File ref: 17/7/4/1/3

Annexure A

Concept Paper
On
Cyber Security

Prepared by: ICT Steering Committee

Date: August 2017

Table of Contents

1. Purpose

The purpose of this document is to provide background information on cyber security by detailing the most prevalent types of cyber activities that constitute cybercrime in most jurisdictions. The paper also serves to present a proposal for a cyber security framework that regional central banks could adopt and implement, based on the G7 Cyber Security Principles, to combat cybercrime and ensure cyber resilience across the region.

2. Executive Summary

Cyber security is the process through which information and communication systems are protected against damage, unauthorised use, modification or exploitation. Cyber threats present a set of pressing operational, reputational and financial stability risks to the global financial system. Sovereign borders do not contain these threats, and accordingly, nations must work together to address them. Complex regulatory requirements established over the years have only served to attract greater cyber threats and heightened concerns for data security and privacy across virtual borders. Security against threats can be achieved by implementing appropriate technology, policies and best practices. A holistic risk-based approach is therefore required for the mitigation of cyber risks. This concept paper defines cyber security in the context of central banking, outlining major and most prevalent types of cyber-attacks as well as key focus areas where mitigation measures could be implemented to combat cybercrime. The paper concludes by making a recommendation on a Cyber Security Framework that could be adopted and implemented by all member central banks to ensure cyber resilience across the region. The development of the regional Cyber Security Framework by Cyberm would amount to USD $107 000.00 for all central banks. For compliance with the recommended framework and ease of monitoring, Cyberm recommends using ComplianceMapperTM tool, whose annual licence would amount to $12 485.00 per bank if a minimum of 8 banks sign up.

3. What is Cyber Crime?

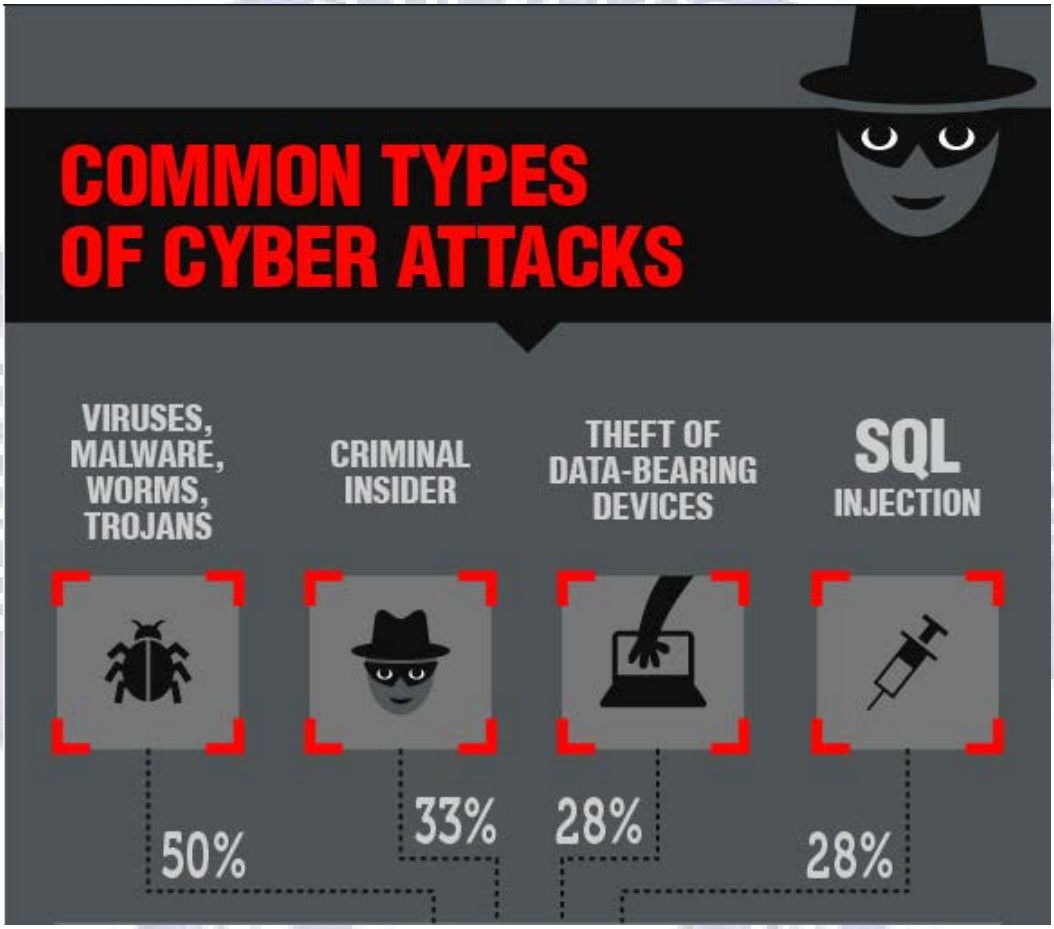
Cybercrime, or computer related crime, is crime that involves a computer and a network (Moore, R. 2005). The computer may have been used in the commission of a crime, or it may be the target (Warren G. Kruse & Jay G. Heiser, 2002). Cybercrimes can be defined as offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as the Internet and other networks. Cybercrime may threaten a person or a nation's security and financial health (Steve Morgan, 2016). Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, and unwarranted mass-surveillance. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Globally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyberwarfare. A report sponsored by McAfee estimates that the annual damage to the global economy is at $445 billion (Reuters 2014).

Crimes that use computer networks or devices to advance other ends include among others, the following:

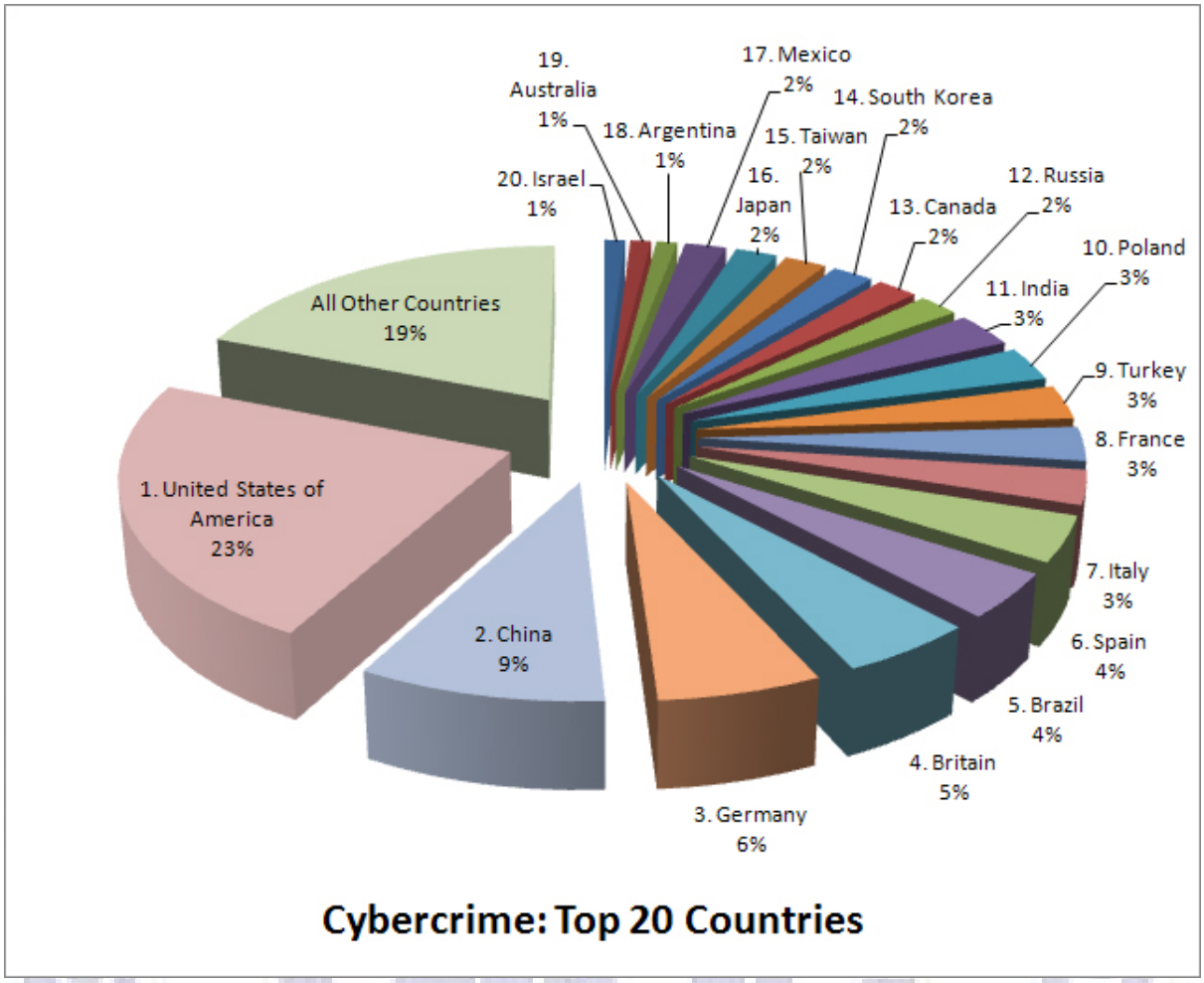
- Fraud;
- identity theft;
- phishing scams;
- email spam;
- the propagation of illegal obscene or offensive content;
- cyber extortion;
- cyber stalking and harassment;
- cyber contraband;

- child pornography;
- cyber laundering;
- cyber terrorism;
- cyber vandalism;

The figure below shows the prevalence of the most common cyber-attacks, where email based attacks, being viruses, malware, worms and trojans are the most prevalent attacks..



The rate of the occurrence of cyber-attacks varies from country to country. The pie chart below shows the prevalence of cybercrime in the top 20 countries in the world. However, it must be emphasised that the SADC region is not an exception.



3.1 Fraud

Fraud is the deliberate deception to secure unfair or unlawful gain, or to deprive a victim of a legal right. While the precise definitions and requirements of proof vary among jurisdictions, the requisite elements of fraud as a tort generally are the intentional misrepresentation or concealment of an important fact upon which the victim is meant to rely, to the harm of the victim (Judicial Council of California, 1900). Proving fraud in a court of law is often said to be difficult in that each and every element of fraud must be proven, and the elements include proving the states of mind of the perpetrator and the victim, and that some jurisdictions require the victim to prove fraud by clear and convincing evidence. Remedies for fraud may include rescission of a fraudulently obtained agreement or transaction, the recovery of a monetary award to compensate for the harm caused, and punitive damages to punish or deter the misconduct.

3.2 Identity Theft

Identity theft on the other hand is the deliberate use of someone else's identity, usually as a method to gain financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss (Hoofnagle, Chris Jay, 2007). The person whose identity has been assumed may suffer adverse consequences if they are held responsible for the perpetrator's actions. Identity theft occurs when someone uses another's personally identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes. Identity theft may be used to facilitate or fund other crimes including illegal immigration, terrorism, phishing and espionage. There are cases of identity cloning for purposes of attacking payment systems, including online credit card processing and medical insurance (World Privacy Forum). The most common type is financial identity theft, where someone attempts to gain economic benefits in someone else's name (ID Theft Center, 2014). This includes getting credits, loans, goods and services, claiming to be someone else. The graph below shows identity fraud victims and their losses between 2010 and 2014.

3.3 Phishing

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details and, indirectly, money, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication (Ramzan, Zulfikar, 2010).. Phishing is an example of social engineering techniques used to deceive users, and exploit weaknesses in current web security (Jøsang, Audun; et al., 2007). Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. Several phishing attacks have been directed specifically at senior executives and other high-profile targets within businesses, and the term whaling has been coined for these kinds of attacks. Attackers may gather personal information about their target to increase their probability of success. This technique is by far the most successful on the internet today, accounting for 91% of attacks (Stephenson, Debbie, 2014). In the case of whaling, the masquerading web page/email will take a more serious executive-level form. The content will be crafted to target an upper executive and the person's role in the company. The content of a whaling attack email is often written as a legal subpoena, customer complaint, or executive issue. Whaling scam emails are designed to masquerade as a critical business email, sent from a legitimate business authority. The content is meant to be tailored for upper management, and usually involves some kind of falsified company-wide concern. Whaling phishers have also forged official looking subpoena emails, and claimed that the executive needs to click a link and install special software to view the subpoena. Targeted phishing, where known information about the recipient is used to create forged emails, is known as spear-phishing.

3.4 Spam

Email spam, also known as junk email, is a type of electronic spam where unsolicited messages are sent by email. Many email spam messages are commercial in nature but may also contain disguised links that appear to be for familiar websites but in fact lead to phishing web sites or sites that are hosting malware. Spam email may also include malware as scripts or other executable file attachments (trojans). Spam is

named after Spam luncheon meat by way of a Monty Python sketch in which Spam in the sketch is ubiquitous, unavoidable and repetitive. Email spam has steadily grown since the early 1990s. Botnets, networks of virus-infected computers, are used to send out spam. Spammers collect email addresses from chatrooms, websites, customer lists, newsgroups, and viruses that harvest users' address books. These collected email addresses are sometimes also sold to other spammers. The legal status of spam varies from one jurisdiction to another. Many spam emails contain URLs to a website or websites. According to a Cyberoam report in 2014, there are an average of 54 billion spam messages sent every day. Pharmaceutical products (Viagra and the like) jumped up 45% from last quarter's analysis, leading this quarter's spam pack. Emails purporting to offer jobs with fast, easy cash come in at number two, accounting for approximately 15% of all spam email (Sophos Cyberoam., 2014).

3.5 Cyber Extortion

Cyber extortion occurs when a website, e-mail server, or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand money in return for promising to stop the attacks and to offer "protection". According to the Federal Bureau of Investigation, cyber extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. More than 20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the public domain. Perpetrators typically use a distributed denial-of-service attack (Lepofsky, Ron, 2011). An example of cyber extortion was the attack on Sony Pictures of 2014.

3.6 Cyber Vandalism

Cyber vandalism is the act of damaging or destroying data rather than stealing or misusing them (as with cyber theft). This can include a situation where network services are disrupted or stopped, depriving the computer/network owners and authorised users (website visitors, employees) the data or information contained on the network. Examples include accessing a network without permission and altering, destroying, or deleting data; deliberately entering malicious code (viruses, rootkits, trojans) into a computer network to monitor, follow, disrupt, stop, or perform any other action without the permission of the owner of the network.

3.7 Cyber Terrorism

Governments and information technology security specialists have documented a significant increase in cyber related crimes over the years. In 2016, a study by Juniper Research estimated that the costs of cybercrime could be as high as 2.1 trillion by 2019 (Juniper Reserch, 2016). There is a growing concern globally that such intrusions are part of an organised effort by cyberterrorists, foreign intelligence services, or other groups to map potential security holes in critical systems. A cyberterrorist is someone who intimidates or coerces a government or an organisation to advance his or her political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them. Cyberterrorism in general can be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker 1983).

4. Implications for SADC Central Banks

Cybersecurity is key to financial stability and economic security, as global finance, payment systems and currency markets become increasingly dependent on digital technologies. The role of technology in the provision of financial services has deepened over the past decades. Further, the degree of interdependency and interconnectedness between operators in financial markets is very high and growing.

Banks, large investment firms, insurers and other entities within the financial markets infrastructure can be vulnerable to potentially devastating cyber-attacks, which are becoming increasingly more frequent and sophisticated. Both attackers and their motivations have become more diverse, bringing fresh threats from unexpected sources, including but not limited to: those who merely seek to disrupt activity; cyber criminals motivated by financial gain; terrorists aiming to cause political and financial instability; and nation state-related actors attempting to interfere with or gain access to sensitive information, or to cause systemic instability (World bank Group, 2014).

In view of cyber security issues discussed herein, a primary objective for SADC central banks should be to make the SADC financial landscape a safer place to conduct business by facilitating and cultivating a safe and secure technological environment. SADC central banks therefore have a clear role to play in developing and implementing guidelines and ensuring that all stakeholders effectively address potential risks considering the threat that cyber-attacks can present to financial stability. Cyber-preparedness and resilience is crucial to the entire banking system and can be achieved by developing greater awareness and planning, as well as by improving domestic and cross-border cooperation and knowledge sharing across the SADC region. The appropriate governance of IT in SADC central banks and cyber-preparedness are crucial to ensure that cyber-attacks are quickly identified and appropriately dealt with, to limit contagion and quickly resume normal business operations.

Cybersecurity should therefore be a significant focus for SADC central banks. Regional central banks must take a proactive approach to technological and digital innovations by developing governance frameworks and management standards for introducing new technologies and monitoring associated risk. A spate of attacks on central banks in South Korea, Indonesia, Bangladesh, Saudi Arabia and Russia underlines the hazards. Clear rules and regulations are needed on registering actual and attempted cyber-attacks, otherwise unreported cases are likely to become more frequent. The potential impact of a successful cyber-attack is growing in view of the proliferation of digital financial systems. SADC central banks should be key to

strengthening national payment systems and to coordinating supervisors, regulators and market participants. More work needs to be done in increasing regional central bank resilience to cybercrime, training central bank personnel on emerging risks and threats, educating board members about best practice, and implementing contingency plans for successful attacks. Above all, closer regional central bank cooperation and information sharing could yield significant benefits for financial resilience across the region.

5. Recommendations

Pertinent cybercrime issues discussed in this paper present opportunities for SADC central banks to institute appropriate cyber security governance and operational structures that would facilitate the drawing up and implementation of standard cyber security guidelines across the region to safeguard national assets. Of primary importance is the need to have a cyber-security framework that would govern the implementation of agreed guidelines across member central banks for standardisation on security technology, monitoring, reporting and information sharing.

5.1 Cyber Security Framework

It is recommended that SADC central banks should develop, adopt and implement a standard Cyber Security Framework that would provide a basis for the implementation of cyber security controls in line with best practice. A proposal on a Cyber Security Framework (Annex I) has been obtained from Cyberm, a renown Cyber Security Specialist company based in the United States of America. The recommended framework focuses on using business drivers to guide cyber security activities and considering cyber security risks as part of the bank's risk management processes. At a high level, the framework aligns to international recommendations of the G7 and centres on the following key cyber security elements:

- **Element 1:** Cyber Security Strategy and Framework

- **Element 2:** Governance
- **Element 3:** Risk and Control Assessment
- **Element 4:** Monitoring
- **Element 5:** Response
- **Element 6:** Recovery
- **Element 7:** Information Sharing
- **Element 8:** Continuous Learning

The strategy is to align to the Centre for Internet Security Control (CISC)'s 20 prioritised actions to mitigate against the vast majority of common cyber-attacks. These controls will provide coverage for all elements of the G7 Cyber Security recommendations. The controls are as follows:

- **Critical Security Control #1**: Inventory of Authorized and Unauthorized Devices;
- **Critical Security Control #2**: Inventory of Authorized and Unauthorized Software;
- **Critical Security Control #3**: Secure Configurations for Hardware and Software;
- **Critical Security Control #4**: Continuous Vulnerability Assessment and Remediation;
- **Critical Security Control #5**: Controlled Use of Administrative Privileges;
- **Critical Security Control #6**: Maintenance, Monitoring, and Analysis of Audit Logs;
- **Critical Security Control #7**: Email and Web Browser Protections;
- **Critical Security Control #8**: Malware Defenses;
- **Critical Security Control #9**: Limitation and Control of Network Ports;
- **Critical Security Control #10**: Data Recovery Capability;
- **Critical Security Control #11**: Secure Configurations for Network Devices;
- **Critical Security Control #12**: Boundary Defense;
- **Critical Security Control #13**: Data Protection;
- **Critical Security Control #14**: Controlled Access Based on the Need to Know;
- **Critical Security Control #15**: Wireless Access Control;

- **Critical Security Control #16**: Account Monitoring and Control;
- **Critical Security Control #17**: Security Skills Assessment and Appropriate Training to Fill Gaps;
- **Critical Security Control #18**: Application Software Security;
- **Critical Security Control #19**: Incident Response and Management;
- **Critical Security Control #20**: Penetration Tests and Red Team Exercises.

The development of the regional Cyber Security Framework by Cyberm would amount to USD $107,000.00 for all central banks.

5.1 Compliance

For compliance with the recommended framework and ease of monitoring, Cyberm recommends using ComplianceMapperTM tool, developed by the US company C2C SmartCompliance, which will have a module designed to cover compliance with the SADC Central Banks Cyber Security Framework. Annual licence fees for ComplianceMapperTM based on negotiated group volume licensing (GVL) fees would amount to $12 485.00 per bank if a minimum of 8 banks sign up. Otherwise the license would be $16 400.00 per bank if GVL rates are not applied.

5.2 Cyber Security Resources

Cyber-attacks are increasing in sophistication and frequency, yet the shortage of skilled technical professionals has continued to grow exponentially. For the appropriate implementation, monitoring and compliance with the recommended Cyber Security Framework, it is therefore recommended that SADC Central Banks should develop capacity in cyber security and establish dedicated cyber security functions that would holistically oversee cyber security related matters in domestic central banks.

6. Conclusion

In conclusion, in view of the ever increasing prevalence of cyber-attacks on financial institutions and central banks in particular, the need for heightened cyber security control measures both in domestic central banks and across the region cannot be overemphasised. The ICT Steering Subcommittee therefore seeks the approval of the CCBG to proceed with the development of a Cyber Security Framework based on the G7 Cyber Security Principles for the region as per the CCBG's instruction to go beyond normal protocol in response to this very topical issue. It should be noted that this task involves cost and as such, approval is also being sought to engage Cyberm as per their proposal.

7. References

Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 0-201-70719-5.

Steve Morgan (January 17, 2016). "Cyber Crime Costs Projected To Reach $2 Trillion by 2019". Forbes. Retrieved September 22, 2016.

"Cyber crime costs global economy $445 billion a year: report". Reuters. June 9, 2014. Retrieved June 17, 2014.

"Cybercrime will Cost Businesses Over $2 Trillion by 2019" (Press release). Juniper Research. May 21, 2016.

Parker D (1983) Fighting Computer Crime, U.S.: Charles Scribner's Sons.

Lepofsky, Ron. "Cyberextortion by Denial-of-Service Attack" (PDF). Archived from the original (PDF) on July 6, 2011.

Mohanta, Abhijit (December 6, 2014). "Latest Sony Pictures Breach : A Deadly Cyber Extortion". Retrieved 20 September 2015.

"California Civil Jury Instructions: 1900. Intentional Misrepresentation". Judicial Council of California. Retrieved 2013-12-27.

Synthetic ID Theft Cyber Space Times Archived October 9, 2015, at the Wayback Machine.

Hoofnagle, Chris Jay, Identity Theft: Making the Known Unknowns Known. Harvard Journal of Law and Technology, Vol. 21, Fall 2007

"What is Financial Identity Theft". ID Theft Center. Retrieved 3 December 2014.

Medical Identity Theft: What to Do if You are a Victim (or are concerned about it)"., World Privacy Forum

Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures". In Stamp, Mark & Stavroulakis, Peter. Handbook of Information and Communication Security. Springer. ISBN 9783642041174.

Tan, Koontorm Center. "Phishing and Spamming via IM (SPIM)". Retrieved December 5, 2006.

Jøsang, Audun; et al. (2007). "Security Usability Principles for Vulnerability Analysis and Risk Assessment." (PDF). Proceedings of the Annual Computer Security Applications Conference 2007 (ACSAC'07).

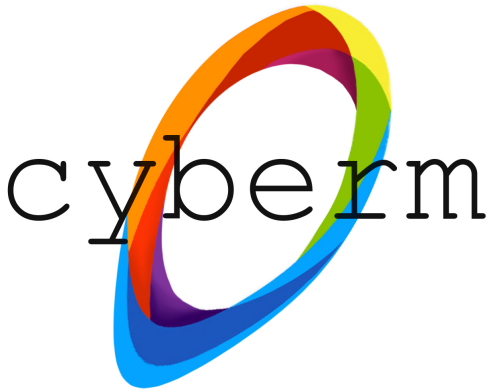
Stephenson, Debbie. "Spear Phishing: Who's Getting Caught?". Firmex. Retrieved July 27, 2014.

Sophos Cyberoam *"Q1 2014 Internet Threats Trend Report*" (Press release). Retrieved 2015-11-01.

World Bank Group. Committee on Payments and Market Infrastructures (November 2014)

8. Annexes

Annex I Refer to the attached Cyberm proposal for a Cyber Security Framework for SADC Central Banks.



proposal

cyber security framework

Bank of Botswana

Plot 17938, Khama Crescent, Gaborone, Botswana

Ref: Proposal_BoB_CSF_2Aug17_v4
Wednesday, August 2, 2017

Table of Contents

1. Executive Summary

Cyber threats present a set of pressing operational, reputational and financial stability risks facing the international financial system. Sovereign borders do not contain these threats, and accordingly, nations must work together to address them.

Since banks and financial institutions conduct business worldwide, complex regulatory requirements have been established causing greater cyber threats and heightened concerns for data security and privacy across virtual borders.

Cyber security is the process, ability or state in which information and communication systems are protected against damage, unauthorized use or modification or exploitation.

Security against threats can be achieved by implementing different types of technology, policies and best practices to the Banks, cyber issues facing Banks today include, but are not limited to:

- ✓ If a Bank does not properly implement regulations and standards, they can suffer from data loss and improper management of assets
- ✓ Being compliant is not a guarantee that risk is being mitigated properly
- ✓ Data Is not identified and classified based on the sensitivity and criticality
- ✓ Banks lack an understanding of what information is most important
- ✓ Solutions are used for data loss but not used for a risk-based approach
- ✓ Instead of treating incidents, there should be a holistic approach on how to mitigate risk

The framework solution being put forward will address these issues and allow Bank of Botswana and other central banks in SADC region to move forward with confidence.

The proposal that follows describes the different functions involved in such project, methodologies, CVs, and processes of the project.

2. Project Objectives

Bank of Botswana has requested consultancy services to develop a framework for cyber security that can be applied to various Central Banks within the Southern African Development Communities ("SADC") that will provide them with the Security against threats, by implementing different types of technology, policies and best practices at the Banks.

3. Project Tasks and Deliverables Summary

During this project, the following tasks and deliverables will be performed (all deliverables will be provided in English language):

Project Tasks and Deliverables

Tasks	Deliverables
1. Project Initiation	
✓ Project Documentation	✓ Project Plan ✓ Project Progress and Status Reports ✓ Project closure and lessons learned
2. Cyber Security Framework	
✓ Develop Cyber Security Framework	✓ Cyber Security Framework

4. Detailed Project Methodolgy Elements

Cyberm's Consultants shall deliver the mentioned tasks to ***Bank of Botswana ("Customer")*** according to the following understanding and methodology:

4.1 Project Initiation

The purpose of this step is to determine the objectives of the project, as well as to design the proposed project plan. Furthermore, it will ensure that the objectives and scope of the project are clearly understood in advance by both parties and that the project is conducted according to the defined timetable. Therefore, ***Cyberm*** will conduct:

- ✓ Kickoff meeting with the Customer's Project Management.
- ✓ Presentation to the Customer's Management.
- ✓ Project Plan and schedule shall be agreed upon with ***the Customer***.
- ✓ Periodic status and progress reports once required.

4.2 Develop Cyber Security Framework

The recommended framework focuses on using business drivers to guide cyber security activities and considering cyber security risks as part of the Bank's risk management processes. The Framework consists of two (2) parts:

- ✓ Framework Core – Controls.
- ✓ Framework Implementation.

Identifying the correct approach could be a momentous task. The proposed framework will follow an approach that will provide confidence to the Central Banks in SADC and the Banks implementing the framework.

For better compliance with the framework and ease monitoring for **the Customer**, **Cyberm** recommends using ComplianceMapper™ tool, developed by the US company C2C SmartCompliance, which will have a module designed to cover compliance with the Customer's Cyber Security Framework. For more information about ComplianceMapper™ tool, please refer to Appendix B below.

It is proposed to provide a high-level approach that aligns to international recommendation, the following 8 elements are recommended from the G7 for Cyber Security, which **Cyberm** will adopt:

- ✓ Element 1: Cyber Security Strategy and Framework
- ✓ Element 2: Governance
- ✓ Element 3: Risk and Control Assessment
- ✓ Element 4: Monitoring
- ✓ Element 5: Response
- ✓ Element 6: Recovery
- ✓ Element 7: Information Sharing
- ✓ Element 8: Continuous Learning

4.2.1 Element 1 – Strategy and Framework

The strategy is to align to the Center for Internet Security – CIS Control – 20 prioritized actions to beat the vast majority of common attacks, vis-a-vie:

- ✓ Critical Security Control #1: Inventory of Authorized and Unauthorized Devices:

  Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

- ✓ Critical Security Control #2: Inventory of Authorized and Unauthorized Software:

  Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

- ✓ Critical Security Control #3: Secure Configurations for Hardware and Software:

  Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a

rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

- ✓ Critical Security Control #4: Continuous Vulnerability Assessment and Remediation:

  Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

- ✓ Critical Security Control #5: Controlled Use of Administrative Privileges:

  The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

- ✓ Critical Security Control #6: Maintenance, Monitoring, and Analysis of Audit Logs:

  Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

- ✓ Critical Security Control #7: Email and Web Browser Protections:

  Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.

- ✓ Critical Security Control #8: Malware Defenses:

  Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

- ✓ Critical Security Control #9: Limitation and Control of Network Ports:

  Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

- ✓ Critical Security Control #10: Data Recovery Capability:

  The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

- ✓ Critical Security Control #11: Secure Configurations for Network Devices:

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

- ✓ Critical Security Control #12: Boundary Defense:

  Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

- ✓ Critical Security Control #13: Data Protection:

  The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

- ✓ Critical Security Control #14: Controlled Access Based on the Need to Know:

  The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

- ✓ Critical Security Control #15: Wireless Access Control:

  The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

- ✓ Critical Security Control #16: Account Monitoring and Control:

  Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

- ✓ Critical Security Control #17: Security Skills Assessment and Appropriate Training to Fill Gaps:

  For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

- ✓ Critical Security Control #18: Application Software Security:

Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

- ✓ Critical Security Control #19: Incident Response and Management:

  Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

- ✓ Critical Security Control #20: Penetration Tests and Red Team Exercises:

  Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

The above controls will provide coverage for all elements of the G7 Cyber Security recommendations.

4.2.2 Element 2 - Governance

Governance will provide the capability to link the controls to Banks policies and procedures, the recommendation for the Governance aspect of this service will be the use of C2CSmartCompliance's Compliance Mapper product that will show mappings and responsibilities of individuals to their respective roles and ensure that all policies are adhered to. See Appendix B for additional information on Compliance Mapper.

4.2.3 Element 3: Risk and Control Assessment

Compliance Mapper will provide the appropriate risk and assessments necessary to ensure that the controls have been implemented appropriately, all components are included in the product to ensure that disparate systems are not used causing inconsistencies in the cyber security relation models.

4.2.4 Element 4: Monitoring

Covered by Control #16: Account Monitoring and Control: Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

4.2.5 Element 5: Response

Covered by Control #19: Incident Response and Management: Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

4.2.6 Element 6: Recovery

Covered by Control #10: Data Recovery Capability: The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

4.2.7 Element 7: Information Sharing

Covered by multiple controls

4.2.8 Element 8: Continuous Learning

Covered by Control #17: Security Skills Assessment and Appropriate Training to Fill Gaps: For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

Please note that the G7 Elements displayed are at the highest level – each control has sub requirements that will be implemented during the overall implementation process.

Any control requirements outside the G7 elements will be covered by ISO 27001:2013 Information Security Standard, ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for Cybersecurity, NIST CyberSecurity Framework v1.1 and NIST 800-53 rev 4 Security Controls.

The elements provide a mechanism for Banks to view and understand the characteristics of their approach to managing cyber security risk. It also includes a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cyber security activities. While processes and existing needs will differ, the elements will assist Banks in incorporating privacy and civil liberties as part of a comprehensive cyber security program. The elements enable Banks – regardless of size, degree of cyber security risk, or cyber security sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The elements also provide Banks and structure to today's multiple approaches to cyber security by assembling standards, guidelines, and practices that are working effectively in industry today. Moreover, because it references globally recognized the elements can also be used by Banks located outside their borders and can serve as a model for international cooperation on strengthening critical infrastructure cyber security.

5. Project Resources and Schedule

We will conduct this project by utilizing 2 resources working onsite and offsite; also an SME will be assisting the team during the project (please refer to Appendix A below for BIOs). We will perform the required tasks within a period of 2 months. This period could be broken down and scheduled upon agreement with project team as the project progress.

6. Project Management

We are committed to provide the best of service to ***the Customer*** by implementing the best practices and always seeking the customer satisfaction as well as the quality of implementation of the mentioned tasks, this project shall be managed by ***Cyberm*** team by considering the following:

- ***Cyberm*** team:
  - Project team will be headed by a senior resource designated as project manager, who will be responsible for successful project execution including project management activities.
  - Project team will comprise technical resources as per the tasks / activities in each phase. Project team will be committed to the phase throughout its duration, unless otherwise agreed upon in advance with ***the Customer***.
- Project Plan:
  - ***Cyberm*** with the coordination with ***the Customer*** team shall prepare the project plan and schedule immediately after the kickoff meeting with the ***Customer***.
- Change Management:
  - Any changes during the execution of this project shall be made through an official change management request and both parties should approve it.
- Status and tasks progress reports:
  - ***Cyberm*** shall prepare a periodic status report showing the progress of the tasks.
- General assumptions:
  - ***The Customer*** will provide adequate office accommodation, telephones, intranet and Internet connectivity, secretarial support and IT support for the project team.
  - ***The Customer*** will provide administrative support for the scheduling of site visits and meetings with stakeholders.
  - ***The Customer*** will ensure that necessary stakeholders make themselves available for interviews at times and places that do not unduly impact the timescales of the project.
  - Any software/hardware required to mitigate the identified risk is not part of the proposal and could be purchased by client, if required.

- ✓ **Project Completion:**
  - ✓ Project sign-off: the formal sign-off is obtained from ***the Customer*** indicating the completion of the project.

7. Confidentiality

Cyberm agrees that it shall hold ***the Customer's*** confidential information in confidence and shall take reasonable steps to safeguard the confidential information including those steps that it takes to protect its own confidential information of a similar nature.

Cyberm shall not disclose or otherwise provide any confidential information to any third party without the prior written consent of ***the Customer***. Non-Disclosure Agreement can be signed to this effect if need be.

Cyberm agrees to limit its internal disclosure of confidential information to only those of its employees or contractors who are bound by confidentiality agreements prohibiting further disclosure of the confidential information.

8. Financial Section

8.1 Services Fees

Our financial offer is based on the agreed upon scope of work as per the request from ***Bank of Botswana*** and the time and resources needed to complete the work.

Cyber Security Framework

Phase	Fees
Cyber Security Framework (55 man-days, on-site and off-site including T&E) Project Management (15 days, off-site)	USD 107,000.00
Total	USD 107,000.00

Note: Service Fees include all travel and accommodation costs

ComplianceMapper™ Tool

Option 1	<u>Group Annual Cloud License</u> cost including maintenance for up to 15 SADC Central Banks @ **$12 485.00** per Bank ***Note: Price valid only if a minimum of 8 licenses are purchased***	USD 187,275.00
Option 2	<u>Individual Bank Annual Cloud License</u> cost including maintenance for SADC Central Banks @ **$16 400.00** per Bank	USD 246,000.00

8.2 Terms and Conditions

- ✓ Proposal is estimated based on the information provided, ***Cyberm*** reserves the right to change any part of the proposal, if new information arises from the customer side that will affect the scope of work or required engagement.
- ✓ The above prices represent the cost of professional services that will be provided by ***Cyberm***.
- ✓ Pricing valid for **6 months** from date of proposal.
- ✓ Upon acceptance of the proposal, Cyberm will issue the Customer with a formal Statement of Work.

- ✓ Work performed by ***Cyberm*** will be on-site and off-site, as needed.
- ✓ PO and/or contract shall be issued before the kick-off meeting.
- ✓ Travel and accommodation expenses are included in the above prices.
- ✓ Payments shall be divided as follows:

  Service Fees
  - First Payment shall be 50% of project upon the issuance of the PO.
  - Second Payment of 50% upon the successful closure of project.

  License Fees:
  - 100% upfront payment
- ✓ Payments shall be due not more than 30 days of receiving the invoice.
- ✓ **Deliverables will be considered approved after 2 weeks of submitting them.**

9. Appendices

9.1 Appendix A: Consultants' Resumes

SC
Subject Matter Expert (SME)

Experience and Skills Summary:

SC has in excess of 40 years' experience in IT, much of this spent working internationally in the USA, Europe, South Africa and the Middle East. SC is also a content expert related to regulations, standards and best practices. SC is currently the founder and CEO of C2CSmartCompliance (C2C) a specialist Risk, Governance and Compliance firm with its HQ in Alexandria Virginia and the product architect for the Regulatory Compliance products, Compliance Mapper; MyRiskAssessor and MyRiskTreatment. SC is also a practitioner and regularly undertakes assignments supporting Compliance and privacy initiatives for clients. SC was previously the President and CTO and co-owner of 4FrontSecurity Inc. a US based global information security infrastructure consultancy and services firm that was acquired by Symantec Corporation.

With more than 20 years' experience in Business Protection, combined with an extensive knowledge of the industrial, commercial, government and financial areas, SC has dedicated his skills over this time to be highly focused on risk, governance, compliance, information security and information assurance. SC's intuitive skill is to provide management with tools and techniques that enable them to understand the intricacies in an area where competence and expertise is in short supply worldwide. There is a clear need for executives to understand compliance and risk as it relates to, and serves their organization. As the threats and vulnerabilities increase, and the laws and regulations become more complex, risk increases dramatically. SC is a specialist in information compliance and security solutions ranging from strategies, policies, and architectures with specific emphasis on content and international standards, which encompass the multiple disciplines within the industry. SC also has a solid understanding of e-commerce and the Law as it stands today. With extensive experience in Business and Security Management SC was involved in Government infrastructures providing security and privacy advice. SC has worked closely with all the major security solutions providers and has created skilled teams of security professionals that can support e-commerce business structures. He was also instrumental in the first major PKI roll out in South Africa.

SC has held senior positions in government, corporate and private businesses for many years and has a solid track record of prior achievements. Although his experience was developed from being technology related, his roles have been various, from operational support, service management, through to sales and marketing, business development and executive management. This has provided him with the breadth and depth of knowledge required to drive Compliance and Information Assurance and IT initiatives in today's challenging times. In a sector where the noise is mixed and confusing, SC is able to help organizations navigate through the business protection (security), compliance and national and international privacy maze to assist them in the selection and delivery of the processes and solutions that will mitigate risk and support corporate governance. SC has significant skill in various standards and control structures including, but not limited too; ISO 9001, ISO 27001, ISO 20000, ISO 22301, ISO 38500, COBIT, ISF, NIST, COSO, GAPP, GLBA, HIPAA, NERC, PCI and Industrial Control Systems. SC has deep International expertise, which is a key differentiator in the GRC and Compliance industry today.

SME Experience

- Member of the British Standards Society - Compliance Committee
- Product architect for Consult2Comply products – Compliance Mapper, Compliance Assessment Professional (CAP) and Risk Asset Professional (RAP)
- ACP for British Standards Institute for ISO 27001 (ISMS), ISO 20000 (ITSM) BS 25999 (BCM) ISO 9001 (QMS)
- Member of the South African Digital Signature Law Advisory Committee representing the interests of Information Security Businesses in relation to government policy.
- Produced Green Paper for the South African Government on Security and Privacy in e-Commerce environments
- Managing Director for a publicly listed IT Service Bureau in South Africa
- Certified in numerous security technologies
- TV appearances for CNBC related to hacking and security issues
- TV appearance for FOX 5 – Virus Protection recommendations
- Contributed to Network Middle East publication – regular monthly column related to security issues
- Contributor to Secure Computing magazine in the USA and UK for security articles
- Presented at NetSec 2002, San Francisco – IDS –v- Forensics
- Sector 5 Presenter – Washington DC – August 2002

- Conducted Webinar for TechTarget on "How to measure Security" September 2002
- Conducted Webinar for TechTarget on "IDS –v- Forensics" October 2002
- Conducted Webinar for TechTarget on "Vulnerabilities- Lets Look Internally" June 2003
- Appointed to Prince George's Community College as Lead Advisor for Faculty Education for Cyber Security Colloquium
- Computerworld article – The Value of Security - Peer to Peers
- SME for ITsecurity.com Security Clinic
- Book and Product Reviewer for ITsecurity.com
- Speaker for ITAA SPEAKERS BUREAU
- Seminar Speaker for Purdue University, Center for Education and Research in Information Assurance and Security - CERIAS – December 2002 and April 2003
- FEAC – Member of the adjunct Faculty, developing course material for Enterprise Architecture certification, specializing in Information Security
- Developed a Enterprise Security Architecture model for integration into existing Enterprise Architectures
- RSA 2003 Conference Speaker – Taking Security to the Boardroom
- industry professionals exchange data and knowledge with each other, as well as financial analysts
- Keynote speaker for "Enterprise Wide Integrity Strategies" http://www.cimcor.com/integrityseries/ September 2003
- Book and Product Reviewer for ITSecurity.com
- Conference speaker – Middle East Business Continuity Conference May 2004 – Dubai, UAE
- Keynote speaker – IT Security Summit 2004 – Knowledge Village, Dubai Internet City, UAE
- Conference Speaker – Gitex 2004 – Dubai UAE
- Conference Speaker – IT Security Summit, Dubai, UAE – February 2005
- Conference Speaker and trainer for FutureIT Conference, Bahrain – May 2005
- Product Architect for 4FrontSecurity Inc. Assessment Manager
- Product Architect for 4FrontSecurity Inc. Asset Risk Calculator
- Developed Assessment Manager Modules for assessments, audit and risk alignment to various regulations, standards, and processes.
- Developed various mapping for standards and regulatory requirements for International Businesses
- Conducted various Webinars on behalf of BSI Americas and BSI Mexico
- Speaker and trainer at the Symantec annual sales conference in Las Vegas

- Speaker at Rendez-vous de la Sécurité de l'information 2006 (RSI) – Montreal Canada

Accreditation and Certifications:

- Educated in the UK. Academic Equivalent in the United States;
- Bachelor of Science in Management Information Systems (B.Sc. Management Information Systems) with the concentration in Information Security.
- Certified in the Governance of Enterprise IT (CGEIT)
- Certified Information Security Manager (CISM)
- Certified and endorsed ISC² Security Subject Matter Expert-II (SSME-II)
- Qualified Lead Auditor for BS 7799/ISO 17799/ISO 27001
- Instructor for the IRCA 802 Certified Lead Auditor for ISO 27001 and ISO 27001 Implementation Courses
- Instructor for ISO 20000 IT Service Management Internal Audit and Implementation courses. Qualified Auditor for ISO 20000
- ISACA Accredited Trainer for CobIT
- Approved trainer (Lead Auditor) and implementer for BS 25999 BCM standard

MT

Senior Information Security Consultant

Experience and Skills Summary:

Eng. MT has more than 9 years of strong experience in Information Technology, Information Security, IT Governance & Compliance, Information Risk Management, IT Service Management, and IT Audit. MT is capable to offer excellent analytic abilities and strong organizational skills, goal driven team player with excellent written/oral communication and practical approach to project delivery.

His main approach is to assure the enhancement of the security posture of the client, as well as utilizing team work and knowledge transfer practices. MT has experience and exposure to various industries and sectors, such as banking & financial, telecom, real-estate, government, transportation, logistics, education NGOs, and manufacturing.

Proven expertise in:

- IT Security Consulting & Management.
- IT Risk Management.
- ISMS implementation based on ISO 27001.
- ITSM implementation based on ISO 20000 and ITIL.
- Project and Program Management.
- Developing Processes, Policies and Procedures.
- Resource Management and Team Leading.
- IT Security Technical Solutions Implementation.
- IT Audit (Internal & External) based on ITGCs and COBIT.
- EU General Data Protection Regulation.
- Privacy Impact Assessment.

Accreditation and Certifications:

- **MSc** in Information, Computer, & Systems Security from University of Bradford, Bradford – UK.
- **BSc** in Computer Engineering from Princess Sumaya University for Technology, Amman – Jordan.
- Certified **ISO 270001:2013 Lead Implementer** (BSI).
- Certified **ISO 270001:2013 Lead Auditor** (BSI).
- Certified **ITIL v3** (Information Technology Infrastructure Library).
- Certified Information Systems Auditor (**CISA**).
- Certified Ethical Hacker (**C|EH**) v8.

- Certified in CCNA (Cisco Certified Network Associate).

KS

Senior Information Security Consultant

Experience and Skills Summary:

KS is a solutions-oriented IT Service and Support Manager with notable success, directing a range of corporate IT initiatives while leading the planning and implementation of ITSM (ITIL) solutions, procedures and policies in direct support of business objectives as well as IT processes. With a considerable experience (16 years) in Information Technology, IT Service Management, Information Security and governance, Risk Management, IT Master Plan, User awareness program development & delivery and implementation in the corporate organization as well as medium and large size organizations.

Also he has delivered ITIL V3 courses as he is an accredited trainer.

Proven expertise in:

- IT Service management
- Service Desk building and management
- IT Security Consulting & Management.
- IT Risk Management.
- Project and Program Management.
- Resource Management and Team Leading.
- IT Service Management Technical Solutions Implementation.
- Service Management Processes awareness and Training.
- ITIL Processes developing and implementing
- IT Policies and Procedures
- Governance and Compliance management

Accreditation and Certifications:

- Bachelor of Information Technology.
- 2 years Diploma in Telecom engineering.
- Training Security+.
- Certified ISO 27001 Lead Auditors.
- Certified ISO 27005 Risk manager.
- Certified ITIL V3 Expert (Life Cycle Module).
- ITIL V3 Foundation and Intermediate Courses Accredited Trainer.
- Training PMP.

AB

Information Security Consultant/Trainer

Experience and Skills Summary:

AB has over than 7 years in information technology experience providing services ranging from security, development to support and implementation for a numerous number of customers.

Main Tasks and Expertise:

- ISMS implementation based on ISO 27001.
- IT Security Consulting & Management.
- IT Risk Management.
- Perform technical activities for delivering effective host, network, data, and application security services.
- Security system deployments, configuration monitoring and reporting.
- Perform vulnerability assessments, security testing, and working with operations and development teams on remediation and mitigation of findings.
- Provide technical support for various technologies.
- Network Security Monitoring related tasks.
- Technologies: RSA (Security Analytics) and VMware.

Certifications and Training Courses:

- Master Degree in MBA/Finance.
- Bachelor Degree in Business information systems.
- ISO 27001 Lead Implementer, bsi.
- ISO 27001 Lead Auditor, bsi.
- Systems Security Certified Practitioner Course, (ISC)2.
- Oracle forms, reports and database (SQL, PL-SQL) training course.
- Oracle essentials E-business suite (general ledger module) training course.
- Certified ITIL v3 (Information Technology Infrastructure Library).
- Web service course for oracle tools training course.
- Secure Coding Course.

9.2 Appendix B: ComplianceMapperTM

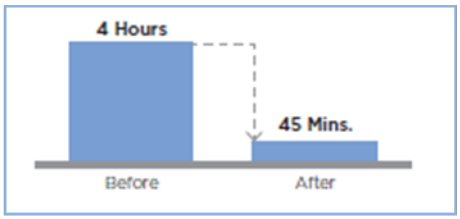
ComplianceMapper™ makes risk and compliance management more efficient and effective

- Ease of adding content to the compliance framework enables global use and ability to map all content (currently over 8,000 regulations, laws, and best practices available)
- Dynamic mapping of regulations to best practices, controls, and bank policies and procedures enables visualization of both direct and indirect relationships of content
- Mappings also enable smart compliance thru combined assessments; assess once, cover all requirements
    - Simplifies and reduces the number of compliance assessments/audits
    - Saves significant operational time due to less disruption of key staff
    - Avoids duplicate or contradictory controls

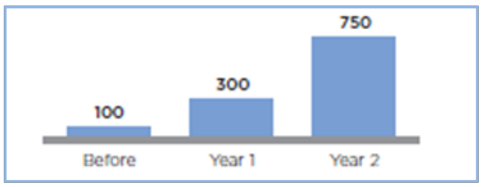
- Work flow management with automatic task assignments notifications
- Repeatable and sustainable audit reporting, both graphical and detailed
- Asset risk assessment methodology compliant with ISO 27001, ISO 20000, and ISO 31000
    - Speeds up risk assessment process by using standard and customizable threats and controls
    - Simply drag a threat to an asset and related vulnerabilities and controls are also selected
    - Consistent risk reporting
- Business impact analysis simplifies and standardizes BIA execution
- Enterprise use by internal audit, vendor management, security, IT, privacy, legal, et.al.

✓ **Smart compliance results in significant benefits across the organization**

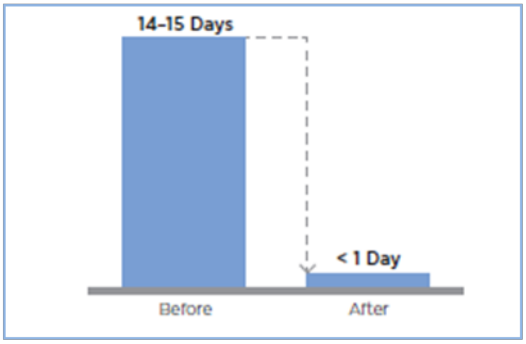
- Studies indicate that compliance programs supported by strong leadership and informed by business risk result in measurable enterprise benefits:
- Fewer disruptions to business due to security events;
- Fewer non-compliance findings;
- Lower cost of compliance;
- Increased security awareness across the organization;
- Security controls address risks;
- Reduced time to maintain compliance requirements;
- Fewer unreported data losses;
- Multi-national Bank reported time savings in vendor risk management, assessments, and control selection shown in graphs below:



Reduced vendor time for risk inputs

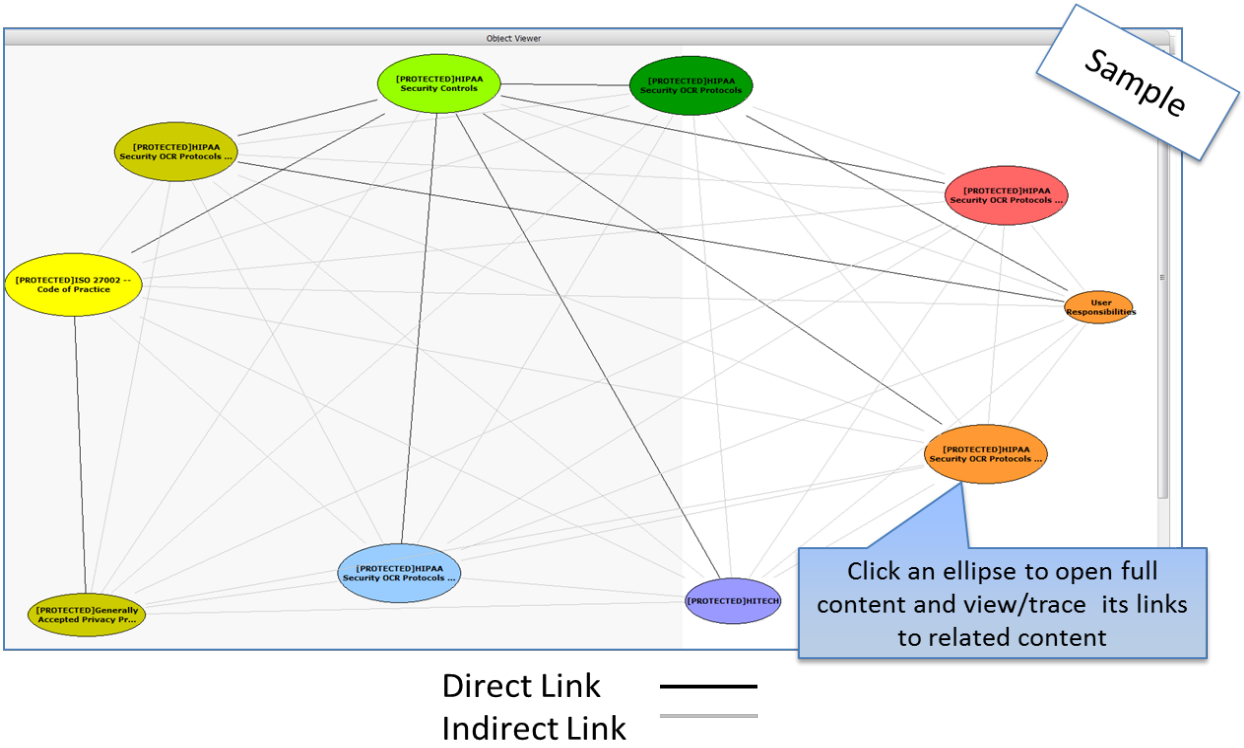


Increased assessments/yr

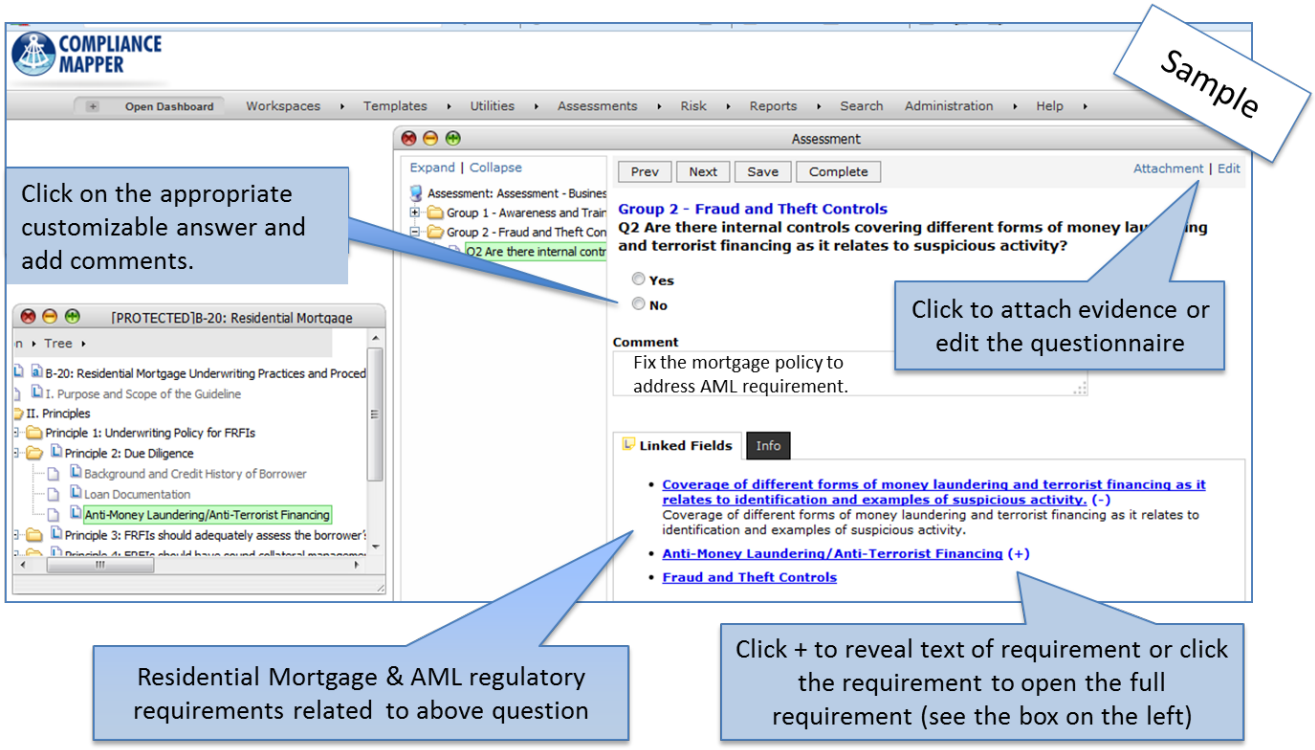


Reduced time to select security controls

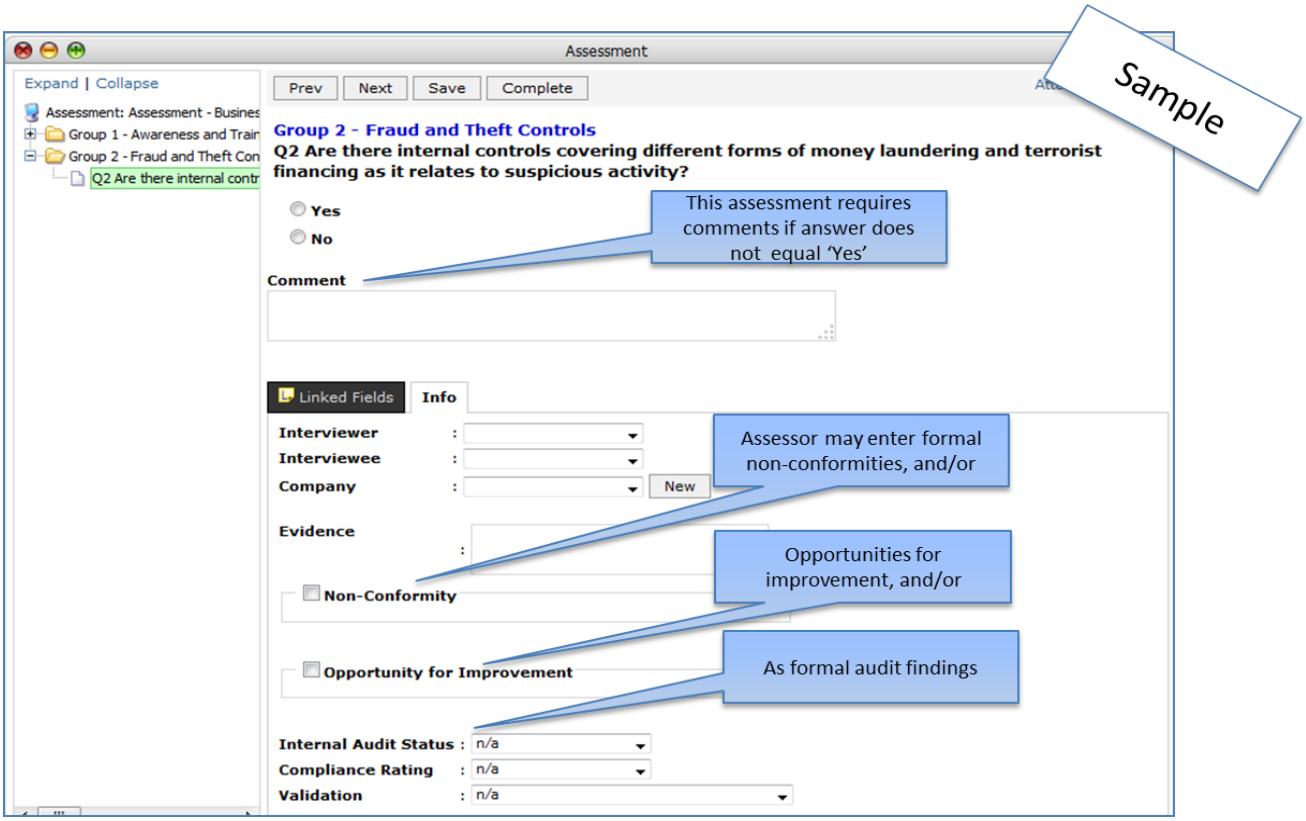
- ✓ Tool Screenshots



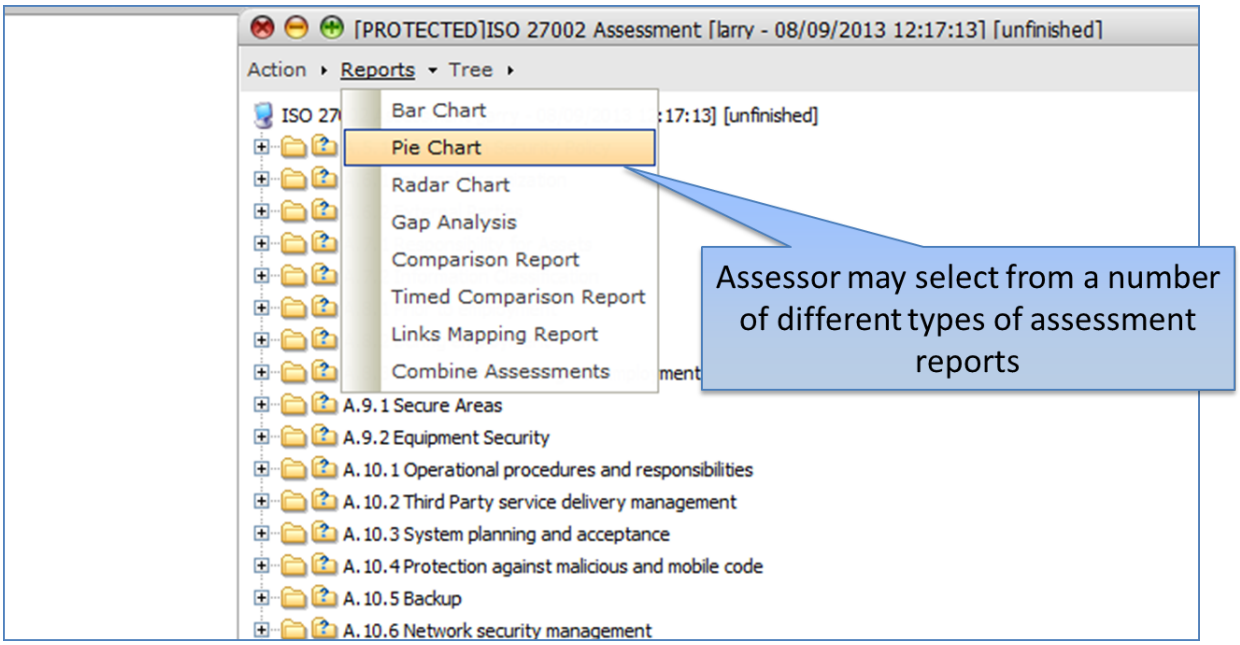
View of direct & indirect relationships between regulations, best practices, policies/procedures, etc.



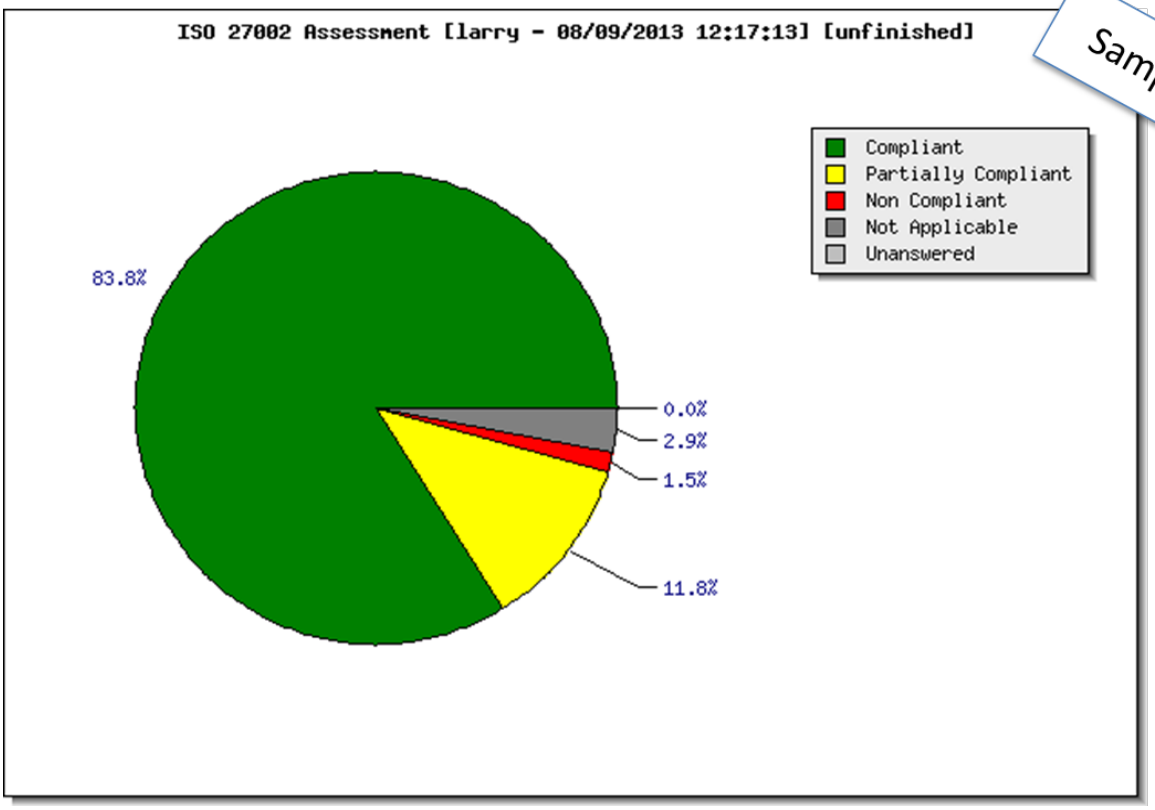
SmartCompliance is enabled by assessing once to cover multiple related regulatory requirements or best practices



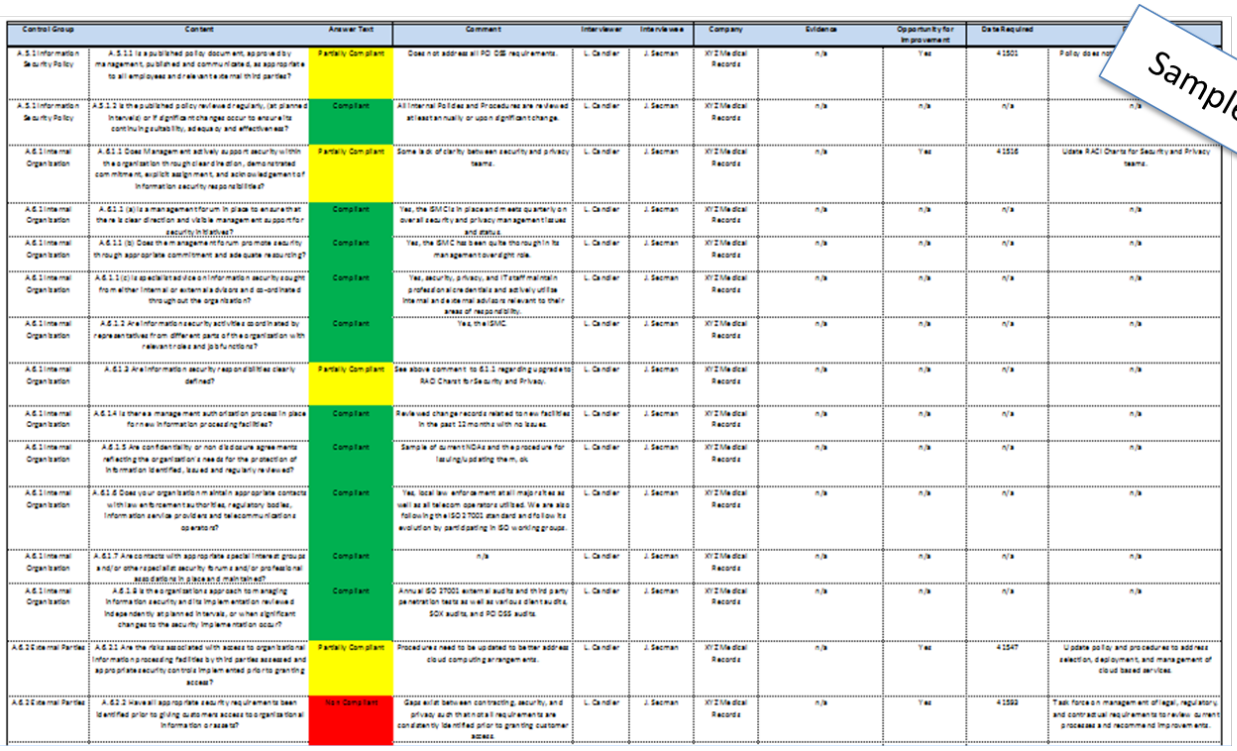
Assessors/Auditors have options for collecting information depending on formalities and personal preferences



Upon completion of an assessment, the assessor may generate and export a variety of report types

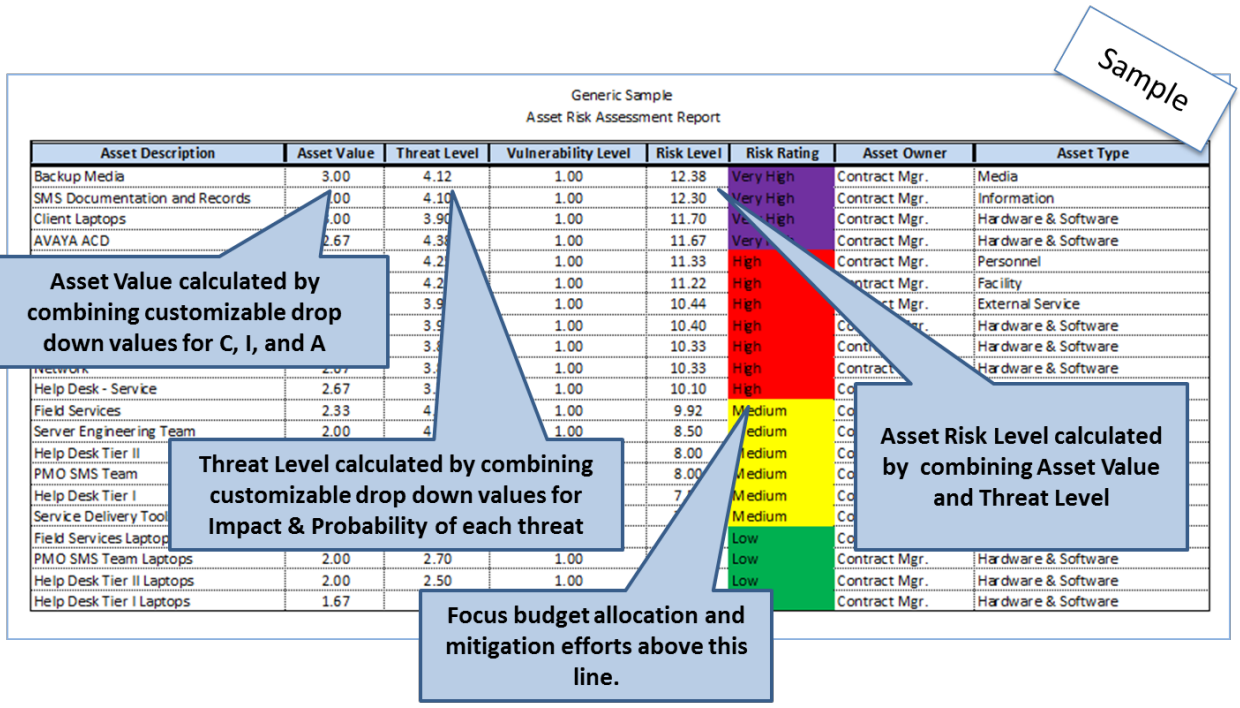


ComplianceMapper generates graphic assessment summary reports



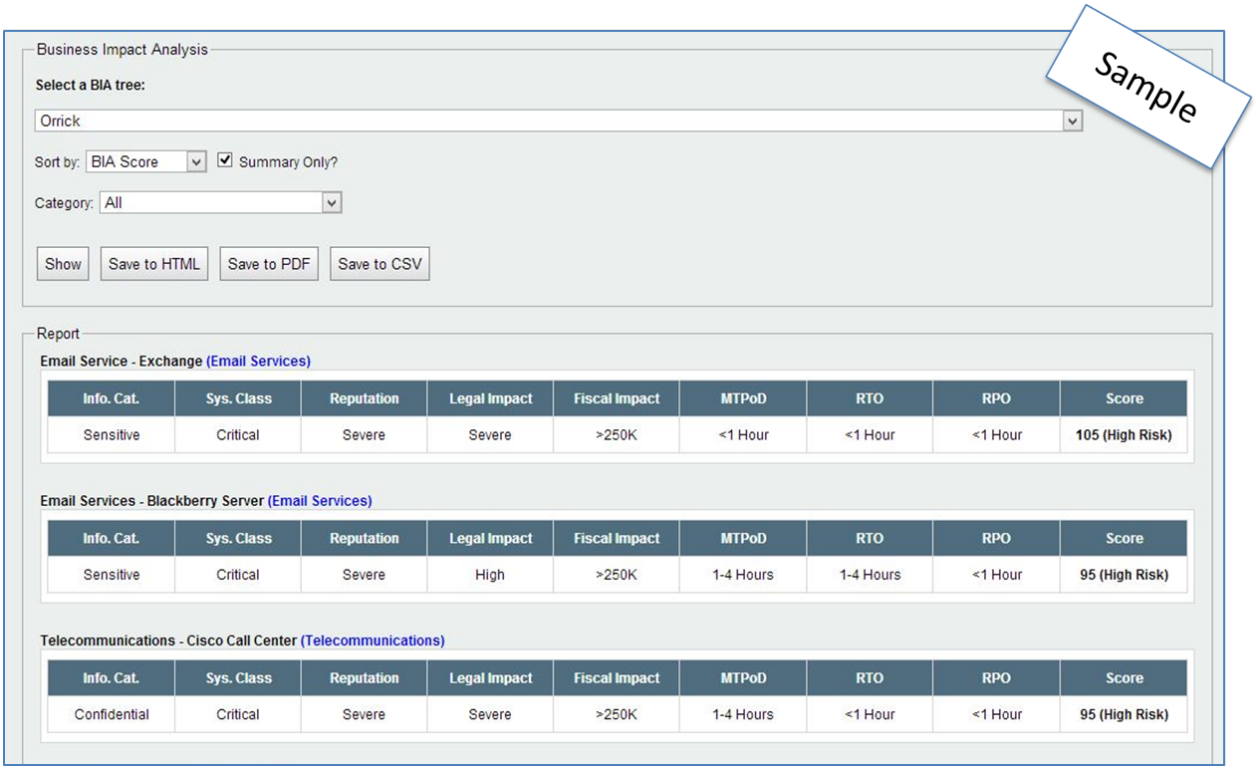
Control Group	Content	Answer Text	Comment	Interviewer	Interviewee	Company	Evidence	Opportunity for Improvement	Date Required	
A.5.1 Information Security Policy	A.5.1.1 Is a published policy document, approved by management, published and communicated, as appropriate to all employees and relevant external third parties?	Partially Compliant	Does not address all PCI DSS requirements.	L. Candler	J. Seeman	XYZ Medical Records	n/a	Yes	4.1501	Policy does not
A.5.1 Information Security Policy	A.5.1.2 Is the published policy reviewed regularly, (at planned intervals) or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness?	Compliant	All Internal Policies and Procedures are reviewed at least annually or upon significant change.	L. Candler	J. Seeman	XYZ Medical Records	n/a	n/a	n/a	n/a
A.6.1 Internal Organization	A.6.1.1 Does Management actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities?	Partially Compliant	Some lack of clarity between security and privacy teams.	L. Candler	J. Seeman	XYZ Medical Records	n/a	Yes	4.1516	Update RACI Charts for Security and Privacy teams.
A.6.1 Internal Organization	A.6.1.1 (a) Is a management forum in place to ensure that there is clear direction and visible management support for security initiatives?	Compliant	Yes, the SMC is in place and meets quarterly on overall security and privacy management issues and status.	L. Candler	J. Seeman	XYZ Medical Records	n/a	n/a	n/a	n/a
A.6.1 Internal Organization	A.6.1.1 (b) Does the management forum promote security through appropriate commitment and adequate resourcing?	Compliant	Yes, the SMC has been quite thorough in its management oversight role.	L. Candler	J. Seeman	XYZ Medical Records	n/a	n/a	n/a	n/a
A.6.1 Internal Organization	A.6.1.1(c) Is specialist advice on information security sought from either internal or external advisors and co-ordinated throughout the organization?	Compliant	Yes, security, privacy, and IT staff maintain professional credentials and actively utilize internal and external advisors relevant to their areas of responsibility.	L. Candler	J. Seeman	XYZ Medical Records	n/a	n/a	n/a	n/a
A.6.1 Internal Organization	A.6.1.2 Are information security activities coordinated by representatives from different parts of the organization with relevant roles and job functions?	Compliant	Yes, the SMC	L. Candler	J. Seeman	XYZ Medical Records	n/a	n/a	n/a	n/a
A.6.1 Internal Organization	A.6.1.3 Are information security responsibilities clearly defined?	Partially Compliant	See above comment to 6.1.1 regarding upgrade to RACI Charts for Security and Privacy.	L. Candler	J. Seeman	XYZ Medical Records	n/a	n/a	n/a	n/a
A.6.1 Internal Organization	A.6.1.4 Is there a management authorization process in place for new information processing facilities?	Compliant	Reviewed change records related to new facilities in the past 12 months with no issues.	L. Candler	J. Seeman	XYZ Medical Records	n/a	n/a	n/a	n/a
A.6.1 Internal Organization	A.6.1.5 Are confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information identified, issued and regularly reviewed?	Compliant	Samples of current NDAs and the procedure for issuing/updating them, ok.	L. Candler	J. Seeman	XYZ Medical Records	n/a	n/a	n/a	n/a
A.6.1 Internal Organization	A.6.1.6 Does your organization maintain appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators?	Compliant	Yes, local law enforcement and magistrates as well as all telecom operators utilized. We are also following the ISO 27001 standard and follow its evolution by participating in ISO working groups.	L. Candler	J. Seeman	XYZ Medical Records	n/a	n/a	n/a	n/a
A.6.1 Internal Organization	A.6.1.7 Are contacts with appropriate special interest groups and/or other specialist security forums and/or professional associations in place and maintained?	Compliant	n/a	L. Candler	J. Seeman	XYZ Medical Records	n/a	n/a	n/a	n/a
A.6.1 Internal Organization	A.6.1.8 Is the organization's approach to managing information security and its implementation reviewed independently at planned intervals, or when significant changes to the security implementation occur?	Compliant	Annual ISO 27001 external audits and third party penetration tests as well as various client audits, SOX audits, and PCI DSS audits.	L. Candler	J. Seeman	XYZ Medical Records	n/a	n/a	n/a	n/a
A.6.2 External Parties	A.6.2.1 Are the risks associated with access to organizational information processing facilities by third parties assessed and appropriate security controls implemented prior to granting access?	Partially Compliant	Procedures need to be updated to better address cloud computing arrangements.	L. Candler	J. Seeman	XYZ Medical Records	n/a	Yes	4.1547	Update policy and procedures to address selection, deployment, and management of cloud based services.
A.6.2 External Parties	A.6.2.2 Have all appropriate security requirements been identified prior to giving customers access to organizational information or assets?	Non Compliant	Gaps exist between contracting, security, and privacy such that not all requirements are consistently identified prior to granting customer access.	L. Candler	J. Seeman	XYZ Medical Records	n/a	Yes	4.1593	Task force on management of legal, regulatory and contractual requirements to review current processes and recommend improvements.

Assessment detail report shows all captured data (comments, opportunities for improvement, recommendations, etc.)



Asset Description	Asset Value	Threat Level	Vulnerability Level	Risk Level	Risk Rating	Asset Owner	Asset Type
Backup Media	3.00	4.12	1.00	12.38	Very High	Contract Mgr.	Media
SMS Documentation and Records	.00	4.10	1.00	12.30	Very High	Contract Mgr.	Information
Client Laptops	.00	3.90	1.00	11.70	Ve High	Contract Mgr.	Hardware & Software
AVAYA ACD	2.67	4.38	1.00	11.67	Very	Contract Mgr.	Hardware & Software
		4.2	1.00	11.33	High	Contract Mgr.	Personnel
		4.2	1.00	11.22	High	ntract Mgr.	Facility
		3.9	1.00	10.44	High	t Mgr.	External Service
		3.9	1.00	10.40	High	Co r.	Hardware & Software
		3.3	1.00	10.33	High	Contr	Hardware & Software
		3	1.00	10.33	High	Contract	Hardware & Software
Help Desk - Service	2.67	3	1.00	10.10	High	Co	
Field Services	2.33	4	1.00	9.92	Medium	Co	
Server Engineering Team	2.00	4	1.00	8.50	edium	Co	
Help Desk Tier II				8.00	edium	Co	
PMO SMS Team				8.00	Medium	Co	
Help Desk Tier I				7	Medium	Co	
Service Delivery Tool					Medium	Co	
Field Services Laptop					Low	Co	
PMO SMS Team Laptops	2.00	2.70	1.00		Low	Contract Mgr.	Hardware & Software
Help Desk Tier II Laptops	2.00	2.50	1.00		Low	Contract Mgr.	Hardware & Software
Help Desk Tier I Laptops	1.67					Contract Mgr.	Hardware & Software

Risk informed compliance identifies the highest value, highest risk assets to prioritize efforts



Info. Cat.	Sys. Class	Reputation	Legal Impact	Fiscal Impact	MTPoD	RTO	RPO	Score
Sensitive	Critical	Severe	Severe	>250K	<1 Hour	<1 Hour	<1 Hour	105 (High Risk)

Info. Cat.	Sys. Class	Reputation	Legal Impact	Fiscal Impact	MTPoD	RTO	RPO	Score
Sensitive	Critical	Severe	High	>250K	1-4 Hours	1-4 Hours	<1 Hour	95 (High Risk)

Info. Cat.	Sys. Class	Reputation	Legal Impact	Fiscal Impact	MTPoD	RTO	RPO	Score
Confidential	Critical	Severe	Severe	>250K	1-4 Hours	<1 Hour	<1 Hour	95 (High Risk)

Example of Business Impact Analysis summary report exportable to HTML, PDF, or CSV formats

10. Optional Services per Bank

The following high-level descriptions are optional services Cyberm can provide each individual Central Bank within the SADC group to assist the Bank(s) with the Management of initial Cyber Security Framework developed by Cyberm and is a pre-requisite to the services offered below:

10.1 Assessment Service: Gap Analysis and Customization (Optional for each bank)

Once the Cyber Security Framework is approved, Cyberm's Consultants shall perform the below phases for each bank:

- ✓ Gap Analysis: This phase shall point out the current weaknesses regarding the developed Cyber Security Framework controls and requirements for each Bank, which shall provide each Bank with a guidance on the domains that needs more concentration and require attention.
- ✓ Customization: During this phase, Cyberm's Consultants shall customize the framework as per the needs for each central bank, based on the country and their environment.
- ✓ Remediation Plan: During this phase, a plan shall be developed recommending the tasks and actions to be implemented by each bank.

10.2 Advisory Support Service (Optional for each bank)

Annually, for the first 3 quarters, **Cyberm** shall review and support each Bank for up-to 5 off-site days per quarter regarding the remediation plan.

10.3 Annual Audit (Optional for each bank)

The 4th quarter, Cyberm's Consultants shall perform an on-site audit and develop a report, including the findings and recommendations for each finding.

10.4 Additional/Optional Services Fees

Our financial offer is based on the agreed upon scope of work as per the request from ***Bank of Botswana*** and the time and resources needed to complete the work.

Service Fees Per Bank

Phase	Fees (USD)
1. Assessment Service: Gap Analysis and Customization (per Bank) Consultant: 15 days (On Site) Project Management: 5 days (Remote)	$29,700.00
2. Advisory Support Service: 5 days per quarters /3 quarters per year (per Bank) Consultant: 15 days (Remote) Project Management: 6 days (Remote)	$24,585.00
3. Annual Audit: 5 days quarter 4 (per Bank) Consultant: 5 days (On Site) Project Management: 2 days (Remote)	$10,150.00

Note: Service Fees include all travel and accommodation costs

10.5 Terms and Conditions

- ✓ Proposal is estimated based on the information provided by ***Cyberm***, ***Cyberm*** reserves the right to change any part of the proposal, if new information arises from the customer side that will affect the scope of work or required engagement.
- ✓ The above prices represent the cost of professional services that will be provided by ***Cyberm***.
- ✓ Upon acceptance of the proposal, Cyberm will issue the Customer with a formal Statement of Work.
- ✓ Work performed by ***Cyberm*** will be on-site and off-site, as needed.
- ✓ PO and/or contract shall be issued before the kick-off meeting.
- ✓ Travel and accommodation expenses are included in the above prices.
- ✓ Payments shall be divided as follows:
    - First Payment shall be 50% of project upon the issuance of the PO.
    - Second Payment of 50% upon the successful closure of project. Payments shall be due not more than 30 days of receiving the invoice.

Deliverables will be considered approved after 2 weeks of submitting them.

11. Contact Details

For more information, contact Cyberm:

Cyberm Contact:
Jeanine Hall
Jeanine.Hall@cyberm.cloud
+27 83 262 2025