Reimagining IT Sourcing for the Digital Age: Partnering for Success
Inside this report

1. Research Scope and Acknowledgment  5

2. Introduction  8

3. Survey Findings  14
   3.1 Governance within Saccos  15
   3.2 IT Security and Strategy  21
   3.3 Outsourcing and Vendor Security  27
   3.4 Business Continuity  32

4. Cyber Intelligence  39

5. Data Protection Law will Impact your Sacco  43

6. Priorities for 2021  48

7. Country Extension Officer Program  50
Acknowledgement

This report was prepared by the Serianu CyberThreat Intelligence Team in partnership with the Africa Cyber Immersion Center. We would like to acknowledge the following individuals who, among others made a major contribution to deliver this report:

Contributors
- Joy Adhiambo - Researcher and Editor
- Barbara Munyendo - Researcher
- Nabihah Rishad - Researcher
- Brian Nyali - Researcher
- Daniel Ndegwa - Researcher
- Brilliant Grant - Researcher
- Cedric Miheso - Sacco Coordinator

We also thank the Serianu Executive Team for their support and guidance:
- Chief Executive Officer, William Makatiani
- Chief Operations Officer, Joseph Mathenge
- Sales and Partnership Lead, Jackie Madowo

Industry Commentaries

The report features key insights from industry experts including:
- David Cracknell - Director, First Principles Consulting Ltd
- Wambui Mbesa - Chief Executive Officer, INTRASOFT International East Africa
- Cynthia Wandia - Co-founder and CEO, Kwara Ltd
- Amos Ngung’u - Information Security Manager, Harambee Sacco
- Carol Muchai - Project Manager, Serianu Ltd
- Martin Mwangi - Cybersecurity Consultant and Technical Solutions Lead, Serianu Ltd

Editor and Report Project Manager
Duncan Ondigo

Design, Layout and Production
Tonn Kriation

©2021 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 Serianu Limited.
1. Research Scope and Report Highlight
The 2020/2021 Sacco cyber security report was researched and compiled from data gathered through interviews, survey forms and interactions with about 110 Sacco’s across Kenya. The key themes covered in this report are:

**Research Scope**

**Governance within Saccos**
A deep dive into governance best practices within Saccos.

**IT Outsourcing**
We look at the need for evolution of the Sacco-vendor relationships from the traditional supplier-buyer relationship to that of partnerships for success.

**IT Security**
This section looks at management of cybersecurity, competency levels for IT management and challenges in implementing IT security.

**IT Governance**
In this section we look at the board’s role in ensuring the success of IT security programs and overall digital strategy, key challenges faced by board members and best practice to follow.

**Cyber Intelligence**
Mobile money fraud has been a top concern for most Saccos. We discuss attack vectors and vulnerabilities that facilitate the success of these attacks and way forward for Saccos.

**Impact of Data Protection Law to Saccos**
Are Saccos ready for the Kenya Data Protection Law? Here we discuss what Saccos need to do to stay compliant with the regulation.

**Priorities for 2020/2021**
As 2020 draws to a close, we have taken the key learnings and summarized them under this section. We also list must have investments for 2020/2021.

**County Cybersecurity Extension Officers Program**
In order to address the resourcing challenge and taking into consideration the unique challenges that saccos face, we developed the first ever concept of independent consultants available to walk with sacco executives during their digital transformation journey.

**Business Continuity**
This section looks at how prepared Saccos are in case of a disaster, key challenges faced in this process and best practice.
Sacco Cybersecurity Report 2020/2021

110

Number of saccos surveyed and interviewed across Kenya

10

10 Eastern

10 Rift Valley

10 Central

5 Western

5 Nyanza

1 North Eastern

30 Nairobi

40 Coast

110

Number of saccos surveyed and interviewed across Kenya

Something exciting is happening within the Sacco industry – digital transformation. Last year we looked at digital transformation within Saccos and highlighted the key milestones made. This year we look at a key outcome of digital transformation - partnering for success in the digital age. Saccos and indeed organisations in general have relied heavily on external vendors for supply of critical hardware, software and services including banking systems, IT infrastructure, services such as audits, cloud hosting etc.

Traditionally, these relationships have been governed by a buyer-seller mindset whereby as long as the service is delivered and payments are done, the relationship works. However, there is a swift transition from this mindset to that of a partner relationship.
Mature organisations are no longer buying hardware, software or a service. They are buying knowledge, processes, capacity and empowerment. They say it is not IF your organisation gets hacked but it is WHEN your organisation gets hacked. So what happens when your organisation is hacked? It is not the hardware or the software that becomes critical, it is more the knowledge, capacity and maturity of your partner that enables your institution to recover.

Therefore, there needs to be a bigger effort around partnering for success. As Saccos go through this digital transformation, they need to build foundations that will enable them to innovate operations and governance while building resilience.

We conducted an extensive survey that polled over 100 Saccos across Kenya.

The goal was simple: identify the milestones made by Saccos specifically in the four (4) critical areas namely,

- IT Governance
- IT Security
- Outsourcing and Vendor Security
- Business Continuity
IT Governance

For the vast majority of Saccos, IT is a core enabler of the business with most, if not all, of the critical business functions supported by IT. As such, it is important that the IT strategy is comprehensive and aligned with the overall business strategy so that it can deliver on objectives to support the current and future strategic direction of the Sacco.

Our research findings indicate that Saccos are increasingly investing more resources in technology and security. However, Majority of Saccos are still unprepared for the Data protection law.

IT Security

IT risk profiles are increasing due to increased mobile banking adoption, growing complexity of IT risk factors, including those driven by the types and numbers of systems used, expanding branch networks, and increased connectivity to external IT networks.

Our research indicates that there is increased targeted attacks on Sacco mobile transaction infrastructure. Additionally, weak IT infrastructure is exposing Saccos to attacks.

Vendor Management

Saccos are required to have adequate governance and risk management processes in place to effectively address the risks associated with outsourcing of IT services, including cloud services.

Our research indicates that Saccos are heavily reliant on vendors for key services and in turn attackers have continuously exploited the loopholes that exist within the vendor management process. There needs to be a shift in relationship model from “Buyer-Seller” to that of a partnership between the Sacco and the vendor.

Business Continuity

Without an incident response plan, business continuity plan, skills and budget to implement, an organisation may not detect a cyber-attack.

Our research indicates that Saccos need to reconsider their Business continuity plans amidst the Covid-19 pandemic to include remote working alternatives.
The Potential of Shared Platforms for Saccos in Kenya

The financial sector is undergoing digital transformation. Equity Bank in Kenya reports that 98% of its transactions are now outside the branch, whilst over 90% of KCBs transactions are digital. Beyond the banking sector over 38 million Kenyans use M-Pesa accounts.

Deposit taking Saccos are responding to the digital finance revolution.

David Cracknell
Director of First Principles Consulting Limited, Nairobi

The Challenges Facing Saccos

Many Saccos struggle to respond to the digital finance challenge, for financial and technical reasons compounded by legacy systems architecture.

a. Financial

To keep up to date and to offer the latest products, Saccos must periodically upgrade their banking platforms and integrate new apps. Many regulated Saccos use systems supplied by local vendors based around ERPs, typically Navision or Microsoft Dynamics. Relatively few Saccos use established, but more expensive, core banking systems such as Banker’s Realm. The choice of system is driven partly by financial considerations – ERP-based systems, whilst more affordable are replaced more frequently than core banking solutions. In addition to the costs of the core platform, the total cost of I.T. operations is even higher due to support costs, service charges, licenses, and the need to integrate additional systems, such as apps.

b. Technical Skills

Procuring, integrating, maintaining systems requires highly skilled staff. Smaller deposit taking Saccos, and especially those based outside Nairobi can struggle to access and finance high quality information technology staff. They are in short supply and there is a competitive employment market for their services.
c. The Pace of Change

The financial sector is evolving more rapidly than at any other time. Payment cards were launched in 1950, ATMs in 1969, real time settlement in 2004, cheque truncation in 2010. By comparison, since 2010 there has been worldwide adoption of mobile money and agent banking, nano credit, merchant services such as Lipa na M-Pesa, and a host of lifestyle services supported by these innovations. Digital finance supports services based on e-commerce, bill payments, foreign exchange, remittances, digital government and more. It’s not easy to be responsive as an institution, but it is extremely easy for customers to shift some of their business to another provider.

d. Compliance

Given the widespread adoption of new technologies, the Sacco regulator has responded by releasing new guidelines on MIS in 2015 and on cybersecurity in 2018. These guidelines are updated as required, and additional guidelines produced. It is not easy for DT-Saccos to comply with these guidelines.

e. Compliance Costs

Lack of compliance can cost more especially when it comes to cybersecurity – with newspaper articles reporting Saccos losing billions of shillings to fraud and theft. Beyond SASRA regulations, national laws are changing in response to the digital revolution including the Data Protection Act 2019. Compliance will become more challenging as more guidelines are issued.

f. Competition

Competition supported by digital finance which in the medium term offers the most threat to Kenya’s Saccos. Competition comes from within the Sacco sector, given that many Saccos have opened their common bond.

Leading Saccos such as Police Sacco, or Unaitas have spent hundreds of millions of shillings on their IT platforms and will be looking to grow through providing new services to new members – partly to leverage the investments they have already made.

Competition comes from banks and microfinance institutions – note that Sacco members paying loans through check off deductions already have bank accounts. Members can choose to move more of their banking services to more agile banks. But in addition, competition comes from mobile money providers or financial technology providers offering instant loans, or invoice discounting.

Introducing Shared Platforms

Shared platforms have their genesis in a fee-based model for software services. An example of this is Office 365, where for a low annual fee a user has a time-based license for Microsoft Office. The user does not have to purchase new software as upgrades are automatic and can use the same license on multiple devices.
The Potential for Shared Services for Saccos

Likewise, banking as a service or BaaS as it is sometimes called, offers financial institutions options to purchase access to a shared core banking platform and/or a range of services. To rent space, rather than to own it. The range of additional services is wide and can cover payments, loans, cybersecurity, clearing, card processing, agency banking, mobile money etc.

Typically, BaaS platforms serve many different institutions, are cloud-based and data is siloed by institution and backed up on a real time basis.

The most common pricing methodology is on per account or per member or per year basis.

Being careful to note definitions here, such as how dormant and/or closed accounts are treated, or multiple accounts held by the same member. Other pricing methodologies include transaction-based pricing, and/or a revenue share for certain services. The total fee will depend upon the range of services that the Sacco is taking up.

Advantages of Shared Platforms for Saccos

a. Perpetual upgrades

Usually the BaaS service provider continually upgrades its solutions and offers the upgraded solution to all clients paying for that service. By comparison, Saccos in Kenya typically upgrade EPR systems on a three to four-year cycle and banking systems on a five to eight-year cycle.

b. Improved Security

A BaaS platform will usually meet international standards but must be configured to meet local regulatory requirements and laws. Indeed, there are separate categories of BaaS, called RegTech and Compliance as a Service. Given that established BaaS platforms need to comply with regulators from multiple jurisdictions, standards around identification, authentication and authorisation are high. However, an additional cybersecurity layer could also be offered from cybersecurity specialists such as Serianu in Kenya.

c. More Predictable and Regular Financing Cost

Given the pricing methodologies outlined, financing becomes a regular cost, monthly, quarterly, or annually, rather than a fixed cost. The core banking module is often priced on a per member per year service, and additional services are priced on revenue shares, fees could even be offset by small annual charges to members, combined with regular service charges. Offsetting these cashflows can have significant liquidity benefits to Saccos.

d. Access to a Range of Additional Services

The BaaS provider can tailor additional services to a local market. For example, offering access to agency banking services across Saccos within its network. This would enable any participating Sacco to offer its members services through other Saccos or their agents in the network. A range of payment services could be provided.

Another example could be digital credit, where the BaaS provider collaborates with a third-party system provider to enable all Saccos on the network to benefit from a digital credit platform. Technically access to the clearing system could be offered through the BaaS platform – though this would require other regulatory hurdles to be met and may require a banking partner.

e. Adopting Shared Platforms

Moving to any new platform is a process which often involves data cleaning and migration, this is time consuming, challenging and can be costly, particularly where full file records are transferred to the new core banking platform.

A final note on outsourcing

Moving to shared platforms implies that a Sacco is outsourcing key functions to third parties. However, outsourcing technology does not outsource responsibility for the application of the technology. Responsibility for outsourcing and its implications remains with the Board of the Sacco. Further guidance from SASRA may be forthcoming.
3. Survey Findings

3.1 Governance within Saccos

3.2 IT Security and Strategy

3.3 Outsourcing and Vendor Security

3.4 Business Continuity
3.1. Governance within Saccos

Sacco boards and management are responsible for setting and overseeing their business strategy and risk appetite and should ensure that IT risk is considered in this context.
Our survey revealed the following.

We asked:

Does your organisation have a cybersecurity strategy or roadmap or plans?

<table>
<thead>
<tr>
<th></th>
<th>2019</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>38%</td>
<td>55%</td>
</tr>
<tr>
<td>No</td>
<td>60%</td>
<td>26%</td>
</tr>
<tr>
<td>In Draft</td>
<td>1%</td>
<td>15%</td>
</tr>
<tr>
<td>Don’t Know</td>
<td>4%</td>
<td>1%</td>
</tr>
</tbody>
</table>

What we learnt:
The percentage of Sacco’s that have a cybersecurity strategy improved from 38% in 2019 to 55% in 2020.

We asked

Have you documented your cybersecurity policies and procedures?

<table>
<thead>
<tr>
<th></th>
<th>2019</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>50%</td>
<td>19%</td>
</tr>
<tr>
<td>In Draft</td>
<td>19%</td>
<td>28%</td>
</tr>
<tr>
<td>Don’t Know</td>
<td>50%</td>
<td>3%</td>
</tr>
</tbody>
</table>

What we learnt:
Policies and procedures are an essential component of any organisation because they address pertinent issues, such as what constitutes acceptable behavior by employees and clearly defines standard operating procedures to ensure continuity.

However, these policies and procedures are rendered useless if employers neglect to adhere to them or fail to effectively communicate them to employees.

Who should write the security policies?
The IT department, often the Security Manager, CIO or CISO, is primarily responsible for all information security policies. However, other stakeholders usually contribute to the policy, depending on their expertise and roles within the organisation.
We asked:
How much do you spend on Cybersecurity?

<table>
<thead>
<tr>
<th>Amount</th>
<th>2020</th>
<th>2019</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-100,000</td>
<td>44%</td>
<td>36%</td>
<td>19%</td>
</tr>
<tr>
<td>100,001-500,000</td>
<td>36%</td>
<td>19%</td>
<td>10%</td>
</tr>
<tr>
<td>500,001-1,000,000</td>
<td>27%</td>
<td>14%</td>
<td>6%</td>
</tr>
<tr>
<td>Above 1,000,000</td>
<td>18%</td>
<td>3%</td>
<td>6%</td>
</tr>
</tbody>
</table>

What we learnt:
There has been a consistent increase in Cybersecurity budget in the Sacco industry over the last 3 years and this can be attributed to:
- Increased awareness on the importance of Cybersecurity.
- Increased attacks targeted towards Saccos.
- Digitization and adoption of new technology channels.

We asked:
Does your board of governors regularly discuss Cybersecurity/IT issues?

<table>
<thead>
<tr>
<th>Frequency</th>
<th>2020</th>
<th>2019</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, Monthly</td>
<td>22%</td>
<td>7%</td>
<td>26%</td>
</tr>
<tr>
<td>Yes, Quarterly</td>
<td>18%</td>
<td>22%</td>
<td>26%</td>
</tr>
<tr>
<td>Yes, Annually</td>
<td>5%</td>
<td>5%</td>
<td>18%</td>
</tr>
<tr>
<td>Ad-hoc</td>
<td>18%</td>
<td>22%</td>
<td>26%</td>
</tr>
<tr>
<td>Never</td>
<td>3%</td>
<td>7%</td>
<td>22%</td>
</tr>
</tbody>
</table>

What we learnt:
Board buy-in is an important requirement for any successful internal initiative, including Cybersecurity. The board agenda has been crowded since the start of the pandemic, and many issues have acquired new urgency including continuity of operations, adoption of new working models and compliance with regulators.
3.1.1. Cyber Governance: What Every Director Needs to Know

Many Saccos struggle with five fundamental challenges to cybersecurity governance:

1. **Cybersecurity Strategy and Goals**: How to set direction and prioritize cybersecurity initiatives across the organisation.
2. **Enforcement and Accountability**: How to identify and mitigate cybersecurity risks across the organisations in a measurable and accountable manner across all personnel levels.
3. **Budget and Acquisition**: How to manage investments in strategic cybersecurity priorities as part of budget and acquisition processes across the organisations.
4. **Continuity and Incident Response**: How to prepare for and respond to cyber incidents that require coordinated action with different stakeholders.
5. **Information Sharing**: How to engage across multiple organisations to share cybersecurity-related information without compromising organisation’s reputation?

Here are some basic guidelines Sacco directors should consider to help inform their cybersecurity governance framework:

- To establish a good cybersecurity governance program, the Sacco Board must clearly define its risk management policies, strategy, and goals. The board MUST also determine:
  1. What are the greatest threats and risks to the Sacco’s highest-value cyber assets? Is the Sacco’s human and financial capital set up to in a way protect those high-value assets?
  2. What is the Sacco’s volume of cyber incidents on a weekly or monthly basis? What is the magnitude/severity of those incidents? What is the time taken and cost to respond to those incidents?
  3. What would the worst-case cyber incident cost the company in terms of lost business (because of downtime of systems that were attacked and need to be brought back and because of the harm to the Company’s reputation as a result of the attack)?
  4. What part of the Board should handle examination of cyber security risks? Should it be the whole Board? Should this responsibility be assigned to the Audit & Risk Committee?
  5. How often should the Board (or Committee) be receiving cyber security briefings?
  6. Finally, should the Company consider adopting, in whole or in part, the Cyber Risk Quantification framework as a way or method of showing affirmative action to protect the Sacco’s assets?
It is Time for Saccos to Embrace Digitization

Emerging technologies and digitization have transformed the business landscape and forever changed our ways of working.

There are over 22,000 registered cooperative societies in Kenya out of which about 13,000 are Savings and Credit Cooperative Societies (Saccos) that play a critical role in every sector of the community, especially as a great vehicle for mobilizing savings and facilitating investment. 175 are deposit-taking and therefore regulated by the Sacco Societies Regulatory Authority (SASRA).

The Fourth Industrial Revolutions (4IR) is built on the foundations of Third revolution and combines emerging technologies like Internet of Things (IoT), Robotics, Artificial Intelligence and Blockchain among others. Whereas many financial services players have invested heavily in digitization and deployed secure core banking systems (CBS) with seamless integrations to front-end technologies, omni-channels, cloud, and other emerging technologies, Saccos continue to rely on customized ERPs for their banking needs. As an entry level intervention, this setup was sufficient in yesteryears, but is no longer adequate for the digitization era.

ERPs are not inherently developed with integration in mind since they are intended to be “all-ensuite”. They are built for enterprise internal functions like financial management, payroll, HR, procurement etc and not for core banking functions. When used to perform Sacco or banking functions including integration to channels, many things could and have gone wrong including: latencies where response time for transactions is delayed; introduction of a single point of failure especially when running batch jobs; integration and security vulnerabilities; among others.

Saccos continue to rely on customized ERPs for their banking needs.

Wambui Mbesa  
Chief Executive Officer, INTRASOFT  
International East Africa
Customer demand has been increasingly shifting for the last decade but has recently been accelerated by the Covid-19 Pandemic. Today they are accustomed to doing things online. In the same way, and partly due to government regulation (e.g. social distancing, handling money), people are increasingly hesitant to visit banking halls, having been pushed by prevailing circumstances to adopt a digital-first mindset.

Saccos members are no exception. The financial services sector is not yet a level playing ground and Saccos need to increase their uptake of technology for their survival and growth.

In my view, since core banking systems are capital intensive, they have the option of adopting microservice architectures because these make applications easier to scale and faster to develop thus enabling innovation. For Saccos to optimize their potential in this digital era, they need to deploy Core Banking Services (CBSs) inherently built to serve their core business.

A CBS is built for faster processing of transactions such as instant loans and appraisals, onboarding via channels, smooth bulk processing of batch jobs such as check off and dividends all during work hours without impacting operations.

Other digitized processes include loan scoring, seamless top-ups, automated interest management, loan restructuring, repayment and loan recovery using sniffing functionality. Without a proper CBS that removes many of the manual processes, Saccos face Credit, Liquidity and Operational risks as they may issue loans to borrowers who are not creditworthy and make disbursements that exceed deposits. All these can be detected and managed through digitization. Security is at the core of CBSs which run on more secure platforms and enable integrations that are secure and less exposed, leading to better confidence from stakeholders in the sector including regulatory spheres.

In recent years, digitization has become a high priority conversation among Sacco ICT Managers, CEOs and their Boards. Some already have a Digital Strategy and a well-defined roadmap for actualization. However, many are moving slowly, adopting only mobile banking, yet mobile banking and digital payments are only a part of digitization and their adoption without strategy may be even more “dangerous” if the holistic fundamentals of a successful digitization strategy and process are not undertaken.

The key pillars of a successful Sacco digital transformation include infusing a revolutionary digital mindset into the traditional Sacco culture, replacing old technological infrastructure, empowering decision makers and improving processes by introducing speed and policies that support the change.

It is time for Saccos to embrace digitization with intentionality. They should begin with a digital strategy and a well-defined roadmap for actualization, source the services of experts in order to navigate this process and enable a rapid digital recruitment and onboarding process. They need to automate digital lending decisions, digitize all lending and recovery processes to entice millennials and the next generation of members.
3.2. IT Security and Strategy

IT risk profiles are increasing due to increased automation, growing complexity of IT risk factors, including those driven by the types and numbers of systems used, expanding branch networks, and increased connectivity to external IT networks.
Our survey revealed the following:

**We asked:**
Do you have a dedicated internal/external resource for managing Cybersecurity?

- Yes: 58%
- No: 35%
- Don't know: 7%

**We asked:**
How do you manage Cybersecurity?

- In-house: 47%
- Outsourced: 39%
- Both: 8%
- None: 6%

**What we learnt:**

The key pain point areas for Sacco Security Managers include:

1. **Rapidly Growing (and Evolving) Technical Landscape:** Internet-connected devices that have been developed without proper security measures in place.

2. **Scope of Work is Too Broad:** Having a scope of work that's too broad can result in under-staffing and segregation of duty breach and fraud.

3. **Competing Operational Priorities:** Operational needs often prioritize speed and information sharing over information security and this can result in poorly architecture networks.
4. **Inconsistent Cyber Hygiene:** Particularly stand-alone technologies that are being digitized and integrated with other systems, creating interoperability dependencies, network segmentation risks, and other cybersecurity challenges.

5. **Budgetary Constraints:** Organisations are spending a vast majority of limited IT budgets on acquisition, implementation, and adoption of technical solutions with few resources left to secure and maintain their networks capabilities or conduct activities ad hoc without having anyone internal who is accountable for security nation-states alike.

---

**We asked:**

Do you conduct Cybersecurity training for your employees, executives and Board?

- **Never:** 11%
- **Ad-hoc:** 18%
- **Quarterly:** 28%
- **Annual:** 28%
- **Semi-annual:** 15%

**What we learnt:**

89% conduct training either annually, semi-annually, quarterly or whenever needed.

---

**We asked:**

Do you conduct regular IT and Cybersecurity audits?

- **Never:** 21%
- **Ad-hoc:** 17%
- **Quarterly:** 8%
- **Annual:** 48%
- **Semi-annual:** 6%

**What we learnt:**

The biggest challenge when remediating audit gap is inadequate budget and funds.
We asked:
What’s your biggest challenge in remediation of audit gaps?

- 50% Inadequate budget to remediate
- 39% Limited Technical Skills
- 21% Too many gaps to be remediated

What we learnt:
The biggest challenge when remediating audit gap is inadequate budget and funds.
Cloud Computing as a Catalyst for the Growth of Saccos and Other Cooperatives

From machine learning and artificial intelligence (ML/AI), blockchain, the Internet of Things (IoT) to Cloud Computing, the application of these technologies have sought to more evenly distribute development.

The imminent Fourth Industrial Revolution (4IR) presents an opportunity for the third world to leapfrog traditional development models by taking advantage of advanced technologies that, compared to those of previous industrial revolutions, are cheaper and more available to the masses.

The result is more organisations domiciled in the third world are quickly able to start up and become competitive on a global scale.

On the African continent, hubs such as Nairobi, Lagos, Johannesburg and Cairo continue to take advantage of these technologies to churn out globally competitive startups that solve real life problems. Further down the value chain, industries such as financial services, agriculture and education are impacted as a whole by new service offerings available to them through these new technologies. This has made many organisations prioritise technology as a key enabler for their growth.

The financial sector is arguably the sector that has benefited the most from the technological revolution across the globe. In 20 years, many financial institutions have moved from fully manual organisations, to being almost fully dependent on technology for their operations.

The traditional banking and insurance companies have been the largest beneficiaries, as their processes do not greatly differ worldwide. Alternative providers of financial services such as Savings and Credit Cooperatives (Saccos) and other cooperatives, have more unique processes and as a result have lagged behind.

Incumbent technology providers have tried and failed to copy and apply solutions made for the traditional banking model to this market. They failed to understand the unique structures and challenges these member-owned organisations face, and would provide expensive, insecure solutions that provided almost no value to the organisations resulting in massive sunk costs and other financial losses through fraud and hacking.

“Many organisations prioritise technology as a key enabler for their growth.

Cynthia Wandia
Co-founder and CEO of Kwara
Saccos and other cooperatives stand to benefit the most from the adoption of cloud computing technology that not only provides a more cost effective solution for digitisation, but provides more secure platforms for managing data and transacting.

In the context of the Fourth Industrial Revolution, cloud computing provides the rails on which Saccos and other cooperatives can launch their end-to-end digitisation agenda relatively inexpensively. Saccos and other cooperatives can save up to 45% in lower infrastructure and storage costs, reduce time to market by up to 36%, achieve up to 53% in improved efficiencies and have up to 73% better security through the adoption of cloud based core solutions.

This illustrates the importance of cloud computing as a catalyst for growth and efficiency for Saccos that aim to be market leaders.

As a sector with more than KES. IT in assets, the importance of the Sacco sector in Kenya cannot be muted.

The efficiency, security and the ability to collaborate using cloud technology provides an unbeatable value proposition to springboard Saccos from being 8 to 5 organisations to becoming new age digital financial institutions that serve members 24/7.

Regulatory compliance is another major driving force for the digitisation of Saccos and the adoption of cloud technologies. The recent decree by Kenya’s Saccos Societies Regulatory Authority (SASRA) for all non-deposit taking Saccos to comply with regulatory reporting standards to gain certification, has further helped to increase momentum for the uptake of digital solutions for Saccos. Cloud-based core solutions provide the best bet for these SaccoS to digitise and transform their reporting in the shortest possible time.

In an increasingly digital world, it is incumbent on all stakeholders to ensure that these members’ assets are protected and continue to provide returns in the long term by ensuring that transformation through digitisation is achieved in the most efficient and secure manner.
3.3. Outsourcing and Vendor Security

Saccos are required to have adequate governance and risk management processes in place to effectively address the risks associated with outsourcing of IT services, including cloud services.
Our survey revealed the following:

**We asked:**

*Do you conduct due diligence on vendors before you engage them?*

- **22%** No
- **58%** Only major vendors
- **20%** Yes – all vendors

**Important to note:**

**Vendor due diligence checklist for Saccos**

The contents of a Vendor due diligence assessment will often vary due to the nature of the target company being audited; however, the contents of the due diligence report will largely remain similar across most industries.

The main information to include in the assessment and report include:

1. **Financial Review:** A complete review of the vendor’s historical and current financial information.
2. **Operational Risk:** This encompasses organisation structure, liquidity, and a growth analysis.
3. **Cybersecurity Risk:** This encompasses the vendor’s capability to minimize security breach to your Sacco.
4. **Reputation:** References from past clients will give great insights into the vendors’ reputation.

**We asked:**

*Do you maintain contracts with all your vendors?*

- **11%** No
- **27%** Only major vendors
- **62%** Yes – all vendors

**Important to note:**

Without proper contracts, a Sacco cannot measure performance and hold its vendors responsible for service delivery.
**We asked:**
Do you regularly audit your vendors?

- **52%** No
- **18%** Yes – all vendors
- **30%** Only major vendors

**What we learnt:**
More than half of the respondents i.e. 52% do not audit their vendors.

---

**We asked:**
Have you implemented monitoring and alerting for vendor activities in your network?

- **16%** Only if there is a problem
- **42%** No
- **42%** Yes

**What we learnt:**
42% have no monitoring and alerting activities in place.
Balancing the delicate symbiotic relationship with vendors

The field of technology is wide and it is ever growing, so are the control and by extension the information security space.

"Third parties have been found to have exposed organisations through myriad of risks."

How does an organisation balance the delicate symbiotic relationship with the vendors?

1. **Governance**

For scalability, efficiency, shorter time to detect, discover, respond and recover, organisations resort to collaborate with institutions that have a narrower and deeper focus on a specific niche of service delivery as opposed to building capabilities internally.

This model gives organisations shorter return on security investment, ensures quality products or services from the start, shorter time to deliver results, leverage in mature and refined products/services and abstracts the organisation from the hiring process and its related internal social complexities in a highly technical field.

That said, third parties have been found to have exposed organisations through myriad of risks and in some cases, found complicit or used as conduit to execute a cyber-heist. Occasionally, vendors have pushed for services or products, which are not aligned with an organisation’s cybersecurity strategy and digital strategy.

2. **Contracting**

The organisation ought take its time and define to the granite atomic detail - the scope, deliverables and milestones in the contract, this ensures the terms of engagement are explicitly and there are no grey areas.

3. **Key Performance Indicators and service level agreements**

During contracting or after, it is very vital for the organisation and 3rd party vendor to define Key Performance Indicators (As measures By metrics) and sign off a binding service levels agreement. These documents provides a base for performance measurement and a metricized services level expectation from the vendor. Contract extension and renewal with the vendor becomes a very objective conversation and expectation on both ends well managed.

---

Amos Ndung’u
Information Security Manager, Harambee Sacco
4. Vendor Security Questionnaire

These are a series of the questions developed by the organisation to gauge vendor’s security and privacy posture. Depending on the responses, and risk of a particular item, the organisation can request to verify through a site visit or proof of implementation of a certain control.

5. Certification & Accreditation, Past Systems Audit

It is important for the organisation to request and verify cyber security certifications and accreditations acquired by the 3rd party vendor e.g. ISO 27001, verified PCI DSS SAQ, OWASP etc. The organisation can go further and scrutinize at least 3 independent system Audit reports to check the cybersecurity issues exposed and whether they have been satisfactorily closed.


For every service or product to be consumed, the organisation ought to state and verify the bare or based security expectation. This shields the organisation from glaring risks exposure as a result of consuming an immature product or one which has not been properly hardened.

7. Vulnerability Assessment and Penetration Testing

Depending on the product/service to be consumed, it is vital for the organisation to carry out its own independent vulnerability assessment and penetration testing.
3.4. Business Continuity

Without a proper response plan, adequate skills and budget, an organisation cannot fully respond to IT and security incidents.
Our survey revealed the following:

**We asked:**
*Do you have a business continuity plan in place?*

- 22% No
- 60% Yes - Approved
- 18% Yes - in draft stage

**What we learnt:**
Most of the respondents have a business continuity plan either implemented or in draft process. 78%

**Important to note:**
*Building Your Budget*

BCM is often not treated in a straightforward manner in organisation’s budgeting process, either it will get a budget in one year and will be left out the following year, or money budgeted for BCM will be raided with little warning and used for something else.

So how do you build your BCM program budget?

You start by figuring out your requirements. Including any external or internal audits, your Business Impact Analysis (BIA) and any threat or risk assessments that have been made of the organisation.
**We asked:**

Does the board regularly discuss the sacco’s business continuity management plans?

- **8%** I don’t know
- **22%** Ad-hoc
- **53%** Yes
- **17%** No

**What we learnt:**

Most of the respondent i.e. 75% agree that their board discusses the Sacco’s business continuity management plans. 

---

**We asked:**

Has the organisation implemented disaster recovery infrastructure?

- **35%** Yes
- **12%** No
- **51%** Not extensively
- **2%** I don’t know

**What we learnt:**

51% of the respondents have not extensively implemented a disaster recovery infrastructure. Only 35% of the respondents have implemented a disaster recovery infrastructure.
**We asked:**
What was the impact of Covid-19 to you and your organisation?

- 20% Cyber attack attempts
- 30% Forced leave
- 30% Employment Termination
- 20% Other

**What we learnt:**
Cyber attempts, forced leave and employment termination were among the top effects experienced by employees during the Covid-19 Pandemic period.

---

**We asked:**
Does your organisation train staff members on the business continuity plans?

- 43% Not extensively
- 33% Yes
- 24% No

**What we learnt:**
Only 33% of the respondents train their organisation on business continuity plans.
We asked:
Which of the following would you rate as the challenges most experienced when implementing the BCP process? (A scale of 1 to 5)

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of financial resources</td>
<td>5</td>
</tr>
<tr>
<td>Lack of proper training</td>
<td>4</td>
</tr>
<tr>
<td>Lack of senior management support</td>
<td>4</td>
</tr>
<tr>
<td>Lack of human resources</td>
<td>3</td>
</tr>
<tr>
<td>Identification of right stakeholders</td>
<td>3</td>
</tr>
</tbody>
</table>

What we learnt:
Lack of financial resources was the highest rated challenge in terms of when implementing the BCP Process, followed by lack of proper training and lack of support from the management.
Resilience and the New Reality

As the pace of change in information technology accelerates, business continuity management (BCM) needs continue to evolve rapidly within organisations, including Saccos, to meet increased market and regulatory demands.

In the current environment, in which businesses of all sizes and types are being tested in unprecedented ways by the coronavirus (COVID-19) pandemic, business continuity and resilience has become a critical discussion in boardrooms and with key business leaders, including, Chief Executive Officers, Chief Information Officers, Chief Risk officers etc. around the world. The pandemic’s widespread impact has forced organisations to revisit business continuity planning (BCP) and how to embed BCP practices in day-to-day operations.

The goal of business continuity planning (BCP) is to prepare financial institutions and other industry organisations to respond quickly and decisively in an emergency to ensure employee safety and resume business operations with minimal amount of disruption. It is aimed at ensuring that critical business services such as FOSA, BOSA etc. are delivered continuously to customers even in the midst of a disaster.

Our recent survey on business continuity for Saccos, revealed that 40% of Saccos do not have an approved business continuity plan while only 35% have an existing disaster recovery infrastructure.

This begs the question, are organisations really ready to resume business operations during a pandemic or any other disruption?

In the wake of the pandemic’s spike in new cases and deaths in Kenya, it is possible that these new infection rates will necessitate sporadic county lockdowns and that these might be ongoing and unpredictable.

With future implications of COVID-19 still unclear, some questions to consider for the long-term operating model of many businesses include:

- Do we anticipate organisations will go back to their old ways of working once the spike goes down?
- How do we proactively manage the impact of the pandemic to the business operations?
- Will management require employees (after all, employees are an organisation’s greatest asset) to work from home or have a split workforce to limit interactions for an extended period even after the crisis has subsided?
- Will organisations still continue to leverage secure technologies and capabilities built to support work-from-home efforts in the delivery of key products and services?
for new business continuity and disaster recovery strategies. For this to actualize, organisations need to:

- Identify the third-party dependencies for critical services and ensure no loopholes exist e.g., are there alternative service providers or workarounds for the services offered? Are the current communication channels with the third-party service providers smooth and coordinated?

- Ensure that adequate controls have been put in place to facilitate the new work-from-home reality. There is increased exposure of sensitive data as result of using VPNs, Cloud Services etc.

- Ensure that adequate resilience needs are available to support the technological infrastructure supporting key business operations i.e., how quickly a system is expected to recover (RTO) and the maximum amount of data that can be lost (RPO) should be met;

- Finally, ensure that the plans and strategies are stress tested against emerging and evolving cyber-security threats and any other unforeseen scenarios such as the pandemic. Data Protection Law will impact your Sacco.
4. Cyber Intelligence

Mobile Money Ecosystem - Security Concerns

**Threat Vector**

- **Organisation**
  - Database compromise
  - Transaction manipulation
  - Customer data manipulation
- **Integrator**
  - API compromise
  - Transaction manipulation
- **Telco**
  - GSM compromise
  - API compromise
  - Transaction manipulation

**Controls**

- Database audit
- Application audit
- Data integrity checks
- Data encryption checks
- Contracts/Liability review

- API assessment
- Network/Application audit
- Data integrity checks
- Data encryption checks
- Transaction monitoring

**Data Protection - Mobile Money Ecosystem**

- Carry-out Internal Risk Assessment
- Seek Explicit Consent of the Data Subjects
- Document Policies for Data Protection
- Appoint a Data Protection Officer

**Data Protection**

- Appoint a Data Protection Officer
- Seek Explicit Consent of the Data Subjects
- Document Policies for Data Protection
- Carry-out Internal Risk Assessment

**Controls**

- Database audit
- Application audit
- Data integrity checks
- Data encryption checks
- Contracts/Liability review

- API assessment
- Network/Application audit
- Data integrity checks
- Data encryption checks
- Transaction monitoring
The Top 10 Indicators of a Cyber Attack

What should Saccos be worried about?

With the rise and complexity of cyber-attacks, organisations often feel helpless and handicapped against cyber criminals, whose techniques and tactics always seem to outmatch the organisation’s defenses.

Weaknesses in the technologies, people and processes, coupled with the lack of adequate cybersecurity controls, has made it possible for cyber criminals to continuously compromise enterprise networks and systems.

The efforts to win the war against cyber criminals starts with organisations understanding the risks they are exposed to, vulnerabilities existent within their environments and the eminent cyber threats they face. Let us use an analogy to better understand these terms.

In an unfortunate incident where someone is about to punch you in the face, the Risk is the potential of you being punched in the face, the Vulnerability is your inability to defend yourself against the punch and the Threat is the punch being thrown at you. The sign(s) that someone is about to punch you in the face is the Threat indicator.

Successful cybersecurity programs are therefore those that are modelled around the understanding of an organisation’s risks, vulnerabilities, threats and ultimately its threat indicators. Such threat indicators are the inputs of successful enterprise cybersecurity operations programs.

Outlined below, are the Top Ten indicators that every Sacco should focus on:

1. Presence of Rogue Device and Software

Rogue devices and software are those that exist within a network for malicious intent. The presence of such devices and software point to a gap in an organisation’s asset management program, and therefore the need to implement automated processes that manage devices and software within the network. Such automated processes can be achieved through technologies such as Network Access Control (NAC) solutions that manage authorized devices connected to the enterprise network.

2. Presence of End-Point, Network and Email level Malware

Malware (Malicious Software) is one of the most predominant threats facing organisations and prevalent in majority of local cyber-attacks, with attackers often introducing such malware at the endpoints, network and email. The lack of automated processes in place to detect such malware makes it easy for attackers to compromise targeted systems leading to loss of service, data and money.

Organisations should invest in technologies such as Antivirus, Firewalls and Email Security Gateways to enable timely detection and prevention of malware propagation at these levels.
3. Communication Protocol Misuse

Common communication protocols such as DNS (Domain Name Service) are often misused by attackers to sneak malicious traffic past organisations’ defenses. For example, by using malicious domains and DNS servers, an attacker can use DNS to evade network defenses and perform data exfiltration.

Since most DNS tunneling tools rely on the fact that DNS is often not monitored, organisations should deploy both payload and traffic analysis detection techniques. Payload analysis focuses on tunnel indicators from the DNS requests and responses, whereas in traffic analysis the traffic is analyzed over time taking into consideration such attributes as the count, frequency and other request attributes.

4. Malicious services and registry modifications

Malicious services and registry modifications are among the common techniques used by attackers upon successful target compromise. The detection of these post-exploitation techniques greatly determines the success or failure of a cyber-attack. Technologies such as enterprise detection and response (EDR) tools help organisations to automate both their detection and responses processes and therefore reducing attack response times.

5. Presence of Network and endpoint level Vulnerabilities

During the reconnaissance and threat assessment phases, attackers take time to understand their targets and the existing weaknesses. Such weaknesses on devices, software and/or configurations, commonly known as vulnerabilities, are the attackers’ entry point to an organisation’s network. Organisations should implement vulnerability management programs to ensure timely detection and closure of identified vulnerabilities.
6. **Unauthorized Device Configuration Changes – Network, Linux/Windows**

Unauthorized changes in an organisation’s devices pose a major risk to the business. For instance, an unauthorized configuration change to a router’s routing table would adversely impact the availability of external facing systems.

Technology solutions with File Integrity Monitoring (FIM) capabilities would help organisations detect such unauthorized changes and therefore reducing such risk exposures.

7. **Unauthorized Database Object and Files’ Modification**

Databases are the crown jewels of any organisations. Unauthorized modifications of records within these databases greatly impact the confidentiality and integrity of such records, a common attack vector used to commit fraud.

Organisations need therefore to implement Database Activity Monitoring (DAM) solutions to monitor for unauthorized modifications, in an effort to prevent fraud.

8. **Unauthorized User Accounts Modifications**

A common denominator of most attacks is characterized by cyber criminals modifying privileged user accounts and using them to access critical systems. Such activities, if undetected, allow attackers to spend months within such compromised hosts.

Privilege Access Management (PAM) solutions greatly help organisations to automate the management of privileged accounts, whereas anomaly detection in user activity can be automated through technologies with User Behavioral Analytics (UBA) capabilities.

9. **Critical Systems User Access**

A critical system is one whose compromise would lead to significant loss to the business. Such systems include but not limited to transaction systems, databases, firewalls and domain controllers. Since such systems are the common targets by malicious actors, uncontrolled privileged users’ access pose a significant risk to them.

Proper user access management and monitoring processes should therefore be implemented to help reduce the risk exposure against such critical systems.

10. **Social Engineering Attacks**

People often represent the weakest link in the security chain. As such, cyber criminals often target the users through social engineering techniques such as phishing.

Here, the target users receive an email requiring them to either download a file or click on a link that redirects them to a phishing portal. Through such phishing emails, users are made to share confidential data such as passwords.

Organisations therefore need automated programs in place that measure their risk exposure through such social engineering attacks. This can be done through scenarios’ simulations coupled with periodic user awareness training programs.
5. Data Protection Law will impact your Sacco

The Data Protection Act, 2019 provides a legal framework on personal data usage, especially on digital platforms. The data protection law brings about several changes in the business environment.
**Who Is affected?**

Any entity that is in direct control of another person’s data.

**What is covered?**

The law sets out several requirements that must be put in place when handling another’s personal data and this includes processing and profiling. The data must be handled lawfully, accurately and the data subject’s consent must be given before it is shared with third parties.

---

**What this means for Saccos:**

- **Onboarding members (KYC):** Saccos must ensure they get formal consent prior to collecting KYC.
- **Transfer of member data to 3rd parties:** A Sacco must seek consent from member before transferring their personal data to other 3rd parties.
- **Automated Loan Processing:** A Sacco that conducts automated loan processing must provide meaningful information about the logic involved to its members.
- **Marketing to Members:** A Sacco must ensure that a member has given consent prior to sharing marketing materials.
- **Member’s rights to move their data to another Sacco:** A Sacco member legally allowed to request a Sacco to share his/her data with another Sacco.
- **Internal Assessment:** A Sacco is required to conduct impact assessments (pursuant to section 31 (1) of the Act and section 41 of General Regulations).
- **Incident Notification:** Sacco is expected to report data breaches affecting its member’s personal data to the Data commissioner within reasonable timelines.
- **Expertise:** Depending on the size of the Sacco and the volume of personal data handled, a Sacco may be required to have an in-house Data Protection Officer.

*Penalties for non-compliance can result in fines of up to 5 Million shillings or 10 years in prison.*
Is your Sacco a Data Controller or a Data Processor?

**Data Controller**
- Any legal person or organisation that
  - Defines WHAT data that is to be collected.
  - Defines WHY the data is being collected (Purpose).
  - Determines HOW the data will be processed.

**Data Processor**
- Any legal person or organisation that
  - Processes personal data on behalf of the data controller including:
    - Collection, recording, organisation, structuring;
    - storage, adaptation or alteration;
    - retrieval, consultation or use;
    - disclosure by transmission, dissemination;
    - alignment or combination,
    - restriction, erasure or destruction.

---

Principles of Privacy

1. Lawfulness, Fairness & Transparency
2. Purpose Limitation
3. Data Minimization
4. Accuracy
5. Storage Limitation
6. Security
7. Accountability

---

Partnering for success
Rights of the Sacco Members (Data Subjects)

- **Right to Information:** of the use to which their personal data is to be put.
- **Right to Be Informed:** of false or misleading data about them.
- **Right to Access:** their personal data in custody of data controller or data processor.
- **Right to Correction:** of false or misleading data.
- **Right to Deletion:** to the processing of all or part of their personal data.
- **Right to Object:**

Steps your Sacco can take to start the Data Protection Compliance Journey

- **01 Awareness:**
  Understand the requirements of the Law (Awareness for Board, Managers, Staff and Members)

- **02 Current State Assessment:**
  Data Protection Process Compliance Review

- **03 Remediation of Gaps:**
  People, Policy, Process and technology.
  **People:** Training and appointment of a Data Protection Officer.
  **Policy:** Documentation of data protection policy & procedures.
  **Process:** Data Protection Impact Assessment
  **Technology:** Deployment of security technologies for data confidentiality, integrity, authenticity and non-repudiation.

- **04 Controls Implementation**
  **Sacco Member Consent:** Validation of customer’s consent
  **Sacco Registration:** Registration with the Data Protection Authority
  **Breach Notification:** Data breach identification and notification within 72 hours
  **Data Protection Authority:** Continuous engagement with Data protection authority office.
What are the Legal provisions for collecting and processing data

A sacco can collect, store, transfer and adapt members data under the following conditions:

1. Consent
   - The Sacco member has given consent to the Sacco to process their data.

2. Performance of Contract
   - The processing is necessary for the performance of contract between the data subject and the controller.

3. Public Interest
   - For any matter of public interest.

4. Legal Claim
   - For the establishment, exercise or defence of a legal claim.

5. Vital interests
   - In order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

6. Legitimate interest
   - For the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.

---

What are The Legal Provisions for Collecting and Processing Data

A sacco can collect, store, transfer and adapt members data under the following conditions:

<table>
<thead>
<tr>
<th>Processing Operation</th>
<th>Personal Data Processed</th>
<th>Processing Purpose</th>
<th>Data Subject</th>
<th>Processing Means</th>
<th>Recipients of the Data</th>
<th>Legal Basis for Processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees Payroll</td>
<td>Last &amp; first name, address, telephone number, KRA PIN, salary information</td>
<td>Payroll management</td>
<td>Employees</td>
<td>Human Resources IT System</td>
<td>External: Financial Institutions &amp; Social Insurance Schemes</td>
<td>Employment contract</td>
</tr>
</tbody>
</table>
6. Priorities for 2020/2021
Compliance with Data Protection
(Fines up to 5 million Kenyan shillings)

Security of Transaction Integration Systems
(Loses up to 10 Million Kenyan shillings)

Awareness and Training
(For general employees, IT, Board and members)

Continuous Vendor Assessment & Monitoring
(Over 30% of attacks involve vendors)

Resilience and Defense in Depth
(Zero trust network architecture)
7. County Cyber Extension Officer Program

The County Cybersecurity Extension Officer Program is a unique offering (modelled around the agriculture extension officer program) where cyber security professionals provide ongoing consulting services to organisations that lack sufficient budget to sustain in-house cybersecurity consultants.
This program allows organisations to utilize the skills and expertise of Serianu’s Cybersecurity extension officers and systems without necessarily hiring in-house teams.

According to the 2018 Africa Cybersecurity Research report, Cybersecurity skills gap in Kenya is at an all-time high.

Kenya has approximately 1700 Skilled Cybersecurity professionals serving over 40 million Kenyans. Organisations are struggling to find the right experts to assist in Anticipating, Detecting, Responding and Containing Cybersecurity issues within their organisations.

In a bid to assist organisations, county governments, Saccos, MFIs and SMEs curb the skills gap shortage and reduce instances of Cybercrime and Cybersecurity related incidents, Serianu has launched the County Cybersecurity Extension Officer Program.
How it works

Serianu’s Cybersecurity extension officers are deployed to various counties within Kenya. These officers offer organisations (and their branches) top-notch Cybersecurity services and consultancy on a bi-weekly basis.

As opposed to the conventional one-off consulting service, this program allows an organisation to interact with our experts on a continuous basis to ensure that the overall cybersecurity posture of an organisation improves.

Target

- Organisations with branches outside Nairobi
- County Governments
- Saccos
- Microfinance Institutions
- Co-operatives
- Other SMEs

Key Activities

- IT / Cybersecurity Strategy Review
- Disaster Recovery Review
- Business Continuity Review
- Remediation of Audit findings
- Security Awareness Training

Benefits

Regular check-up on cybersecurity posture

- Review your organisation’s Cybersecurity posture with industry experts
- Review your compliance and regulatory compliance posture
- Suggest measures to improve IT related procedures, operations and processes.

Technical expertise

- Improve the technical skills and capabilities of your organisation/branch by utilizing Serianu’s Cyber Security extension officers.
- Revise and analyze IT operations and systems, hardware configurations, physical security and operating procedures across organisation.
- Consult and comply with set controls, standards, policies and procedures while carrying out IT activities.
- Suggest and execute IT technologies, strategies and policies to guard information assets.
- Recommend solutions for explaining risks and reducing exposure areas.
A facilitator conducting a Sacco Data Protection Training in Naivasha.

Group photo of participants during a Sacco Data Protection Training in Naivasha.

Pwani University Training session hosted by Imarika Sacco and Serianu Ltd in Kilifi.

Group photo of participants during a Sacco Data Protection Training in Naivasha.

A group photo of the Imarika Sacco Team with the Serianu CEO (extreme right) during a Youth Empowerment Training in Kilifi.

Serianu CEO giving a participant a certificate during the Coast Region High School Awards hosted by Imarika Sacco in Kilifi.

A Community and Youth Empowerment Training with Tai Sacco in Githunguri.

A group photo of participants during a Sacco Data Protection Training in Naivasha.
8.

References

1. CVEQ Manuals: www.serianu.com
2. Sacco guidelines: https://www.sasra.go.ke/
For more information, contact;

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

General Information
+254 (0) 20 200 6600

Cyber Crime Hotline
+254 (0) 800 22 1377

Email: info@serianu.com

https://www.serianu.com