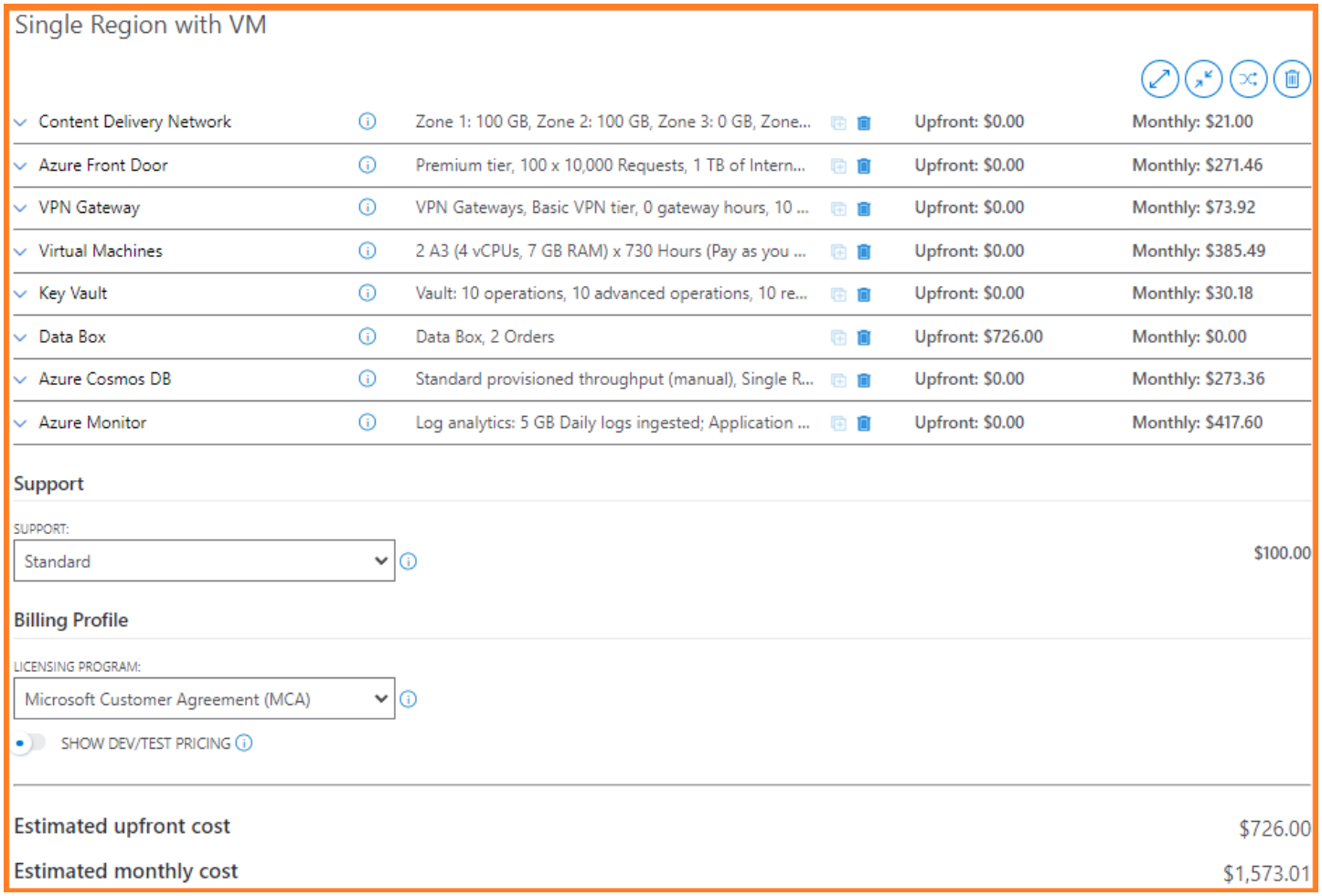


Figure 6: Single Region with VM, Annual cost: $726 + $1,573.01 x 12 = $19,602.12 (Azure, 2022)

High-level Diagram

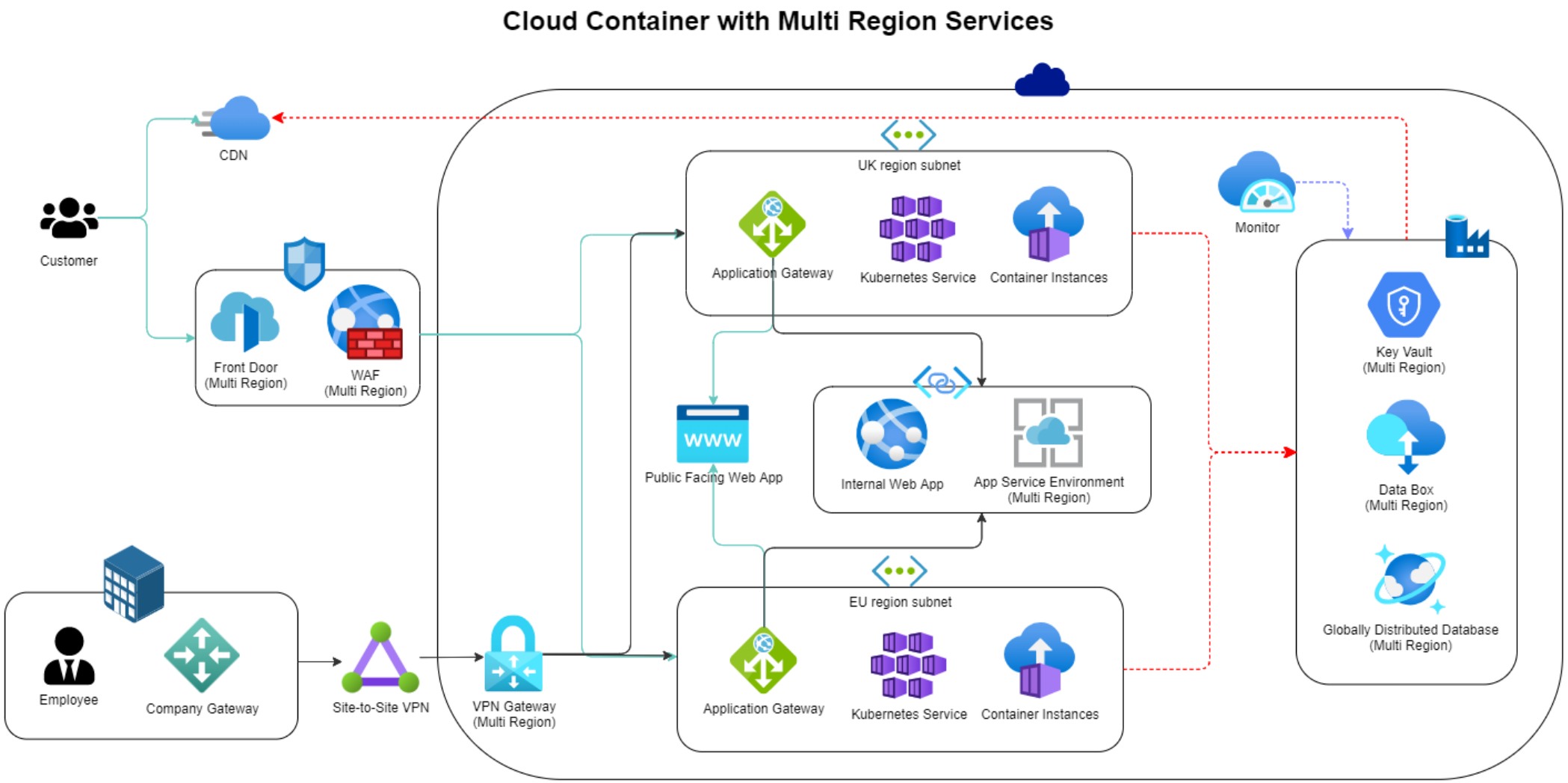


Figure 7: Cloud Container with Multi Region Services (Azure, 2022)

Challenges

Resilience

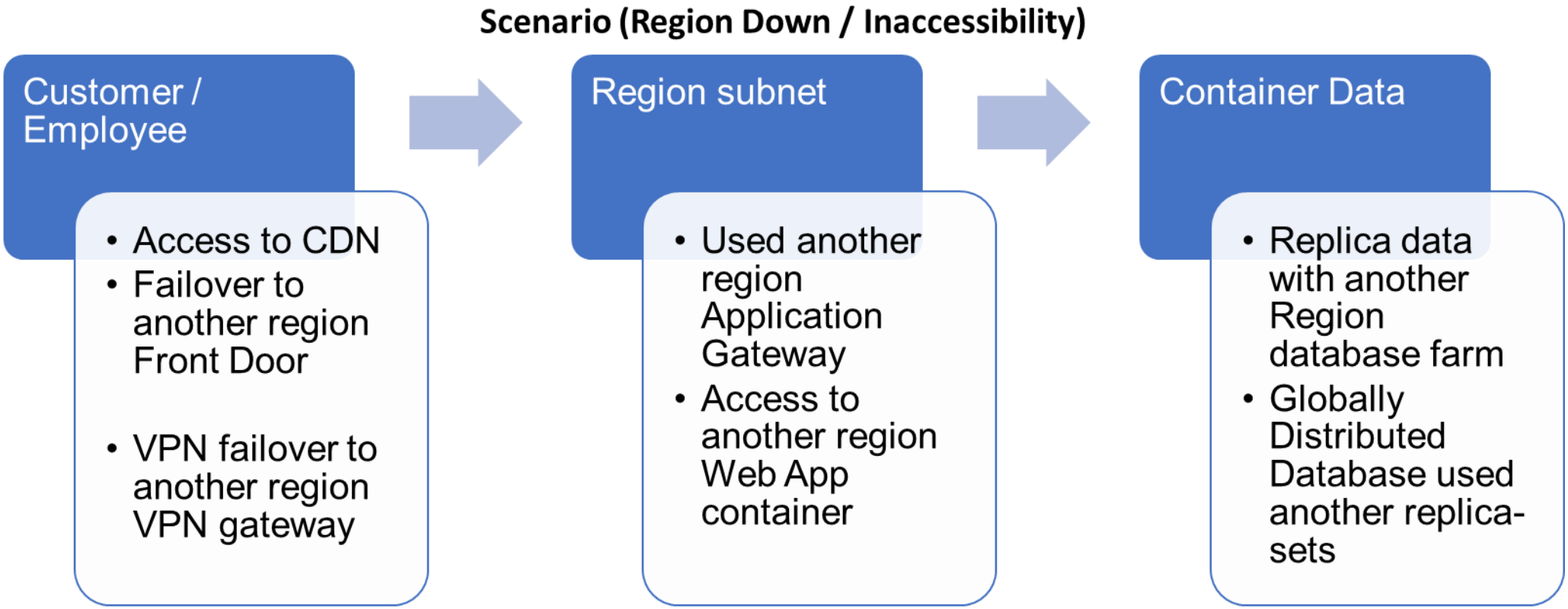


Figure 8: Scenario (Region Down / Inaccessibility), NIST SP 800-160 (NIST, 2021)

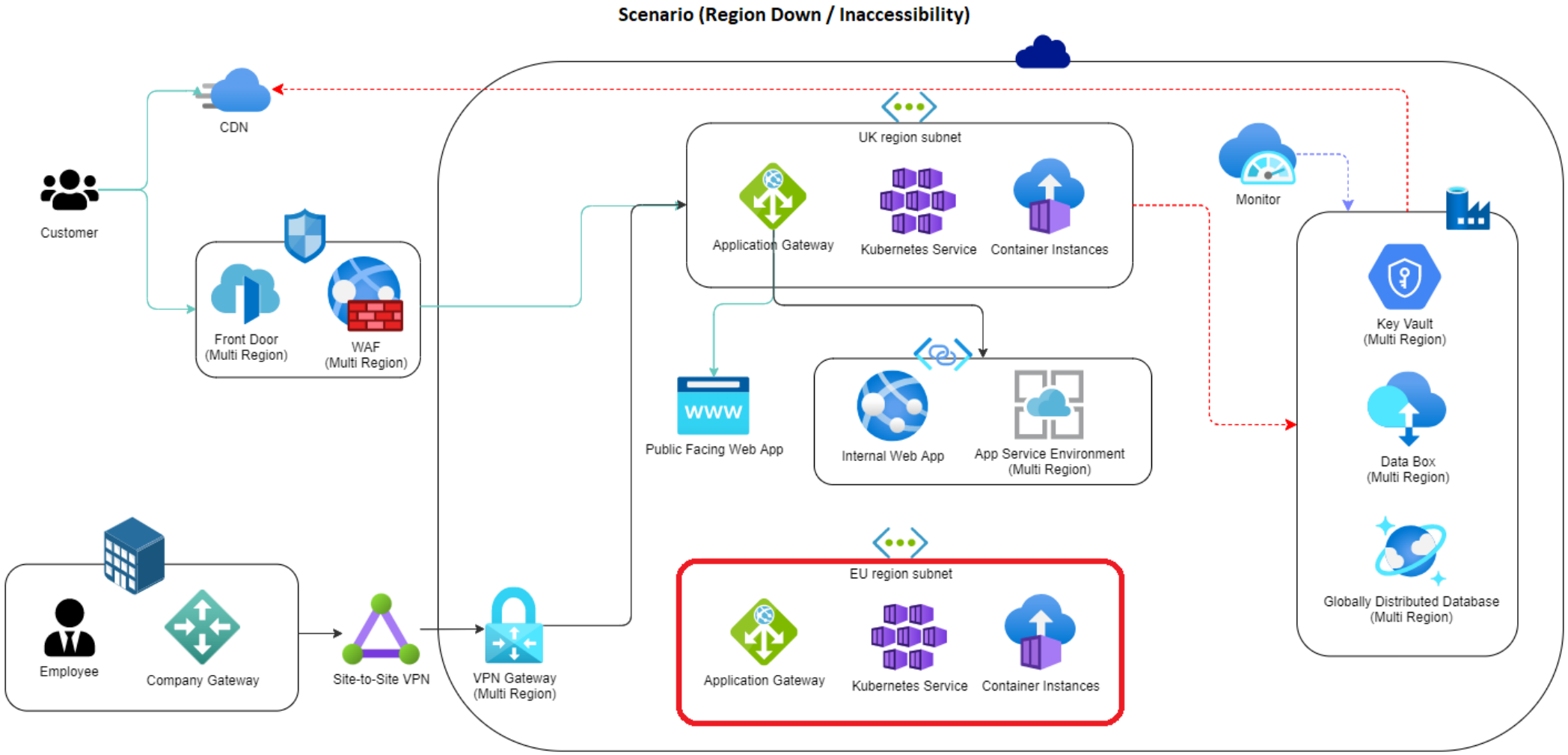


Figure 9: Scenario (Region Down / Inaccessibility) (Azure, 2022)

Network security

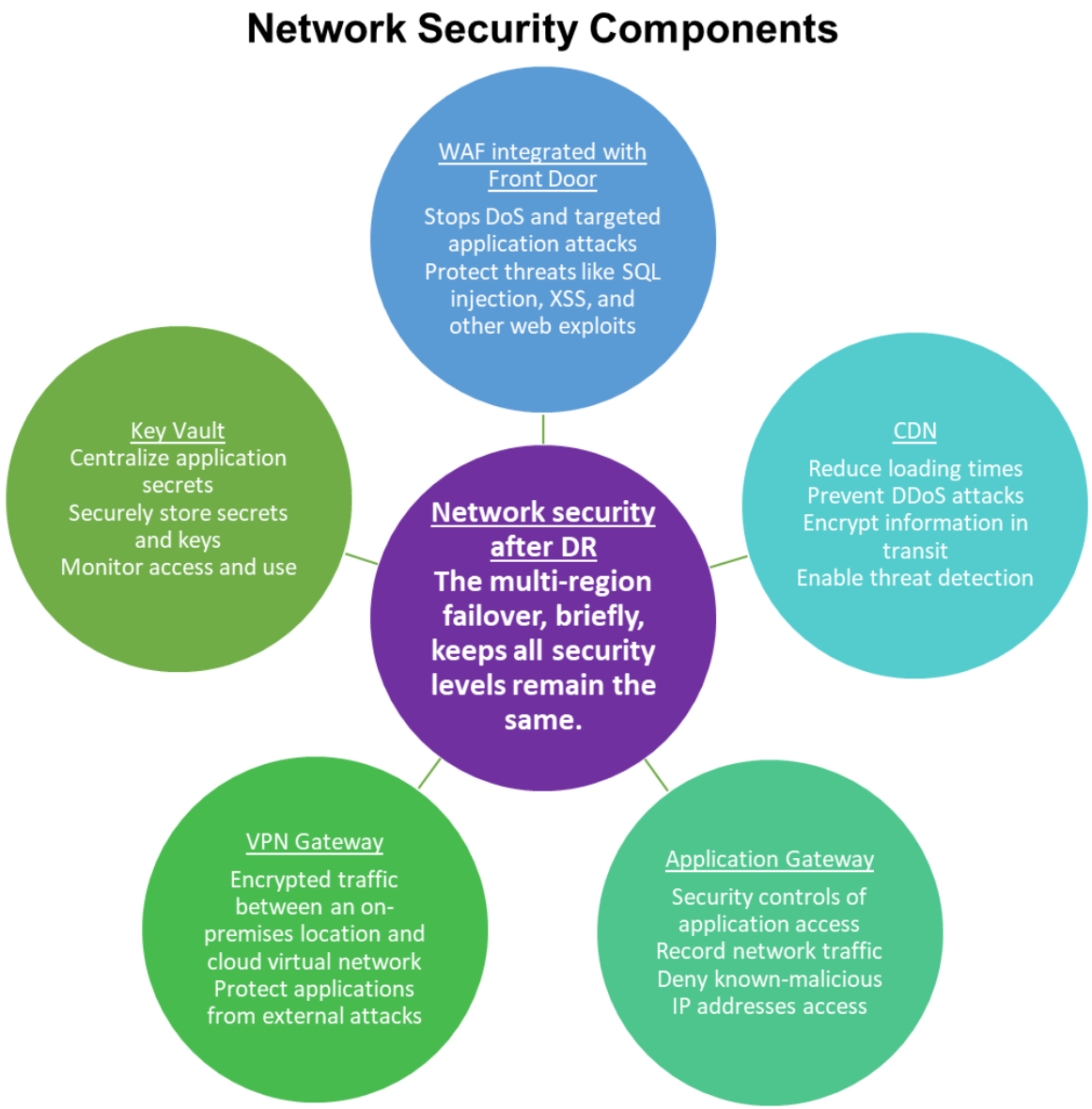


Figure 10: Network Security Components (Azure, 2022), ST18-001 (CISA, 2020)

Vendor provision/ lock-in

Secure Software Development Framework (SSDF)	
Prepare the Organization (PO)	Container instances and application gateway (Figure 11) Separate the loading and states of the application to different user groups
Protect Software (PS)	Vendor (Figure 11) Allowed to make changes in the development environment only Use version control features of the repository to track all changes Adopt CI/CD pipeline to automate the software delivery process
Produce Well-Secured Software (PW)	Quality Assurance (Figure 11) Verify software complies with security requirements and mitigates risks Test executable code to identify vulnerabilities Review the software design to verify compliance
Respond to Vulnerabilities (RV)	Rollback / Take offline (Figure 12) Identify the vulnerabilities version Limit assess and remediate the vulnerabilities in container Analyse the container and identify the root causes

Figure 11: SSDF (NIST, 2022)

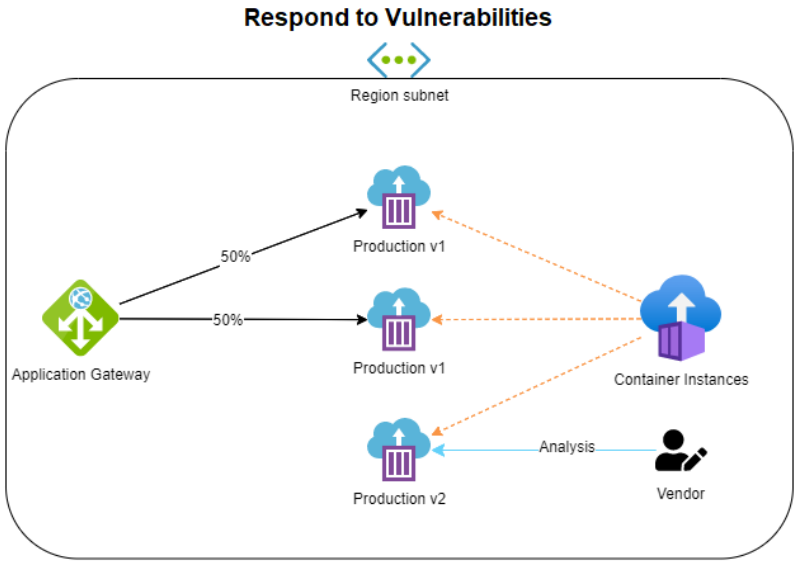


Figure 12: Respond to Vulnerabilities (Azure, 2022)

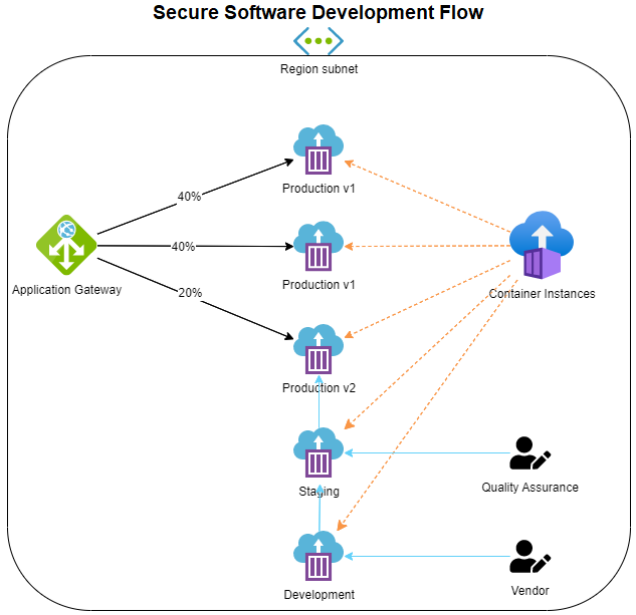


Figure 13: Secure to Vulnerabilities (Azure, 2022)

Appendix 1

Risk Assessment Assignment

University of Essex Online

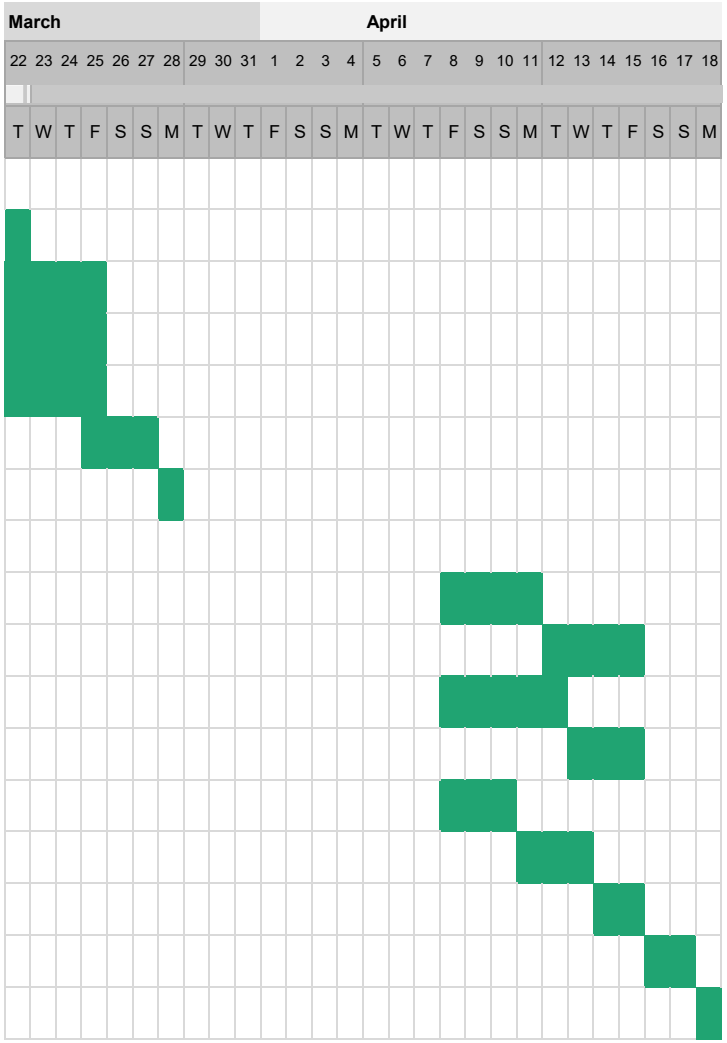
Jonathan Callaghan, Nitin Subramaniam, Ying Chan

Project Start Date: 21/03/2022

Scrolling Increment: 1

Legend: On track | Low risk | Med risk | High risk | Unassigned

Milestone description	Category	Assigned to	Progress	Start	Days
Status Report					
Meet to discuss status report	On Track	All	100%	22/03/2022	1
Research about company status	On Track	Ying	100%	22/03/2022	4
Research about business risks	On Track	Jonathan	100%	22/03/2022	4
Enumerate technical and business risks	On Track	Nitin	100%	22/03/2022	4
Prepare status report	On Track	All	100%	25/03/2022	3
Submit status report	On Track	Ying	100%	28/03/2022	1
Risk Assessment Report					
Select risk assessment methodology	On Track	Jonathan	100%	08/04/2022	4
Prepare assessment methodology report	On Track	Jonathan	100%	12/04/2022	4
Perform analysis on risks identified	On Track	Nitin	100%	08/04/2022	5
Provide risk rating and mitigation	On Track	Nitin	100%	13/04/2022	3
Create Disaster Recovery solution	On Track	Ying	100%	08/04/2022	3
Prepare risk assessment report	On Track	Ying	100%	11/04/2022	3
Prepare risk assessment report	On Track	Ying	100%	14/04/2022	2
Report consolidation	On Track	All	100%	16/04/2022	2
Submit report	On Track	Ying	100%	18/04/2022	1



References:

Al-Moshaigeh, A., Dickins, D. & Higgs, J. L. (2019). Cybersecurity Risks and Controls: Is the AICPA's SOC for Cybersecurity a Solution? *The CPA Journal,* 89, (6): 36-41.

Azure. (N.D.) Frequently asked questions for Azure Web Application Firewall on Azure Front Door Service. Web Application Firewall. Available from: https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/waf-faq [Accessed 15 April 2022]

Azure. (N.D.) Pricing calculator. Pricing. Available from: https://azure.microsoft.com/en-us/pricing/calculator/ [Accessed 15 April 2022]

Azure. (2021) About Azure Key Vault. Security. Available from: https://docs.microsoft.com/en-us/azure/key-vault/general/overview [Accessed 15 April 2022]

Azure. (2021) Azure security baseline for Application Gateway. Security baselines for Azure. Available from: https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/application-gateway-security-baseline [Accessed 15 April 2022]

Azure. (2021) Azure security baseline for VPN Gateway. Security baselines for Azure. Available from: https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/vpn-gateway-security-baseline [Accessed 15 April 2022]

Azure. (2022) Azure security baseline for Content Delivery Network. Security baselines for Azure. Available from: https://docs.microsoft.com/en-

us/security/benchmark/azure/baselines/content-delivery-network-security-baseline [Accessed 15 April 2022]

Azure. (2022) Cross-region replication in Azure: Business continuity and disaster recovery. Availability Zones. Available from: https://docs.microsoft.com/en-us/azure/availability-zones/cross-region-replication-azure [Accessed 15 April 2022]

Azure. (2022) Global data distribution with Azure Cosmos DB - under the hood. Cosmos DB. Available from: https://docs.microsoft.com/en-us/azure/cosmos-db/global-dist-under-the-hood [Accessed 15 April 2022]

Benz, M. & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons,* 63, (4): 531-540.

Carnegie Mellon University, S. S. E. I. (2005). OCTAVE v2.0. Available from: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html [Accessed 10 April 2022].

CHX Products. (N.D.) Spork. Food & Drinkware. Available from: https://www.chxproducts.co.uk/product/spork/ [Accessed 15 April 2022]

CISA. (2020) Security Tip (ST18-001). National Cyber Awareness System. Available from: https://www.cisa.gov/uscert/ncas/tips/ST18-001 [Accessed 15 April 2022]

Dedeke, A. & Masterson, K. (2019). Contrasting cybersecurity implementation frameworks (CIF) from three countries. *Information & Computer Security,* 27, (3): 373-392.

Freund, J. & Jones, J. (2014). *Measuring and managing information risk: a FAIR approach*. Butterworth-Heinemann.

Gremlin. (N.D.) Why Do Large Ecommerce Sites Go Down?. The Cost of Downtime for the Top US Ecommerce Sites. Available from: https://www.gremlin.com/ecommerce-cost-of-downtime/ [Accessed 15 April 2022]

Hanes, D., Salgueiro, G., Grossetete, P., Barton, R. & Henry, J. (2017). Formal Risk Analysis Structures: OCTAVE and FAIR. Available from: https://www.ciscopress.com/articles/article.asp?p=2803867&seqNum=4 [Accessed 13 April 2022].

Information Systems Audit And Control Association (2013). *CRISC review manual 2014*. Rolling Meadows, Illinois: Isaca.

Iorga, M. & Karmel, A. (2020). Cloud Computing Security Essentials and Architecture.

Joint Task Force. (2018). NIST Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. Available from: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final [Accessed 09 April 2022].

Krumay, B., Bernroider, E. W. N. & Walser, R. Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework. 2018 Cham. Springer International Publishing, 369-384.

Linford, J. (2020). The Open Group Security Forum. Available from: https://blog.opengroup.org/2020/12/02/updates-to-the-open-fair-body-of-knowledge-part-2/ [Accessed 10 April 2022].

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity. Available from:

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [Accessed 13 April 2022].

NIST. (N.D.). CYBERSECURITY FRAMEWORK. Available from: https://www.nist.gov/cyberframework [Accessed 10 April 2022].

NIST. (2020) Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. NIST Special Publication 800-218. Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04232020.pdf [Accessed 15 April 2022]

NIST. (2021) Developing Cyber Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800-160 Vol. 2. Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf [Accessed 15 April 2022]

Onetrust GRC. (2021). 5 IT Risk Management Frameworks to Consider. Available: https://www.onetrustgrc.com/blog/5-it-risk-management-frameworks-to-consider-for-your-program/ [Accessed 12 April 2022].

ResearchGate. (N.D.). Table 5 . Top ten risks factors in in-house & outsourced software projects. Available from: https://www.researchgate.net/figure/Top-ten-risks-factors-in-inhouse-outsourced-software-projects_tbl2_319643465 [Accessed 24 Mar. 2022].

RSI Security. (2021). PROS AND CONS OF FACTOR ANALYSIS OF INFORMATION RISK. Available from: https://blog.rsisecurity.com/pros-and-cons-of-factor-analysis-of-information-risk/ [Accessed 9 April 2022].

Santos, O. (2018). *Developing cybersecurity programs and policies*. Pearson IT Certification.

Schall, P. D. (2017). Top Ten—Differences Between RMF and CSF. Available from: https://www.itdojo.com/top-ten-differences-between-rmf-and-csf/ [Accessed 14 April 2022].

Skeen, J. (2021). *Kickstart Guide to Implementing the NIST Cybersecurity Framework*. Netwrix.

Snyk.io. (2021). 5 Risks of Open Source Software | Snyk. Available from: https://snyk.io/learn/risks-of-open-source-software/ [Accessed 22 Mar. 2022].

Software Engineering Authority. (2017). Understanding the Risks of Commercial off-the-shelf software (COTS). Available from: https://ao.ms/understanding-the-risks-of-commercial-off-the-shelf-software-cots/ [Accessed 22 Mar. 2022].

Suloyeva, S., Grishunin, S. & Burova, E. (2019). *Developing a Cybersecurity Risk Analysis System for High-Tech Equipment in Machine Industry*. *Proceedings of the 2019 International SPBPU Scientific Conference on Innovations in Digital Economy.* Saint Petersburg, Russian Federation: Association for Computing Machinery.

Tierney, M. (2021). What Is the NIST Cybersecurity Framework? Available from: https://blog.netwrix.com/2021/03/24/nist-cybersecurity-framework/ [Accessed 14 April 2022].

Tracy, R. (2017). Encouraging NIST CSF Adoption with Automation. Available from: https://www.telos.com/2017/05/encouraging-nist-csf-adoption-automation/ [Accessed 14 April 2022].

Tucker, B. (2018). OCTAVE FORTE and FAIR Connect Cyber Risk Practitioners with the Boardroom. Available from: https://insights.sei.cmu.edu/blog/octavea-forte-and-fair-connect-cyber-risk-practitioners-with-the-boardroom/ [Accessed 9 April 2022].

Violino, B. (2021). 5 IT risk assessment frameworks compared. Available from: https://www.csoonline.com/article/2125140/it-risk-assessment-frameworks-real-world-experience.html [Accessed 14 April 2022].

WhiteSource. (N.D.). Top 3 Open Source Risks and How to Beat Them. Available from: https://www.whitesourcesoftware.com/resources/blog/top-3-open-source-risks-and-how-to-beat-them/ [Accessed 23 Mar. 2022].