



Leading the risk profession



# Cybersecurity Risk Management Framework *for* *Small and Medium Enterprises (SMEs)*



A report on the CVEQ Framework for SMEs



“

While, it's true that there isn't a way to make yourself bulletproof from cyber attackers. There are many ways that you can minimize your risk of being a victim of a successful attack.

- Lakeidra Smith



## Introduction



Leading the risk profession

The Institute of Risk Management (IRM) is the world's leading enterprise-wide risk management education Institute. We are independent, well-respected advocates of the risk profession, owned by our members who are practicing risk professionals. IRM passionately believes in the importance of risk management and that investment in education and continuing professional development leads to more effective risk management.

We provide qualifications, short courses and events at a range of levels from introductory to expert. IRM supports its members and the wider risk community by providing the skills and tools needed

to turn theory into practice in order to deal with the demands of an evolving, sophisticated and challenging business environment.

We operate internationally with members and students in over 100 countries, drawn from all risk-related disciplines and a wide range of industries in the private and public sectors. A not-for profit organisation, IRM reinvests any surplus from its activities in the development of international qualifications, short courses and events. IRM East Africa Regional Group is made up of IRM members in East Africa.



An award-winning pan-African research-driven Cybersecurity and risk Consulting firm, Serianu enables organisations to anticipate, detect, respond and contain cyber threats. We specialize in providing cutting edge research-based consulting and managed services around new and emerging cyber risk areas. Serianu's bouquet of services include threat detection and alerting, cyber security awareness and training, technical and non-technical assessments, forensics and investigations and remediation support.



The Africa Cyber Immersion Center (ACIC) is a state-of-the-art cyber security research and training facility that works with cyber security, organisation risk management professionals and corporate leaders in Africa to hone their skills and ramp up their cyber-attack preparedness.

The only one of its kind in Sub Saharan Africa, ACIC mirrors similar facilities existing in Europe, the US and Asia, and is designed to meet a huge demand for a specialized institution that provides professionals with a modern, third-party environment to test individual and organisational cyber threat resilience, train cyber security professionals and

deliver locally designed courses based on relevant case studies.

Since its establishment in 2017, the ACIC has endeavoured to address Africa's current and long-term future needs through unique education, training, research, and practical applications.

Through the years, ACIC has successfully implemented several projects including developing the CVEQ, researching and publishing the Annual Africa Cyber Security Report, implementing Cyber Immersion Programs in different academic institutions and sharing cyber threat intelligence information across the region.





©2023 Institute of Risk Management (IRM) and Serianu Limited

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the express permission of the copyright owner. Permission will generally be granted for use of the material from this document on condition that the source is clearly credited as being Institute of Risk Management (IRM) and Serianu Limited.

The Institute of Risk Management (IRM) and Serianu Limited does not necessarily endorse the views expressed or products described by individual authors within this document.

Photos Credits: © Envanto Elements, Freepik.com, The Institute of Risk Management (IRM) and Serianu Ltd.

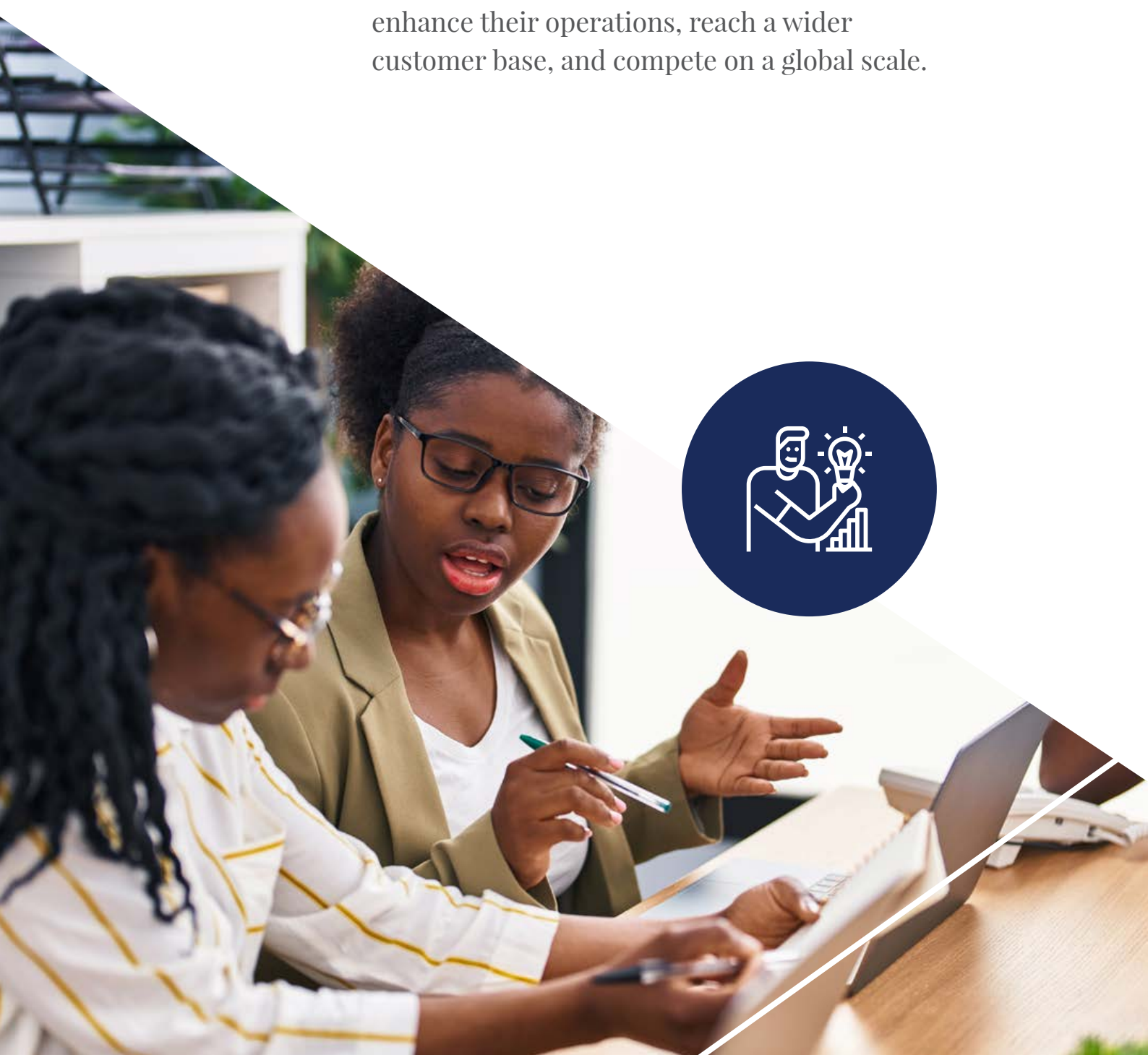
## **Contents**

<b>Introduction .....</b>	<b>3</b>
<b>A Word from IRM East Africa Regional Group.....</b>	<b>6</b>
<b>A Word from Serianu Limited .....</b>	<b>8</b>
<b>A Word From The Industry.....</b>	<b>9</b>
<b>The Project Team .....</b>	<b>12</b>
<b>The African SME Story .....</b>	<b>13</b>
<b>Executive Summary .....</b>	<b>15</b>
<b>SME Technology Challenges .....</b>	<b>17</b>
<b>CVEQ Framework Development Process .....</b>	<b>19</b>
Objectives .....	19
CVEQ is best used to; .....	19
Target Audience .....	20
Methodology .....	20
Outcome .....	21
Industry Engagement.....	24
Testing and Validation.....	24
<b>Framework Components .....</b>	<b>26</b>
About the CVEQ Framework .....	26
Cybersecurity Framework Elements .....	27
Framework Elements.....	28
Framework Profile and Indicators.....	28
Framework Maturity Indicators .....	29
Framework Exposure Indicators.....	31
<b>Annex and Appendix .....</b>	<b>32</b>
Framework Summary .....	32
Framework References.....	35



## **A Word from IRM East Africa Regional Group**

In today's rapidly evolving digital landscape, small and medium enterprises (SMEs) play a vital role in driving economic growth and innovation. These enterprises are at the forefront of technological advancements, leveraging digital tools and platforms to enhance their operations, reach a wider customer base, and compete on a global scale.



However, with these opportunities come significant cyber risks that can have a detrimental impact on SMEs if not properly addressed.

Cybersecurity threats have become increasingly sophisticated, targeting organizations of all sizes and industries. Security, in the form of controls, is expensive and may be out of reach for the majority of the SMEs. The consequences of a cyber incident can be devastating, ranging from financial losses, reputational damage and emotional drain to legal and regulatory implications.

Recognizing the cyber exposures that SMEs have and the limited resources at their disposal to deal with the cyber exposures, this SME Cyber Risk Framework has been developed to provide a reasonable approach to managing cyber risks effectively. The framework aims to empower SMEs with the knowledge, tools, and strategies needed to protect their digital assets, maintain business continuity, and safeguard their customers' trust.

The framework has been designed to be simple, practical, accessible, and adaptable to the unique needs and capabilities of all SMEs. It outlines a step-by-step process for identifying, assessing, mitigating, and monitoring cyber risks, enabling SMEs to establish reasonable controls that align with their business objectives. By implementing the recommended control practices outlined in this framework, SMEs can enhance their resilience against cyber threats and minimize the potential impact of a cyber incident.

As is the case with many other risk types, cyber risk management requires a collaborative approach to manage it effectively. All stakeholders are required to be engaged including the Board or Board Committees, management, employees, customers,

suppliers, and industry associations to foster a culture of cyber security awareness and cooperation. Cybercriminals are becoming smarter by the day, and it is critical that all players in the SME industry keep themselves abreast of the developments within this space and continuously upskill to be prepared to deal with the cyber threats.

I would like to express my appreciation to the dedicated team of the Institute of Risk Management members, Serianu Consulting team and the industry experts who sacrificed their time and contributed their knowledge and insights to develop this SME Cyber Risk Framework. Their expertise and commitment to cybersecurity have been invaluable in creating a resource that addresses the specific challenges faced by SMEs.

I encourage all SMEs to embrace this framework as a guiding resource to proactively manage cyber risk appreciating that business can no longer be conducted as "Business as usual". This will help the SMEs to not only protect their own interests but also contribute to the overall resilience of the global business community.

To achieve cybersecurity, it requires an ongoing commitment to keep up with the ever-changing cyber landscape. All players in the industry should participate in the fight to build a secure digital future for all. Together we can!

Sincerely,

*Catherine N*

**Catherine Nyaga-Mbithi**

Co-Chair, Institute of Risk Management, East Africa  
Regional Group







## A Word from Serianu Limited

This is the first report that we have out together on the CVEQ Framework for SMEs and the fact that we have now brought it to this stage marks a major milestone in a journey that has taken nearly four years.

When we first conceived the idea of developing a quantification framework that is built for our unique circumstances, it seemed like an impossible ambition, yet here we are.

The document we have prepared is an outline of the process that we have taken to put the framework together, introduced and tested it in a formal SME business environment and subjected it to thorough validation in a consultative workshop setting.

As we have explained, there already exists cyber security risk quantification frameworks in other markets such as the North America and Asia. Yet, instead of going off-the shelf solutions, we went the seemingly difficult route and decided to build one that reflects our context from the ground the up.

Furthermore, it was crucial that while we opted to go for an insight-based model, we also believed that a one which has been cocreated together with the end users was what we needed for Africa.

On behalf of the entire team that has contributed to this result, I want to express our utmost gratitude. We are also immensely gratified

by the support and partnership of the Institute of Risk Management in East Africa for believing in our vision and working with us to share this innovative solution with you.

After the conclusion of the entire development process, I can confidently state that we have the most suitable solution for SMEs to manage their cyber risks.

Finally, directors, shareholders and cyber security risk practitioners - can now confidently attach a financial value to the solution that they have provided, preventing them from misallocating scarce resources to unreliable ICT solutions.

We are now in a new era, one that ushers a period of data-driven decision making on a whole new level.

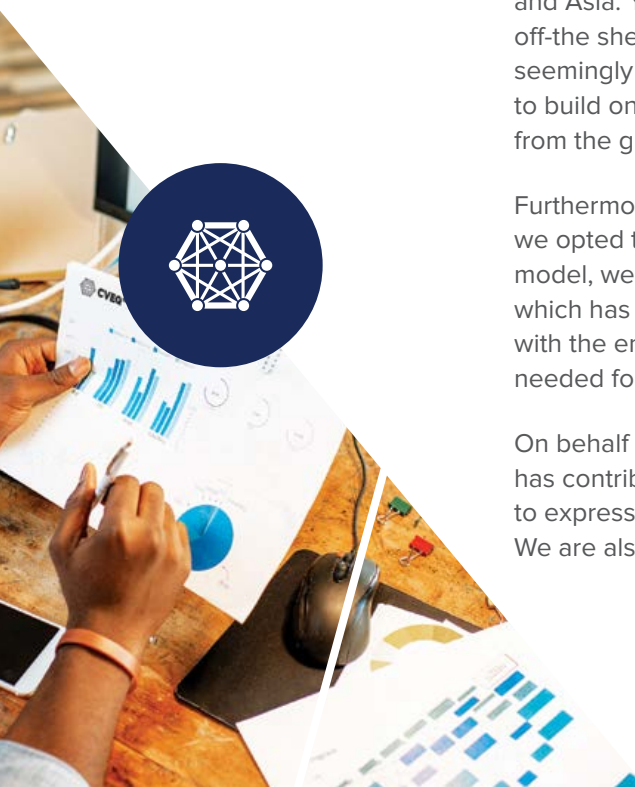
Welcome to the SME CVEQ report. Dig in and embrace the new cyber security risk quantification normal.

*Nabihah Rishad*

**Nabihah Rishad**

Editor-in-chief

Product and Research Lead,  
Serianu Ltd







## A Word From The Industry

In an era dominated by the relentless march to digital transformation, where the digital landscape shapes the very fabric of our interconnected world, the need for a robust and comprehensive approach to managing cyber risks has never been more critical.

As SMEs navigate the complex terrain of cyberspace, they encounter an ever-evolving array of threats that challenge the very foundations of their operations, integrity, and reputation.

The “Cybersecurity Risk Management Framework for Small and Medium Enterprises (SMEs) presented herein is a timely and indispensable guide for cyber practitioners, leaders and decision-makers who recognize the imperative of securing their digital assets in an environment fraught with cyber perils. Developed through a synthesis of industry best practices, cutting-edge research, and real-world experiences, this framework serves as a beacon in the turbulent seas of the digital realm, offering a structured and adaptive approach to identifying, assessing, and mitigating cyber risks.

Our interconnected world thrives on the rapid exchange of information, yet this interconnectedness exposes SMEs to an unprecedented level of cyber threats. From sophisticated cybercriminals seeking financial gain to nation-state actors pursuing geopolitical objectives, the adversaries are diverse, formidable, and persistent. Against this backdrop, “Cybersecurity Risk Management Framework for Small and Medium Enterprises (SMEs)” empowers SMEs to fortify their defenses, cultivate cyber resilience, and proactively respond to the dynamic nature of cyber threats.

This framework is not merely a static set of guidelines; rather, it is a living document

that evolves alongside the cyber threat landscape. It provides a flexible structure that accommodates emerging risks, technological advancements, and regulatory changes. By embracing a risk-based approach, SME’s can tailor their cybersecurity efforts to their unique context, ensuring a pragmatic and effective defense against cyber adversaries.

The authors have drawn upon their deep expertise and experiences in the field of cybersecurity and Risk Management to distill a wealth of knowledge into this comprehensive guide. As technology continues to advance and cyber threats grow in sophistication, “Cybersecurity Risk Management Framework for Small and Medium Enterprises (SMEs)” is a timely and invaluable resource that equips SMEs with the tools and insights needed to navigate the complex and perilous waters of cyberspace.

In an age where digital resilience is synonymous with organizational survival, this framework stands as a testament to the collective commitment to securing SME’s digital future. May it serve as a guiding light for SME’s worldwide, empowering them to navigate the dynamic and challenging landscape of cyber risks with confidence, resilience, and foresight.

*Bonface Asiligwa*

**Bonface Asiligwa** - CISA, CISM, CISSP, CRISC, CGEIT, CCSP





**Cybersecurity is a social responsibility.  
We all have a role to play.**





## A Word From The Industry

### Empowering Growth in the Small and Medium Enterprises (SMEs) Space through Cyber Risk Management.

In the dynamic landscape where Small and Medium Enterprises (SMEs) stand as the architects of economic growth and innovation, the embrace of digital tools is both a necessity and a beacon of progress. Yet, within this realm of possibilities lurk significant cyber risks, threatening to cast a shadow on the strides made by SMEs.

The SME space is characterized by limited cybersecurity regulations, as rules struggle to keep pace with the swiftly evolving cybersecurity landscape and the challenge of a significant skills gap, underscored by the impact of the global cybersecurity skills shortage. Implementing robust cybersecurity measures is therefore often considered difficult or simply surplus to requirements.

In the narrative of SMEs, where the adoption of digital tools propels operations, expands customer bases, and fuels global competitiveness, the digital transformation is a double-edged sword. While it promises innovation with ongoing developments in the technology space, like artificial intelligence, blockchain, and other emerging technologies, it simultaneously exposes SMEs to cyber risks. This vulnerability is further exacerbated by existing regulatory gaps and the absence of comprehensive data protection measures.

Acknowledging the challenges faced by these enterprises, the SME Cyber Risk Framework provides a simple yet comprehensive approach crafted to empower SMEs with the knowledge, tools, and strategies to protect their

digital assets while maintaining seamless business operations for the benefit of their customers. The Framework is a culmination of meticulous development that goes beyond mere guidelines. It is a comprehensive strategy designed to empower SMEs to traverse the complexities of the digital landscape with confidence.

This framework is not just user-friendly; it's an invitation. It beckons even those SMEs with limited resources and technical expertise, providing practical guidelines that seamlessly integrate cybersecurity measures into day-to-day operations. Recognizing the diverse capabilities and needs of SMEs, the framework stands as a testament to accessibility and inclusivity in its adoption. It adapts, recognizing that a one-size-fits-all approach falls short in the unique tapestry of SMEs.

As the SME Cyber Risk Framework is unveiled, it marks the beginning of a journey to foster a proactive cybersecurity culture within the SME sector. It is more than a launch; it's a commitment to fortify the foundation for sustained growth and innovation. For those curious to explore the SME Cyber Risk Framework and access the resources that accompany it, it's an open door to a secure and thriving future.

A handwritten signature in black ink that reads "George Kisaka".

**George Kisaka**

Vice President – ISACA Kenya



## The Project Team

IRM and Serianu would like to thank the following who have contributed towards the drafting and compilation of this report:

### **Serianu Limited**

William Makatiani  
Nabihah Rishad  
Carol Muchai  
Joy Wangeci  
Joy Naeku  
Hope Naserian  
Jackie Madowo  
Brenda Kamangara  
Monica Wangari

### **Industry Contributors**

Kanani Njaramba  
Stephen Robia  
Mark Karige  
Norman Mjomba  
Leroy Musungu  
Bonface Asiligwa  
Saidi Kisulu  
Samuel Kamau



### **IRM EA Focus Group Members**

Catherine Nyaga – Mbithi  
Sospeter Thiga  
Sarah N Kioi  
Grace Ndegwa  
Gakii Dominica  
Johnsey Kivoto  
George Kisaka  
Robert Mwangi  
Agnes Abwao  
Musoke Kibombo Isa  
Ivan Kulubya



## The African SME Story

Cybercrime is growing across Africa and it is a major concern among small and medium enterprises (SMEs) who today form the highest population of players in the economy. This is because as they develop, SMEs are expanding their use of technology, including cloud, mobile devices, smart technologies and work force mobility techniques.



Embracing technology has however unlocked their doors to vulnerabilities and cybercrime. Attackers have been launching increasingly sophisticated attacks on various angles, from business-critical infrastructure to simple devices such as mobile phones. Malware, insider threats, data breaches and system misconfigurations are just a few ways that the criminals have executed coordinated attacks against these organisations.

Evidence shows that with requirements of the 21st century businesses rising and inadequate budgets perennially allocated to IT functions, it's become difficult, especially for SMEs to embrace cyber security solutions. In their view, these are complicated and thus expensive. Cybercrime prevention is often therefore neglected, leading to a situation where SMEs are now some of the more popular targets by cybercriminals. Caught between a rock and hard place, these firms find themselves lacking a comprehensive framework to help them determine their risk exposure and provide visibility to their security landscape without necessarily adding to their strained budgets.

We know however, that directors of the firms want a simple answer to the question "How exposed are we? What is the effect of what we have done to reduce our exposures?" Our experience though, reveals that risk practitioners find these questions difficult to answer.

As the practitioners and business owners grapple with these challenges, every passing year, the African cyber security landscape rapidly evolves. On one hand, industry regulators have gone ahead to draft regulations and policies on cyber security. On the other hand, directors are getting more involved to fulfil their fiduciary roles, for they are expected to be actively involved in cyber security matters.

While there is progress on these fronts and investment in certifications and technologies, most of which do not come cheap, African organizations are still getting compromised. The situation is further complicated by SMEs unwillingness to share information regarding cyber security breaches for fear of loss of confidence by customers and decrease in their brand value.

### Why CVEQ?

From interactions with various project team members and in the process of validating CVEQ, we observed that most organizations believe that once they have invested in a one-time, limited scope assessments on their environments, that is sufficient. Unfortunately, these assessments, we established, are largely done as a check-box compliance exercise, and usually at least until another major breach occurs.

We came across reports that were qualitative on measuring risks, with terms like, high, medium and low used to assign degrees of exposure to cyber risk. Such reports still fall short in quantifying how exposed an organisation is, making it even more difficult to justify deployment of financial and human resources to mitigate against cyber risks.

Many risk professionals are not necessarily technical IT specialists. They prefer to leave the subject of cyber risk for the “experts”. But in their normal course of work, they are required to inform directors and other stakeholders about required financial protection against cyber risks. We found that several executives struggled to answer the question- “How much cyber insurance protection should I purchase?” Notably, the answer lies in the ability of an organization to quantify its cyber risk exposures.

Another key point of departure is that business versus IT reporting captures different sets of information. While the business is, among others, concerned with revenue, profits, assets, liabilities and the competitor environment, technology teams are more concerned with vulnerabilities, breaches, and tools to reduce threats. The challenge therein lies in how the two interests converge for the overall benefit of the company. A silo documentation approach often leads to instances where technology teams deploy tools that are either not fit-for-purpose or not fully exploited.

The business on the other hand, may struggle to understand the benefits accrued from these cyber risk initiatives, ending up with an expectations gap. From the lens of the Board, directors may then lack broad visibility on the impact of cyber security initiatives, resulting in a lack of understanding of the effects of new risk mitigations that have been deployed by the technology and information security teams. Aside from that, if a need arises for directors to rank their institutions, they lack suitable industry benchmarks to work with that are suitably designed for our market.



## Executive Summary

Small and medium sized business are the bedrock of African economies across the continent. There are however triple developments that have necessitated this report. These are the growth of the SMEs in numbers and size, the rising adoption of technology in respective businesses and ultimately, the new voracious attacks on their systems by cyber criminals.

This report outlines the soft under belly of SMEs that the cyber attackers have found and are exploiting with such abandon that entire economies are at risk of collapsing under a weight of financial losses and a high degree of public distrust.

Gratefully, the shareholders, directors and business managers have realized that they are in a hole and the only way out is to stop digging by throwing good resources in a misunderstood pit. They are essentially cybersecurity 'poor', lack the right tools to assess their degree of neediness and the extent of diagnosis to determine the amount of treatment required for their problems. This 'poverty line' is drawn on the skills, technical resources, funding and an entire arsenal necessary to remain fairly safe from cyber security loss.

Below is an outline of the characteristics of an organization that suffers from cyber security poverty.

- **Lack the minimum requirement for fending off an opportunistic adversary.**
- **Are essentially waiting to get taken down by an attack.**
- **There's also the idea of technical debt as a result of postponing important system updates.**
- **Lack in-house expertise to maintain a decent level of security controls and monitoring.**
- **Dependent on third parties hence have less direct control over the security of the systems they use.**
- **They also end up relinquishing risk decisions to third parties they ideally should be making themselves.**
- **Lack resources to implement separate systems for different tasks, or different personnel to achieve segregation of duties.**
- **They'll use the cheapest software they can find regardless of its quality or security. They'll have all sorts of back doors to make administration easier for whoever they can convince to do it.**

The reality is that cyber threats will not ease and that cyber attacks will not cease. There are newer ways and incentives being created and the cybersecurity risk environment continues to evolve.

### What does the future hold for this problem?

As cyber-attacks continue to evolve, it is paramount that organizations rise above the cybersecurity poverty line. In a world where buying a tool is considered a silver bullet to solving a cybersecurity issues, its critical that we ask ourselves key questions.

- What are my organizations top risks?
- What is the worst that can happen to my business?
- What do I need to do to ensure that I have secured my systems against these threats?

This approach creates room for dialogue between business and IT. Years of experience in the cyber security field has shown that organizations with little budgets can still maintain reasonable security levels granted they understand the few critical areas that need to be protected the most.

This document presents the detailed approach in a solution known as the CVEQ for SMEs, following defined principles and its core elements in great detail. A first of its kind in Africa and uniquely built for local context, this report captures the journey taken to the Framework it to life, and explains the importance of partnership and cocreation in achieving such as novel venture.





## SME Technology Challenges

### 1. Limited Awareness of Cybersecurity

Due to the intricacies of cybersecurity involving technical solutions and measures, there is a common misconception that it only pertains to individuals in IT-related roles. However, this is not accurate. Cybersecurity should be ingrained in the organizational culture, with every individual possessing at least a basic understanding of cybersecurity and recognizing how their actions can impact the overall cybersecurity stance of the organization. The crucial shift required is from initial awareness to the establishment of an internal cybersecurity culture.

### 2. Limited Budget

Many SMEs view financial resources allocated to cybersecurity as a cost rather than as an investment in their business. This is in spite of how many SMEs admitted that a major cybersecurity incident resulting in their ICT systems being unavailable would have a major negative impact on their business. New technology requires monetary investment. With SMEs heavily relying on funding and credit to propel their business and projects forward, limited access to credit can pose a great challenge in the running of a company, resulting in budget cuts and compromises.

### 3. Lack of IT Expertise

As a small and medium-sized enterprise (SME) experiences growth and transformations in its business, the technology it utilizes will evolve, and the cybersecurity threat landscape will continually shift. This necessitates SMEs to maintain a continuous and consistent approach to cybersecurity management. In cases where the company does not have an in-house professional with specialized ICT knowledge, which is common for non-technical SMEs, there is a requirement to invest in external expert assistance.

### 4. Security Concerns

This can be a beacon for cybercriminals due to their limited resources for robust security measures. In addition, IT sprawl is common in SMEs, where in a rush to solve and make decisions quickly teams often have to make tools with immediate solutions in mind rather than long term productivity. This can lead to creation of environments where tools don't work well together, weakening integrations and lowering security.



### 5. Scalability Challenges

The scalability of current technology solutions for SMEs may pose challenges due to factors such as limited resources, outdated or inadequate technology, risk management concerns, and the necessity to ensure compliance with diverse regulations. While scalability is desirable, it can present a notable challenge for SMEs.

## 6. Data Management

Data Management can pose a technological challenge to SMEs because of the lack of proper data governance structures and policies in place. This can result in issues to do with data ownership, access controls and overall data governance which leads to potential compliance and security risks. In addition, SMEs may lack the resources to implement robust cybersecurity measures, which makes them more vulnerable to data breaches.

## 7. Compliance and Regulation

Compliance and regulation can pose a significant challenge to SMEs due to their specific characteristics. SMEs operating in complex and evolving regulatory landscapes can struggle to ensure compliance with various laws and regulations especially when they don't have proper guidelines in place. In addition to this SMEs may find it challenging to implement different financial, environmental and data protection measures necessary to secure these landscapes.

## 8. Backup and Disaster Recovery

For SMEs creation of reliable disaster recovery plans may appear to be a complex or overwhelming task. This may be due to lack of proper employee training on procedures in place in the event of a disaster, the limited exposure to testing and validation of backup and disaster recovery plans, Insufficient IT resources or limited technological infrastructure to support efficient backup processes.

## 9. Shadow IT/ Personal devices

Many SMEs have allowed their staff to use their own personal devices to access company data. This practice increased as a result of the pandemic. During the pandemic, many SMEs did not have the budget and resources to purchase and configure corporate devices for their remote workers. This resulted to many SMEs allowing their staff members to use their personal devices to access company systems and data.









## CVEQ Framework Development Process

### Objectives



### CVEQ is best used to;

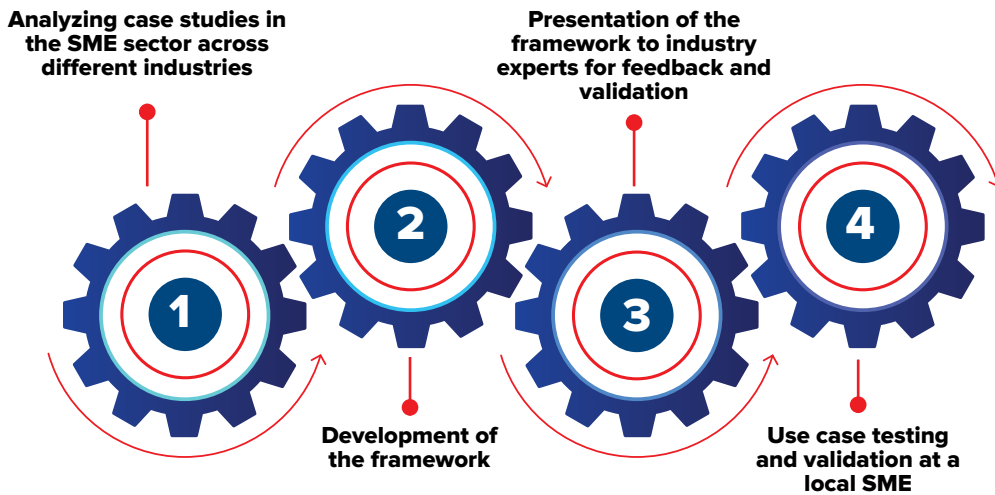
-  **Implement common criteria for assessing program effectiveness** - CVEQ provides a standardized approach to assessing and measuring the effectiveness of cyber security controls through the use of control domain, control assertions and reporting statements.
  -  **Reduce communication and compliance burden** - CVEQ reduces the need and amount of time spent responding to information requests from key stakeholders, especially regulators, shareholders and partners.
  -  **Optimize risk reduction at different levels of investment** - CVEQ's flexibility enables organisations adjust cyber security investments based on the changing risk environment. As a riskbased framework, CVEQ guides the organisation to invest in the most critical solution.
  -  **Scalability and flexibility** - It is useful to organisations of varying sizes and across all industries including public sector, SMEs, financial services and more.
  -  **Deliver management flexibility** - CVEQ gives organisations' the flexibility to pick and select different frameworks without restricting to use a specific cybersecurity description or set of control guidelines.
  -  **Evolutionary nature** - It will be updated and modified in future based on marketplace adoption, a changing environment, specialized organisational and stakeholder experience.
- At its core, CVEQ is also popular due to;

## Target Audience

The framework is targeting SMEs using technology.

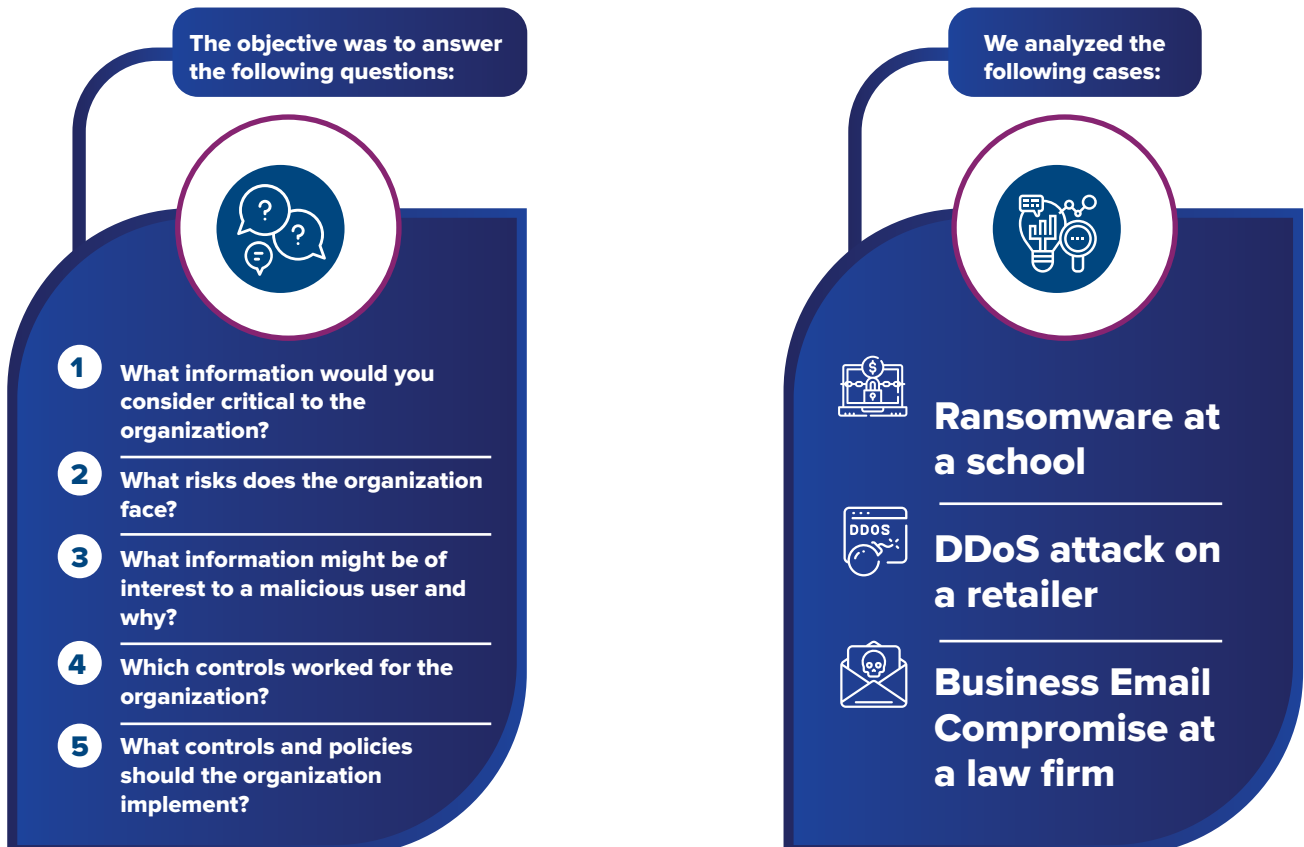
## Methodology

Our methodology involved:



## Case studies

The purpose of the case studies was to analyze cyber-attacks that had occurred at SMEs within various industries.





## Outcome

1. What information would you consider critical?	
<b>School</b>	<ul style="list-style-type: none"> <li>• Medical records</li> <li>• Financial records</li> <li>• Payroll data</li> <li>• Student data (they are minors)</li> <li>• Curriculum data (critical to the school)</li> <li>• Student account balances</li> <li>• Student Biodata</li> <li>• Data on dietary requirements</li> <li>• Research data (proprietary)</li> </ul>
<b>Retailer</b>	<ul style="list-style-type: none"> <li>• Customer data (that might be classified as sensitive e.g. bank card data)</li> <li>• Financial information (e.g., accounting information on sales etc.)</li> <li>• Demographic and geographic information (used in deliveries e.g., PII) - customers and suppliers</li> <li>• Price list and discounts regime (intellectual property)</li> <li>• Stock levels</li> <li>• Information about loyalty programs (has financial implications)</li> <li>• Ordering and re-ordering protocol</li> <li>• Supplier information</li> </ul>
<b>Law Firm</b>	<ul style="list-style-type: none"> <li>• Client information (names and ID numbers)</li> <li>• Buyer/Seller information (e.g signatures)</li> <li>• Property information (plot number etc.)</li> <li>• Transaction information (amount involved etc.)</li> <li>• Contractual information (sensitive specifics detailed in the contract)</li> </ul>

2. What risks does the organization face?	
<b>School</b>	<ul style="list-style-type: none"> <li>• Loss of data to a third party</li> <li>• Financial loss (had they not been able to decrypt the encryption, fines and penalties (regulatory))</li> <li>• Loss of data security and privacy</li> <li>• Reputational damage (if the parents found out or information of the breach was discovered)</li> <li>• Disruption of the school program/operations</li> <li>• Legal risk (potential for lawsuit for the loss of data/breach of privacy – locally and globally possibly, GDPR)</li> <li>• Risk of phishing the victims (minors, staff etc)</li> </ul>
<b>Retailer</b>	<ul style="list-style-type: none"> <li>• Reputational risks</li> <li>• Loss of revenue</li> <li>• Potential for fines (legal implications)</li> <li>• Diversion of payments through online banking</li> <li>• Loss of data (business continuity)</li> <li>• Software malfunction risk (or tampering of software)</li> <li>• Risk of being online</li> <li>• Although the benefit of being online may outweigh the risk, it is better to strengthen defenses by taking into account the risks of being online.</li> </ul>
<b>Law Firm</b>	<ul style="list-style-type: none"> <li>• Reputational risk</li> <li>• Financial risk</li> <li>• Legal risk</li> <li>• Identity theft</li> <li>• Data integrity – Their data can be compromised by threat actors.</li> </ul>

3. Which controls worked for the organization?	
<b>School</b>	<ul style="list-style-type: none"> <li>• Having a Cyber insurance policy</li> <li>• Partnership with an information security entity that assisted with the forensic investigation and provided advice on the incident.</li> </ul>
<b>Retailer</b>	<ul style="list-style-type: none"> <li>• Geo-blocking</li> <li>• IP address filtering</li> <li>• DDoS protections</li> <li>• Cyber insurance that provided incidence response and a payment that assisted in remediation efforts.</li> <li>• A Business Continuity Response plan</li> </ul>
<b>Law Firm</b>	<ul style="list-style-type: none"> <li>• Cyber insurance that helped enable the transaction to proceed.</li> </ul>

4. Which controls and policies should the organization implement?	
<b>School</b>	<ul style="list-style-type: none"> <li>• A VPN and firewalls securing remote access for staff</li> <li>• Offline backups</li> <li>• Proper password hygiene Use of MFA</li> <li>• Daily offline backups</li> <li>• Robust backup policy (guiding backup storage outside of day-to-day servers)</li> <li>• Implement penetration testing, system monitoring, intrusion detection, frequent patching and updating</li> <li>• Implement a risk management framework</li> <li>• Implement anti-malware anti-virus controls</li> <li>• Implement user awareness training.</li> </ul>
<b>Retailer</b>	<ul style="list-style-type: none"> <li>• Checking spam messages</li> <li>• Early Warning (Real Time monitoring) system tracking traffic and website access</li> <li>• Data Backup system</li> <li>• Strong Change Management controls (to manage changes in pricing or business systems)</li> <li>• Firewalls &amp; intrusion scanning systems</li> <li>• A defined risk appetite and a clear determination of escalation points</li> <li>• Have an Incidence management policy and response team (internal)</li> <li>• Frequent Vulnerability Assessment/Penetration Testing</li> </ul>
<b>Law Firm</b>	<ul style="list-style-type: none"> <li>• Two-factor authentication to secure their emails better.</li> <li>• User awareness training for their staff to better identify phishing attempts.</li> <li>• Extra verification between clients/law firm and law firm/bank before the transaction is carried out. e.g a phone call.</li> </ul>



Every opportunity has a different intensity of risks and benefits for different people. Choose the opportunities that fit best in your risk-benefit matrix.

- Sukant Ratnakar

## Industry Engagement

We hosted a forum to engage with industry professionals across different industries to reveal the framework, interrogate its capability and obtain feedback on it.

## Testing and Validation

### Background

CVEQ has demonstrated its effectiveness in directing us to pose pertinent questions tailored to specific areas of the organization. As illustrated below, the results are remarkably straightforward yet impactful. They are also accessible to executives throughout the organization, regardless of their level of technological expertise.

### The Problem

The SME sector in Africa is a magnet for cyber criminals. SMEs are expanding their use of technology, including cloud, mobile devices, smart technologies and work force mobility techniques. Embracing technology has however unlocked their doors to vulnerabilities and cybercrime.

### The Organization

We chose a Kenyan based financial institution for testing. The organization is progressive and has a wide range of services including mobile banking. The selected organization was ideal for testing the framework as it allowed us to test the different assumptions we had made when developing the framework.

### The Assessment

A coordination meeting was convened with the internal ICT security stakeholders. The CVEQ assessment for selected areas took 3 days to conduct whilst on site. We then carried out further analysis and tailored the reports to capture the organization's overall visibility and exposure respectively.

### Data Collection

The data collection process of the assessment was fairly direct. We relied on a qualified and experienced internal analyst to conduct the assessment and capture the data effectively.

### Reporting

The assessment team were able to document and present a summary report that visualised the overall status of cyber posture across the four CVEQ control areas i.e. Inherent Risk, Risk Oversight, Control Framework and Threat Detection.



Photos From The Validation Workshop - Group Discussions





## Framework Components

### About the CVEQ Framework

The CVEQ framework is an innovative risk modeling and quantification approach that enables organizations to measure and quantify their cyber security risk. The CVEQ Framework concepts are based on the globally accepted credit scoring methodology - where a statistical analysis is performed by lenders and financial institutions to access an entity's credit risk based on four key elements: Assets, Liabilities, Income and Liquidity.

The CVEQ framework, enables organizations to model and measure cyber risk using a unique scoring methodology. The CVEQ Cyber Risk Score (CVEQ Score) is a comprehensive, risk-based measurement of cyber risk exposure that indicates an organization's overall cyber risk posture.

An organization's CVEQ Score is a holistic measure that provides the entire leadership team a consistent barometer of cyber security risk with transparency to properly manage their risk posture through management, monitoring, remediation, and transference via insurance.

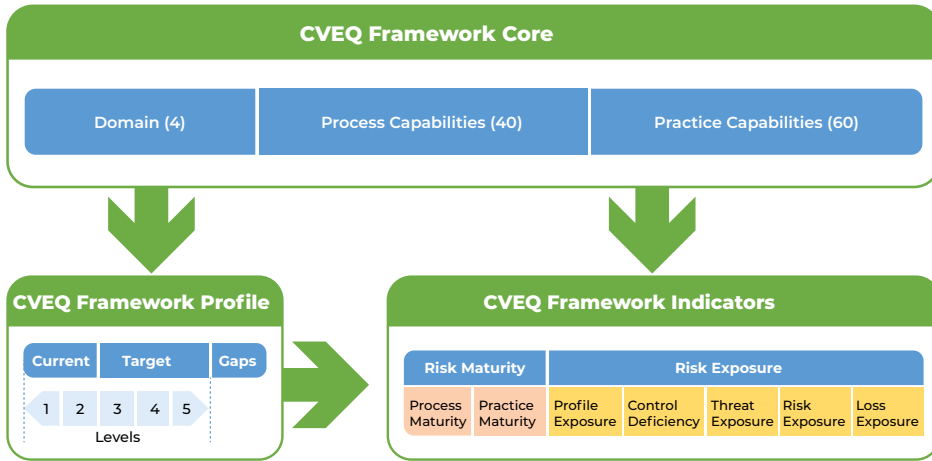
The framework uses knowledge and insights from numerous datasets (research and global/regional partners) and client specific assessment that enables us to model and measure an organization's risk exposure, control effectiveness and loss exposure using both internal and external data sources.

The framework is built on supporting the following core principles:

- 1. Adopt a common criterion for assessing and implementing cyber security program** - CVEQ provides a standardized approach to assessing, implementing and measuring an organization's risk posture through the use of standardized domains, capabilities, metrics, and factors.
- 2. Optimize risk reduction capacity and capability at different levels of investment** - CVEQ enables organizations to adjust cyber security investments based on the changing risk environment. As a risk-based framework, CVEQ guides the organization to invest in the most critical risk countermeasures and track how these investments impact the organization's risk posture.
- 3. Demonstrate alignment with globally recognized best practices** - CVEQ gives organizations the flexibility to pick and select different frameworks without restricting them to use a specific cyber security guideline or a set of control guidelines.
- 4. Reduce stakeholder communication and compliance burden** - CVEQ reduces the need and amount of time spent communicating an organization's Cyber risk posture and responding to information requests from different stakeholders, especially regulators, shareholders and partners.
- 5. Continuously identify gaps and opportunities in the Cyber risk program** - CVEQ framework enables an organization to identify gaps in its current Cyber risk programs and processes; prioritize opportunities for improvement; and, assess progress towards reaching its target Cyber risk posture.

Below diagram provides a pictorial overview of the cyber security framework and its components.

**CVEQ Framework Core**



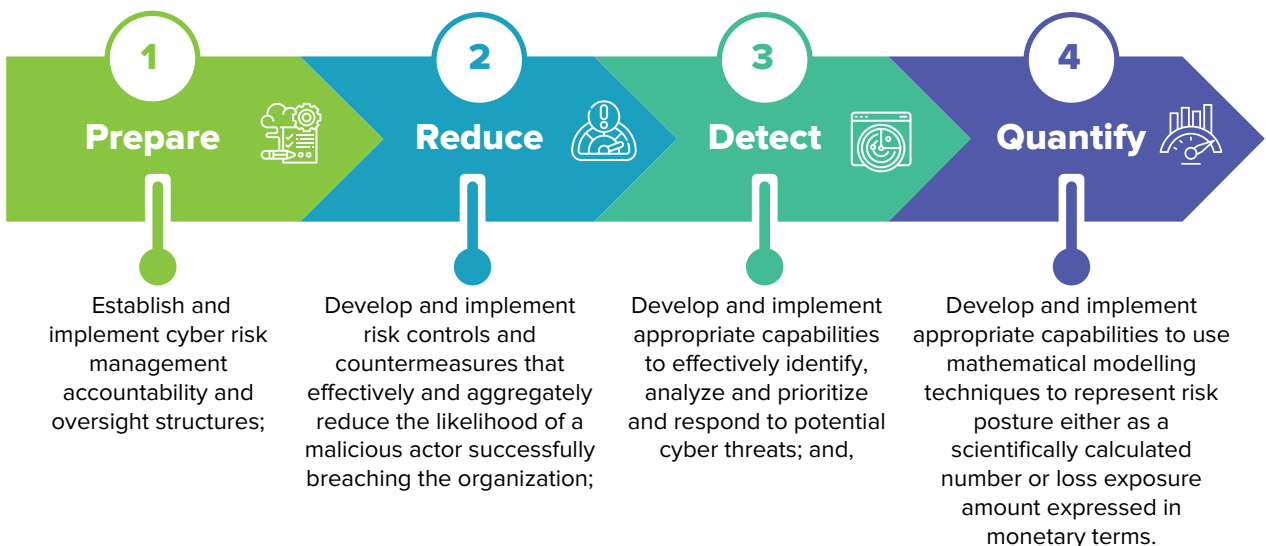
**Cybersecurity Framework Elements**

The Framework core elements work together as follows:

The CVEQ Framework Domains organize Cyber risk management activities at their highest level. They aid the organization in expressing its Cyber risk management activities by organizing information, enabling risk management decisions, addressing threats, implement controls, and improving by learning from previous activities.

The Domains also align with existing methodologies for risk communication and help show the effect of investments in cybersecurity. For example, investments in threat detection capabilities support timely detection and response actions, resulting in reduced impact to the delivery of services.

The four Framework Core Domains are:



## Framework Elements

- **CVEQ General Process Capabilities** are the subdivisions of a Domain into groups of Cyber risk competencies closely tied to programmatic needs and particular activities within the specific domain. Examples of General Capabilities include Data Profile, Risk Oversight, and Control Design.
- **CVEQ Core Process Capabilities** refers to a set of four competencies deemed essential and that each organization is encouraged to develop to ensure they build a strong and sustainable Cyber risk program. The four core capabilities are Risk Oversight, Control Framework, Threat Detection and Risk Analytics.
- **CVEQ Core Practice Capabilities** refers to a capability that supports the achievement of a CVEQ Core capability. Each core capability is decomposed into a set of sub-capabilities that are necessary and sufficient to support the objective of the core capability.

## Framework Profile and Indicators

The CVEQ Framework Profile is the alignment of the domains, capabilities, and core capabilities with the business requirements, risk profile, and resources of the organization.

A profile enables organizations to establish a roadmap for reducing Cyber risk exposure that is well-aligned with organizational goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. The Profiles can be used to describe the current state or the desired target state of specific Cyber risk activities. The Current Profile indicates the Cyber risk outcomes that are currently being achieved. The Target Profile indicates the outcomes needed to achieve the desired Cyber risk management goals. Profiles support business/mission requirements and aid in communicating risk within and between organizations.

CVEQ Framework Indicators are measurable information used to determine if an Authority is implementing their Cyber risk program as expected and achieving their intended outcomes.

The CVEQ Framework Indicators are broken down into:

- **Risk Maturity Indicators** - measure the Cyber risk program's risk management activities and outputs to indicate whether the program is being implemented as planned; and,
- **Risk Exposure Indicators** - measure whether the Cyber risk program is achieving the expected goal of reducing Cyber risk exposure and improving the overall Cyber risk posture in the short, intermediate, and long term.



## Framework Maturity Indicators

The CVEQ Framework Risk Maturity Levels provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Ranging from Basic (Level 1) to Leading (Level 5), Levels describe an increasing degree of sophistication in Cyber risk management practices.

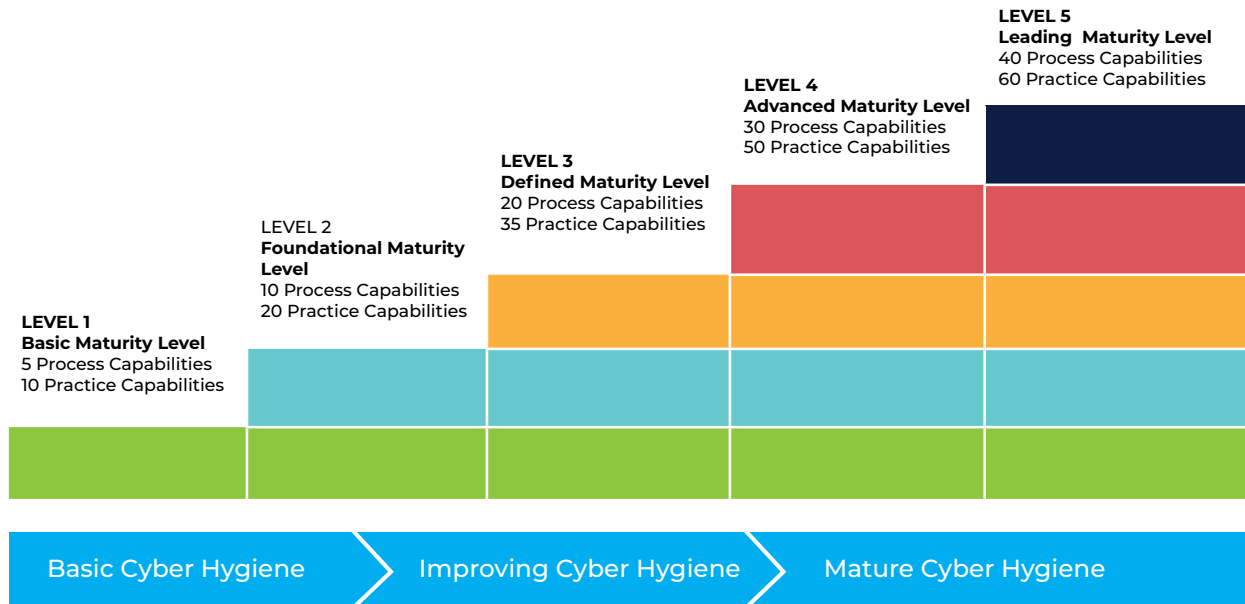
They help determine the extent to which Cyber risk management is informed by business needs and is integrated into an organization’s overall risk management program.

The CVEQ Risk Maturity model levels and the associated sets of capabilities and sub-capabilities across domains are cumulative. In order for an organization to achieve a specific CVEQ level it must demonstrate achievement of the preceding lower levels.

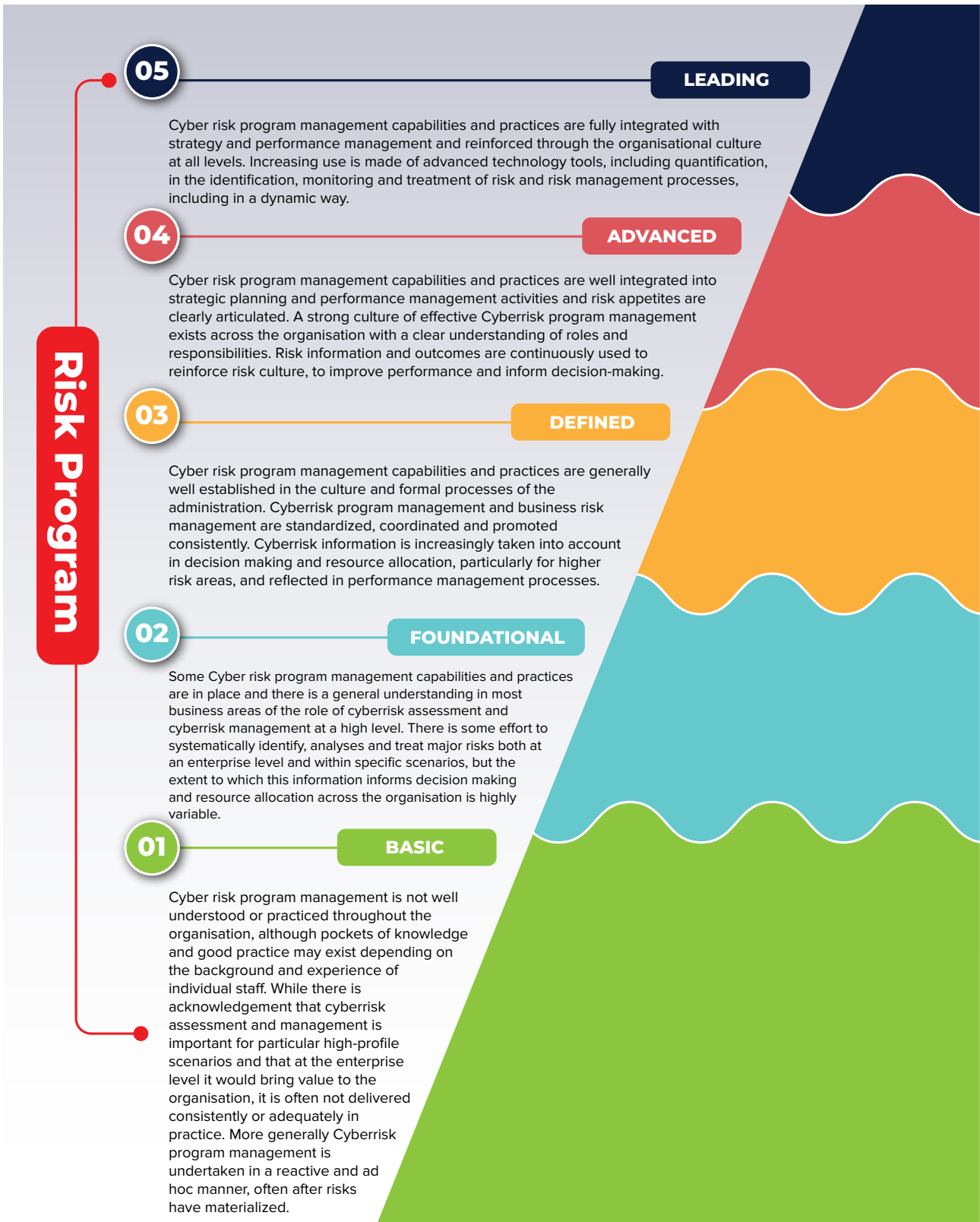
While organizations identified as Level 1 are encouraged to consider moving toward Level 2 or greater, Levels act as simple flexible guides with minimum requirement. Levels are meant to support organizational decision making on how to manage cybersecurity risk, as well as which dimensions of the organization are higher priority and could receive additional resources.

Progression to higher Levels is encouraged when a cost benefit analysis (CBA) indicates a feasible and cost-effective reduction of cybersecurity risk. An organization completes a successful implementation of the CVEQ Framework when it achieves the outcomes described in its Target Profiles; however, Level selection and designation naturally affect CVEQ Framework Profiles.

### CVEQ Maturity Levels and Associated Implementation Tiers



CVEQ Maturity Levels and Profile Descriptions

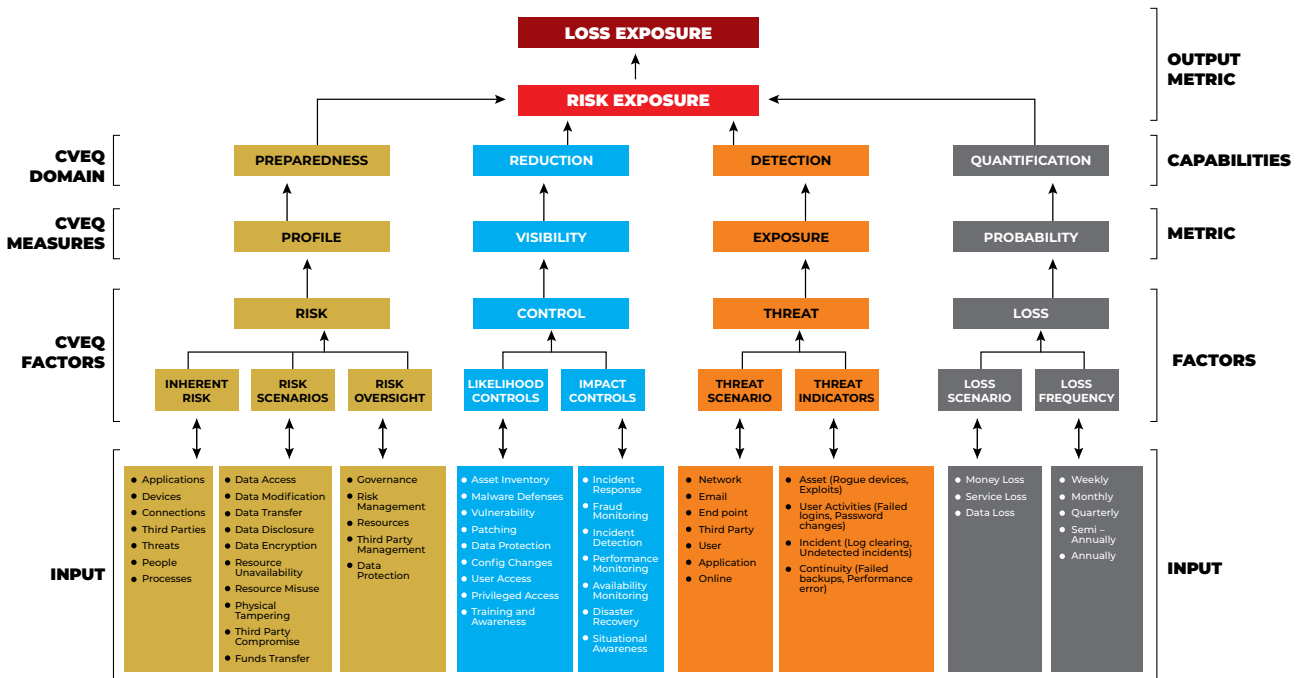


## Framework Exposure Indicators

The CVEQ Risk Exposure Indicators measure and track an organization’s exposure to Cyber risk at a particular point in time. The measurement tracks over 400 data points across an organization’s core Cyber risk management capabilities; risk preparedness, risk reduction and risk detection. The indicators enable an organization to quantify a wide range of Cyber risk scenarios. This enables the organization to represent its Cyber risk posture either as a scientifically calculated number or amount expressed in monetary terms.

The following capabilities are tracked by indicators:

- **Profile Exposure Indicator** – measures an organization’s ability to establish and implement Cyber risk management accountability and oversight structures.
- **Control Deficiency Indicator** – measures an organization’s ability to implement controls and risk countermeasures that effectively and aggregately reduce the likelihood of a successful Cyber breach
- **Threat Exposure Indicator** – Measures and tracks an organization’s ability to effectively identify, analyze, prioritize and respond to potential cyber threats.
- **Risk Exposure Indicator** – Measures and tracks an organization’s exposure to a range of possible negative or loss (data, service or money) outcomes that an organization is likely to experience based on a wide range of factors at a particular point in time.
- **Loss Exposure Indicator** – Measures and tracks potential aggregate financial losses that an organization is likely to face as a result of successful Cyber risk breaches or attacks in a specific period.



## Annex and Appendix

### Framework Summary

#### Risk Profile

The CVEQ Risk profiling domain is designed to enable organizations to determine their sources and levels of inherent risks prior to putting in controls that will be able to mitigate them. It provides a holistic view of the environment and the major risk factors.

The CVEQ Risk Profile domain measures risks across the following categories:

1. **Inherent Risk Analysis:** The organization identifies and analyzes the amount of risk posed to the organization by its technologies and connections, delivery channels, products and services, organizational characteristics, and external threats, notwithstanding the organization's risk-mitigating controls.
2. **Data Assessment:** The organization identifies data available within the organization and determines risks related to usage of this data based on confidentiality, availability and integrity of the file type, contents, and other metadata.
3. **Risk Assessment:** The organisation identifies and analyses a set of cyber risk events whose occurrence increases the probability or likelihood of a successful cyber breach, identifies a range of options for mitigating identified risks, determines the level of treatment plans required for each risk level and prepares risk mitigation action plans

#### Risk Oversight

The CVEQ Risk Oversight domain measures an organisation's ability to establish and implement Cyber risk management accountability and oversight structures.

The CVEQ Risk Oversight domain measures risks across the following categories:

1. **Risk Governance** - The organization establishes and implements cyber risk management and accountability structures to ensure risks are adequately mitigated
2. **Risk Reporting** - The organisation compiles and communicates timely information indicating the organisations risk posture to different stakeholders based on relevant internal and external requirements.
3. **Policy Management** - The organisation develops and implements policies, procedures, and processes to manage and monitor the organization's cybersecurity related risk management.
4. **Control Management** - The organisation designs and implements risk countermeasures or controls that address identified risk scenarios, continuously identifies weaknesses or failures in the implemented controls and remediates these within reasonable timelines.
5. **Third Party Management** - The organisation has implemented processes and policies to oversee and manage third-party relationships including due diligence, contracts, ongoing monitoring, and decommissioning to ensure controls complement the organisation's cybersecurity program.



## Risk Control

The CVEQ Risk control domain is designed to measure an organisation's ability to implement controls and countermeasures that effectively and aggregately reduce the likelihood of an organisation's cyber risk exposure.

The CVEQ Risk Control domain measures risks across the following categories:

1. Asset Inventory - The organisation has implemented processes and tools to manage (take inventory, track, and correct) assets on the network.
2. Malware Defenses - The organisation has implemented processes and tools to control the installation, spread, and execution of malware at multiple points in the organisation.
3. Vulnerability and Patching - The organisation has implemented processes and tools used to detect, prevent and correct security vulnerabilities in devices that are listed and approved in the asset inventory database.
4. Network Security - The organisation has implemented processes and tools to actively manage (track, report on, correct) the security configuration of assets on the network.
5. Data Protection - The organisation has implemented processes and technical controls to identify, classify, securely handle, retain, and dispose of data.
6. User Access - The organisation should implement processes and tools used to control secure access to information based on an approved classification.
7. Privilege Access - The organisation should implement processes and tools used to control the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
8. User Awareness - The organisation has implemented processes and tools to develop and assess cybersecurity training and awareness programs.
9. Threat Monitoring - This metric measures the extent to which the organisation has implemented processes and tools to continuously collect, manage, and analyze internal and external sources of data that could help detect, understand, or recover from an attack.
10. Incident Response - The organisation should develop and implement an incident response process and infrastructure to ensure quick discovery, effective containment and restoration of the network and systems.
11. Payments Monitoring - The organisation has implemented processes and tools used to prevent exfiltration of funds, mitigate the effects of exfiltrated money and ensure the integrity of transactional information.
12. Data Recovery - The organisation should implement processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.
13. Service Availability - The organisation should implement processes and tools to continuously collect, manage, and analyze performance and availability of data that could help detect, understand, or recover from system unavailability or performance degradation incident.

### Threat Detection

The CVEQ threat detection domain measures an organisation's ability to effectively identify, analyze, prioritize and respond to potential cyber threats.

The CVEQ Risk Control domain measures risks across the following categories:

1. **Asset Detection** - The organisation identifies and develops technical and process capabilities to continuously identify and detect observable asset domain threat indicators, behaviours and anomalies.
2. **User Detection** - The organisation identifies and develops technical and process capabilities to continuously identify and detect observable user domain threat indicators, behaviours and anomalies.
3. **Incident Detection** - The organisation identifies and develops technical and process capabilities to continuously identify and detect observable incident domain threat indicators, behaviours and anomalies.
4. **Continuity Detection** - The organisation identifies and develops technical and process capabilities to continuously identify and detect observable continuity domain threat indicators, behaviours and anomalies.



Threat is a mirror of security gaps. Cyber-threat is mainly a reflection of our weaknesses. An accurate vision of digital and behavioral gaps is crucial for a consistent cyber-resilience.

- *Stephane Nappo*

## Framework References

	Control Area	Global Standards/ Framework Mapping	Control Description	Control Practices
<b>RISK PROFILE</b>	1. INHERENT RISK ANALYSIS	<ul style="list-style-type: none"> <li>• COBIT 2019 APO02.01, APO02.06, APO03.01</li> <li>• ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6</li> <li>• NIST SP 800-53 Rev. 4 PM-11, SA-14</li> </ul>	The organisation identifies and analyzes the amount of risk posed to the organisation by its technologies and connections, delivery channels, products, people and services, organizational characteristics, and external threats, notwithstanding the organization's risk-mitigating controls.	<ul style="list-style-type: none"> <li>• Establish and maintain a detailed inherent risk profiling process</li> <li>• Determine the impact of technologies on the organisations cyber risk</li> <li>• Determine the impact of products and services on the organisations cyber risk</li> <li>• Determine the impact of operational processes on the organisations cyber risk</li> <li>• Determine the impact of employees, service providers and partners on the organisations cyber risk</li> </ul>
	2. DATA ASSESSMENT	<ul style="list-style-type: none"> <li>• CIS 3.7, CIS 3.2,CIS 3.12, ID.AM-5, PR.AC-5rd pa</li> <li>• CCS CSC 17</li> <li>• COBIT 2019 APO01.06, BAI02.01, BAI06.01, DSS06.06</li> <li>• ISA 62443-3-3:2013 SR 3.4, SR 4.1</li> <li>• ISO/IEC 27001:2022 A.8.2.3</li> <li>• NIST SP 800-53 Rev. 4 SC-28</li> </ul>	The organisation identifies data available within the organisation and determines risks related to usage of this data based on confidentiality, availability and integrity of the file type, contents, and other metadata.	<ul style="list-style-type: none"> <li>• Establish and maintain detailed data profiling assessment process</li> <li>• Determine type(s) of critical data used in the organisation</li> <li>• Determine location(s) of critical data used in the organisation</li> <li>• Determine sensitivity level(s) of critical data used in the organisation</li> </ul>
	3. RISK ASSESSMENT	<ul style="list-style-type: none"> <li>• CCS CSC 4</li> <li>• COBIT 2019 APO12.01, APO12.02, APO12.03, APO12.04</li> <li>• ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12</li> <li>• ISO/IEC 27001:2022 A.12.6.1, A.18.2.3</li> <li>• NIST SP 800-53 Rev. 4 CA-2, CA-7, CA- 8,</li> <li>• RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5</li> </ul>	The organisation identifies and analyses a set of cyber risk events whose occurrence increases the probability or likelihood of a successful cyber breach, identifies a range of options for mitigating identified risks, determines the level of treatment plans required for each risk level and prepares risk mitigation action plans.	<ul style="list-style-type: none"> <li>• Establish and maintain a detailed cyber risk assessment process</li> <li>• Analyse and document potential risk (events) scenarios</li> <li>• Determine risk likelihood and impact</li> <li>• Prioritize the potential risk (events) scenarios</li> <li>• Prioritize potential threat (events) scenarios</li> <li>• Review and select risk (controls) mitigation controls</li> </ul>

Control Area	Global Standards/ Framework Mapping	Control Description	Control Practices
<b>RISK OVERSIGHT</b>	4. RISK GOVERNANCE	<ul style="list-style-type: none"> <li>• COBIT 2019 APO01.03, EDM01.01, EDM01.02</li> <li>• ISA 62443-2-1:2009 4.3.2.6</li> <li>• ISO/IEC 27001:2022 A.5.11</li> <li>• NIST SP 800-53 Rev. 4 -1 controls from all families</li> </ul>	<p>The organization establishes and implements cyber risk management and accountability structures to ensure risks are adequately mitigated</p> <ul style="list-style-type: none"> <li>• Establish a board and/or management level committee to oversee cyber security program</li> <li>• Allocate a budget to cybersecurity program and initiatives</li> <li>• Recruit and outsource cybersecurity personnel to oversee cyber security program</li> </ul>
	5. RISK REPORTING	<ul style="list-style-type: none"> <li>• CCS CSC 4</li> <li>• COBIT 2019 APO12.01, APO12.02, APO12.03, APO12.04</li> <li>• ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12</li> <li>• ISO/IEC 27001:2022 A.12.6.1, A.18.2.3</li> <li>• NIST SP 800-53 Rev. 4 CA-2, CA-7, CA- 8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5</li> </ul>	<p>The organisation compiles and communicates timely information indicating the organisations risk posture to different stakeholders based on relevant internal and external requirements.</p> <ul style="list-style-type: none"> <li>• Define cyber risk reporting requirements for internal and external stakeholders</li> <li>• Determine reporting format and frequency</li> <li>• Share regular reports and seek feedback on provided information</li> </ul>
	6. POLICY MANAGEMENT	<ul style="list-style-type: none"> <li>• COBIT 2019 APO01.03, EDM01.01,</li> <li>• EDM01.02</li> <li>• ISA 62443-2-1:2009 4.3.2.6</li> <li>• ISO/IEC 27001:2022 A.5.11</li> <li>• NIST SP 800-53 Rev. 4 -1 controls from all families - NIST CSF ID.GV</li> </ul>	<p>The organisation develops and implements policies, procedures, and processes to manage and monitor the organization's cybersecurity related risk management.</p> <ul style="list-style-type: none"> <li>• Review and identify key regulatory, legal, risk, environmental, and operational cybersecurity requirements</li> <li>• Establish and document an organizational cybersecurity security policy</li> <li>• Establish and document cybersecurity procedures and processes</li> <li>• Share the documented policies and procedures with different stakeholders for approval and awareness</li> </ul>



Control Area	Global Standards/ Framework Mapping	Control Description	Control Practices
7. CONTROL MANAGEMENT	<ul style="list-style-type: none"> <li>• CCS CSC 7</li> <li>• COBIT 2019 DSS05.02, APO13.01</li> <li>• ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6</li> <li>• ISO/IEC 27001:2022 A.13.1.1, A.13.2.1</li> <li>• NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7</li> </ul>	<p>The organisation designs and implements risk countermeasures or controls that address identified risk scenarios, continuously identifies weaknesses or failures in the implemented controls and remediates these within reasonable timelines.</p>	<ul style="list-style-type: none"> <li>• Design and implement controls</li> <li>• Remediate control deficiencies</li> <li>• Designs and implement risk countermeasures or controls to address identified risk and threat (events) scenarios</li> <li>• Determine control objectives for implemented controls</li> <li>• Conduct independent reviews/audit of implemented controls to determine their efficiency/effectiveness</li> <li>• Share the documented policies and procedures with different stakeholders for approval and awareness</li> </ul>
8. THIRD PARTY MANAGEMENT	<ul style="list-style-type: none"> <li>• CCS CSC 9</li> <li>• COBIT 2019 APO07.03, APO10.04, APO10.05</li> <li>• ISA 62443-2-1:2009 4.3.2.4.2</li> <li>• ISO/IEC 27001:2022 A.6.1.1, A.7.2.2</li> <li>• NIST SP 800-53 Rev. 4 PS-7, SA-9</li> </ul>	<p>The organisation has implemented processes and policies to oversee and manage third-party relationships including due diligence, contracts, ongoing monitoring, and decommissioning to ensure controls on third party management are aligned with the organisation's cybersecurity program.</p>	<ul style="list-style-type: none"> <li>• Establish and maintain an inventory of third parties</li> <li>• Establish and maintain a third party management policy (classification, inventory, assessment, monitoring, and decommissioning of service providers)</li> <li>• Ensure third party contracts include security and data protection requirements</li> <li>• Ensure contracts include SLAs, indemnity insurance covers</li> <li>• Assess and monitor third parties</li> <li>• Establish and maintain a decommissioning process</li> </ul>

	Control Area	Global Standards/ Framework Mapping	Control Description	Control Practices
<b>RISK CONTROL</b>	9. ASSET INVENTORY	<ul style="list-style-type: none"> <li>• CCS CSC 1</li> <li>• COBIT 2019 BAI09.01, BAI09.02</li> <li>• ISA 62443-2-1:2009 4.2.3.4</li> <li>• ISA 62443-3-3:2013 SR 7.8</li> <li>• ISO/IEC 27001:2022 A.8.1.1, A.8.1.2</li> <li>• NIST SP 800-53 Rev. 4 CM-8</li> </ul>	The organisation has implemented processes and tools to manage (take inventory, track, and correct) assets on the network	<ul style="list-style-type: none"> <li>• Asset register (Hardware and Software inventory listing) - Including information on data types, data location, and asset criticality levels</li> <li>• Asset Discovery Tool</li> <li>• Authorized Software Inventory</li> </ul>
	10. MALWARE DEFENSES	<ul style="list-style-type: none"> <li>• CCS CSC 5</li> <li>• COBIT 2019 DSS05.01</li> <li>• ISA 62443-2-1:2009 4.3.4.3.8</li> <li>• ISA 62443-3-3:2013 SR 3.2</li> <li>• ISO/IEC 27001:2022 A.12.2.1</li> <li>• NIST SP 800-53 Rev. 4 SI-3</li> <li>• NIST CSF DE.CM-4</li> </ul>	The organisation has implemented processes and tools to control the installation, spread, and execution of malware at multiple points in the organisation.	<ul style="list-style-type: none"> <li>• Establish a process to identify and remediate malware</li> <li>• Deploy and Maintain Anti-Malware Software</li> <li>• Configure Automatic Anti-Malware Signature Updates</li> <li>• Centrally Manage Anti-Malware Software</li> <li>• Use advanced Anti-Malware Software for Critical Devices</li> <li>• Use email malware protection tools</li> </ul>
	11. VULNERABILITY AND PATCHING	<ul style="list-style-type: none"> <li>• CCS CSC 4</li> <li>• COBIT 2019 APO12.01, APO12.02, APO12.03, APO12.04</li> <li>• ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12</li> <li>• ISO/IEC 27001:2022 A.12.6.1, A.18.2.3</li> <li>• NIST SP 800-53 Rev. 4 CA-2, CA-7, CA- 8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5</li> <li>• NIST CSF ID.RA</li> </ul>	The organisation has implemented processes and tools used to detect, prevent and correct security vulnerabilities in devices that are listed and approved in the asset inventory database.	<ul style="list-style-type: none"> <li>• Establish and Maintain a Vulnerability Management Process.</li> <li>• Perform Automated OS/Application Patch Management</li> <li>• Remediate detected vulnerabilities and retest</li> </ul>

Control Area	Global Standards/ Framework Mapping	Control Description	Control Practices
12. NETWORK SECURITY	<ul style="list-style-type: none"> <li>• CCS CSC 14, 16</li> <li>• COBIT 2019 DSS05.07</li> <li>• ISA 62443-3-3:2013 SR 6.2</li> <li>• NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4</li> </ul>	The organisation has implemented processes and tools to actively manage (track, report on, correct) the security configuration of assets on the network.	<ul style="list-style-type: none"> <li>• Establish and maintain network architecture diagram(s)</li> <li>• Implement and manage perimeter and internal firewalls</li> <li>• Implement and manage intrusion detection and intrusion prevention systems</li> <li>• Disable unnecessary services on organisation assets and software</li> <li>• Segment the network based on data classification procedure</li> </ul>
13. DATA PROTECTION	<ul style="list-style-type: none"> <li>• CCS CSC 17</li> <li>• COBIT 2019 APO01.06, BAI02.01, BAI06.01, DSS06.06</li> <li>• ISA 62443-3-3:2013 SR 3.4, SR 4.1</li> <li>• ISO/IEC 27001:2022 A.8.2.3</li> <li>• NIST SP 800-53 Rev. 4 SC-28</li> </ul>	The organisation has moderately implemented processes and technical controls to identify, classify, securely handle, retain, and dispose of data.	<ul style="list-style-type: none"> <li>• Establish and maintain a data life cycle management and data inventory process</li> <li>• Establish and maintain an accurate data inventory</li> <li>• Configure data access control lists</li> </ul>
14. USER ACCESS	<ul style="list-style-type: none"> <li>• CCS CSC 16</li> <li>• COBIT 2019 DSS05.04, DSS06.03</li> <li>• ISA 62443-2-1:2009 4.3.3.5.1</li> <li>• ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9</li> <li>• ISO/IEC 27001:2022 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3</li> <li>• NIST SP 800-53 Rev. 4 AC-2, IA Family</li> </ul>	The organisation should implement processes and tools used to control secure access to information based on an approved classification.	<ul style="list-style-type: none"> <li>• Establish and maintain a user access management process</li> <li>• Establish and maintain an inventory of user accounts</li> <li>• Conduct regular reviews of the approved user access matrix</li> <li>• Require multi-factor authentication (MFA) for critical accounts</li> </ul>

Control Area	Global Standards/ Framework Mapping	Control Description	Control Practices
15. PRIVILEGE ACCESS	<ul style="list-style-type: none"> <li>CCS CSC 12, 15</li> <li>SA 62443-2-1:2009 4.3.3.7.3</li> <li>ISA 62443-3-3:2013 SR 2.1</li> <li>ISO/IEC 27001:2022 A.6.1.2, A.9.1.2,</li> <li>A.9.2.3, A.9.4.1, A.9.4.4</li> <li>NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5,</li> <li>AC-6, AC-16</li> </ul>	The organisation should implement processes and tools used to control the use, assignment, and configuration of administrative privileges on computers, networks, and applications.	<ul style="list-style-type: none"> <li>Establish and maintain a privilege access management process</li> <li>Establish and maintain an inventory of privilege user accounts</li> <li>Conduct regular reviews of the approved privilege user access matrix</li> <li>Require multi-factor authentication (MFA) for all administrative accounts</li> </ul>
16. USER AWARENESS	<ul style="list-style-type: none"> <li>CCS CSC 9</li> <li>COBIT 2019 APO07.03, BAI05.07</li> <li>ISA 62443-2-1:2009 4.3.2.4.2</li> <li>ISO/IEC 27001:2022 A.7.2.2</li> <li>NIST SP 800-53 Rev. 4 AT-2, PM-13</li> </ul>	The organisation has implemented processes and tools to develop and assess cybersecurity and data protection training and awareness programs.	<ul style="list-style-type: none"> <li>Establish and maintain a security awareness and training program</li> <li>Conduct awareness and training sessions for different stakeholders</li> <li>Conduct phishing and social engineering tests</li> </ul>
17. THREAT MONITORING	<ul style="list-style-type: none"> <li>CCS CSC 14, 16</li> <li>COBIT 2019 DSS05.07</li> <li>ISA 62443-3-3:2013 SR 6.2</li> <li>NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4</li> </ul>	This metric measures the extent to which the organisation has implemented processes and tools to continuously collect, manage, and analyze internal and external sources of data that could help detect, understand, or recover from an attack.	<ul style="list-style-type: none"> <li>Establish and maintain a listing of all critical data log sources</li> <li>Establish and maintain a listing of prioritized threat scenarios.</li> <li>Implement capabilities to collect, analyze and detect threats</li> <li>Monitor and escalate incidents to relevant stakeholders</li> </ul>
18. INCIDENT RESPONSE	<ul style="list-style-type: none"> <li>COBIT 2019 DSS04.03</li> <li>ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1</li> <li>ISO/IEC 27001:2022 A.16.1.1, A.17.1.1, A.17.1.2</li> <li>NIST SP 800-53 Rev. 4 CP-2, IR-8</li> </ul>	The organisation should develop and implement an incident response process and infrastructure to ensure quick discovery, effective containment and restoration of the network and systems.	<ul style="list-style-type: none"> <li>Maintain an incident response plan.</li> <li>Educate users on how to identify and report security incidents</li> <li>Conduct Periodic Incident Scenario Sessions for Personnel</li> </ul>

Control Area	Global Standards/ Framework Mapping	Control Description	Control Practices
19. PAYMENTS MONITORING	<ul style="list-style-type: none"> <li>NIST SP 800-53 Rev. 4 AU-12, CA-7,</li> <li>CM-3, CM-8, PE-3, PE-6, PE-20, SI-4</li> </ul>	The organisation has implemented processes and tools used to prevent exfiltration of funds, mitigate the effects of exfiltrated money and ensure the integrity of transactional information.	<ul style="list-style-type: none"> <li>Establish and maintain an inventory of payment systems</li> <li>Establish and maintain a listing of prioritized fraud scenarios.</li> <li>Implement capabilities to collect, analyze and detect payment anomalies</li> <li>Monitor and escalate incidents to relevant stakeholders</li> </ul>
20. DATA RECOVERY	<ul style="list-style-type: none"> <li>COBIT 2019 APO13.01</li> <li>ISA 62443-2-1:2009 4.3.4.3.9</li> <li>ISA 62443-3-3:2013 SR 7.3, SR 7.4</li> <li>ISO/IEC 27001:2022 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3</li> <li>NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9</li> </ul>	The organisation should implement processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.	<ul style="list-style-type: none"> <li>Establish and maintain data recovery policy and process</li> <li>Establish and maintain an inventory of all systems for data recovery</li> <li>Perform automated backups</li> <li>Protect recovery data and maintain an isolated of instance of recovery data</li> <li>Conduct regular data recovery tests</li> </ul>
21. SERVICE AVAILABILITY	<ul style="list-style-type: none"> <li>COBIT 2019 APO13.01</li> <li>ISA 62443-3-3:2013 SR 7.1, SR 7.2</li> <li>ISO/IEC 27001:2022 A.12.3.1</li> <li>NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5</li> </ul>	The organisation should implement processes and tools to continuously collect, manage, and analyze performance and availability data that could help detect, understand, or recover from system unavailability or performance degradation incident.	<ul style="list-style-type: none"> <li>Establish and maintain system availability policy and process</li> <li>Establish and maintain an inventory of all systems for availability</li> <li>Perform continuous monitoring of key operational systems</li> <li>Conduct regular service availability tests</li> </ul>



	Control Area	Global Standards/ Framework Mapping	Control Description	Control Practices
<b>THREAT DETECTION</b>	22. ASSET DETECTION	<ul style="list-style-type: none"> <li>• MITRE T1200, T1072, T1542, T1105, T1012, T1595.002</li> <li>• T1602</li> <li>• CCS CSC 5</li> <li>• COBIT 2019 DSS05.01</li> <li>• ISA 62443-2-1:2009 4.3.4.3.8</li> <li>• ISA 62443-3-3:2013 SR 3.2</li> <li>• ISO/IEC 27001:2022 A.12.2.1</li> <li>• NIST SP 800-53 Rev. 4 SI-3</li> </ul>	The organisation identifies and develops technical and process capabilities to continuously identify and detect observable asset domain threat indicators, behaviours and anomalies	<ul style="list-style-type: none"> <li>• Maintain a listing of all in-scope asset threat data log sources</li> <li>• Ensure all asset logged data is aggregated to a centralized analytics tool</li> <li>• Report and alert whenever an in scope asset threat data source is not sending logs</li> </ul>
	23. USER DETECTION	<ul style="list-style-type: none"> <li>• MITRE T1200, T1072, T1542, T1105, T1012, T1602</li> <li>• ISA 62443-3-3:2013 SR 6.2</li> <li>• ISO/IEC 27001:2022 A.12.4.1</li> <li>• NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13,</li> <li>• CA-7, CM-10, CM-11</li> </ul>	The organisation identifies and develops technical and process capabilities to continuously identify and detect observable user domain threat indicators, behaviours and anomalies	<ul style="list-style-type: none"> <li>• Maintain a listing of all in-scope user threat data log sources</li> <li>• Ensure all user logged data is aggregated to a centralized analytics tool</li> <li>• Report and alert whenever an in scope user threat data source is not sending logs</li> </ul>
	24. INCIDENT DETECTION	<ul style="list-style-type: none"> <li>• MITRE T1078, T1078.002, T1548.002, M1017</li> <li>• COBIT 2019 APO12.06</li> <li>• ISA 62443-2-1:2009 4.2.3.10</li> <li>• NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8</li> </ul>	The organisation identifies and develops technical and process capabilities to continuously identify and detect observable incident domain threat indicators, behaviours and anomalies	<ul style="list-style-type: none"> <li>• Maintain a listing of all in-scope user threat data log sources</li> <li>• Ensure all user logged data is aggregated to a centralized analytics tool</li> <li>• Report and alert whenever an in scope user threat data source is not sending logs</li> </ul>
	25. CONTINUITY DETECTION	<ul style="list-style-type: none"> <li>• MITRE T1490, TA0005, T1597.001</li> <li>• COBIT 2019 APO13.01</li> <li>• ISA 62443-2-1:2009 4.3.4.3.9</li> <li>• ISA 62443-3-3:2013 SR 7.3, SR 7.4</li> <li>• ISO/IEC 27001:2022 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3</li> <li>• NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9</li> </ul>	The organisation identifies and develops technical and process capabilities to continuously identify and detect observable continuity domain threat indicators, behaviours and anomalies	<ul style="list-style-type: none"> <li>• Maintain a listing of all in-scope continuity threat data log sources</li> <li>• Ensure all continuity logged data is aggregated to a centralized analytics tool</li> <li>• Report and alert whenever an in scope continuity threat data source is not sending logs</li> </ul>





**Institute of Risk Management**

2nd Floor, Sackville House  
143 - 149 Fenchurch Street,  
London, EC3M 6BN

**IRM EA Regional Group Contacts:**  
kenya@theirm.org

**[www.theirm.org](http://www.theirm.org)**



**Kenya Office**

14 Chalbi Drive, Lavington  
P. O. Box 56966 - 00200, Nairobi

☎ +254 (0) 20 200 6600

**Botswana Office**

Plot 54349, Office Block B  
3rd Floor, CBD Gaborone

+267 77 820 039

**Partners & Resellers**

- Ethiopia
- Nigeria
- Ghana
- Tanzania
- Lesotho
- Uganda
- Mauritius

✉ [info@serianu.com](mailto:info@serianu.com)

✕ [@serianultd](https://twitter.com/serianultd)

**in** [Serianu Limited](https://www.linkedin.com/company/serianu-limited)

**[www.serianu.com](http://www.serianu.com)**