Training for the Saudi National Cybersecurity Authority and Essential Cybersecurity Controls

The First Unit: Course Introduction

At the end of the unit, the trainee should be able to:

- To know about cyber security

- To feel the severity of cyber attacks

- To mention the basic controls of cyber security

- To discover the main areas of cyber security

- To explain the basics of cyber security

- To explain the basic controls of cyber security

Lesson1: Course Introduction

Introduction

Cyber-security is a complex and multifaceted challenge that is growing in importance. Traditionally viewed as an IT security problem, many organizations today realize that cyber security needs to be treated as a broader risk management issue to protect business interests against the adverse effects of cybercrime and hacktivism.

Cyber-attacks are becoming more frequent, widespread and sophisticated. The rise in frequency and breadth of Cyber-attacks can be attributed to a number of factors:

- Unfriendly nation-states breach systems to seek intelligence or intellectual property.

- Hacktivists aim to make political statements through systems disruptions.

- Organized crime groups, cyber gangs, and other criminals breach systems for monetary gain-i.e., to steal funds via account takeovers, ATM heists, and other mechanisms.

As the cost of technology decreases, the barriers to entry for cyber-crime drop, making it easier and cheaper for criminals of all types to seek out new ways to perpetrate cyber fraud.

In this paper, we aim to present some implementation considerations for Saudi Arabia’s National Cybersecurity Authority Essential Cybersecurity Controls (ECC – 1:2018) Standard.

The National Cybersecurity Authority (NCA) today launched the second phase of its CyberIC program, a comprehensive initiative designed to bolster the cybersecurity capabilities of the Kingdom.

The program aims to cultivate specialized national expertise in the cybersecurity sector and elevate the cyber preparedness of national entities. This aligns with NCA’s broader mission to foster the development of the cybersecurity industry and human capabilities, ultimately strengthening cybersecurity in Saudi Arabia.

The second phase of CyberIC focuses on six key areas: cybersecurity specialists and leaders, specialists in investigation and judicial authorities, specialists in fields related to cybersecurity, national entities executives, and students and recent graduates. The program seeks to empower around 13,000 individuals in the field of cybersecurity.

The programs encompass a wide range of cybersecurity disciplines, including data analysis, encryption, and secure cloud computing, in partnership with Saudi Information Technology Company (SITE), NCA’s technical arm, and leading international universities.

The CyberIC program is a cornerstone of the National Cybersecurity Strategy, contributing to the Kingdom's efforts to protect critical infrastructure and government services through its focus on skills development and knowledge enhancement.

Lesson2 : What is NCA-ECC?

NCA ECC – 2: 2024 – A comprehensive update to Essential Cyber Security Controls (ECC)

As the digital environment advances and new cyber threats emerge, the National Cyber security Authority (NCA) has recognized the need to enhance its cyber security guidelines continuously. In response to these growing challenges, the Authority has updated its Essential Cyber security Controls (ECC), releasing NCA ECC–2:2024, an evolution of the previously established NCA ECC–1:2018).

This new version reinforces Saudi Arabia's commitment to robust cyber security and addresses the latest vulnerabilities and trends in information security. ECC–2:2024 offers a more comprehensive, updated set of controls that align with international standards and address traditional IT systems and new-age technologies like cloud infrastructure and industrial control systems.

Let's explore the key changes being done in the new version.

What is NCA ECC–2:2024?

The NCA has introduced an updated version of its Essential Cyber security Controls (ECC–2:2024) after extensively evaluating various global and national cyber security frameworks. This update comes from a thorough analysis that considered international standards, national regulations, and relevant legal requirements.

The NCA also incorporated cyber security best practices and carefully examined past cyber incidents impacting government entities and other critical organizations.

NCA ECC–2:2024 is structured into:

4 Cyber security Main Domains

- 28 Cyber security Subdomains
- 110 Cyber security Controls

- 90 Cyber security Sub controls

It’s worth noting that this latest version refines the previous ECC–1:2018, which included 5 main domains, 29 subdomains, and 114 controls. The updated structure offers a streamlined and more focused approach, addressing the most pressing cyber security challenges organizations face today.

Implementation and compliance

All organizations that fall under the NCA ECC–2:2024 framework must take steps to ensure they continuously meet the required cyber security controls. The Authority may check compliance through various methods, including:

Self-assessments by organizations

- Periodic reports from compliance tools
- On-site audits

Assessment and compliance tool

The NCA will introduce the ECC-2:2024 Assessment and Compliance Tool to help organizations manage their compliance more effectively. This tool will assist organizations in organizing their evaluation processes and measuring how well they meet the ECC requirements.

Updates and enhancements in NCA ECC–2:2024

The latest version of the NCA ECC framework introduces several modifications to enhance clarity and improve security measures across its main domains. Key changes include:

Modifications in terms and conditions.

- Deletion of Domain 5.
- Adjustments to various controls for better alignment with current cyber security practices.
- Enhancements to existing security protocols to address evolving threats.

Notable controls that have been modified include:

Control 1-2-2

- Sub control 2-2-3-1
- Sub control 2-2-3-2
- Sub control 2-4-3-2
- Sub control 2-4-3-5
- Control 2-7-3
- Sub control 2-15-3-5

These updates ensure that organizations can more effectively manage their cyber security responsibilities and respond to emerging risks.

NCA ECC–2:2024 domains and structure

NCA ECC–2:2024 is organized into four main cyber security domains, each addressing specific areas of cyber security. These domains are further divided into subdomains that outline detailed controls and practices.

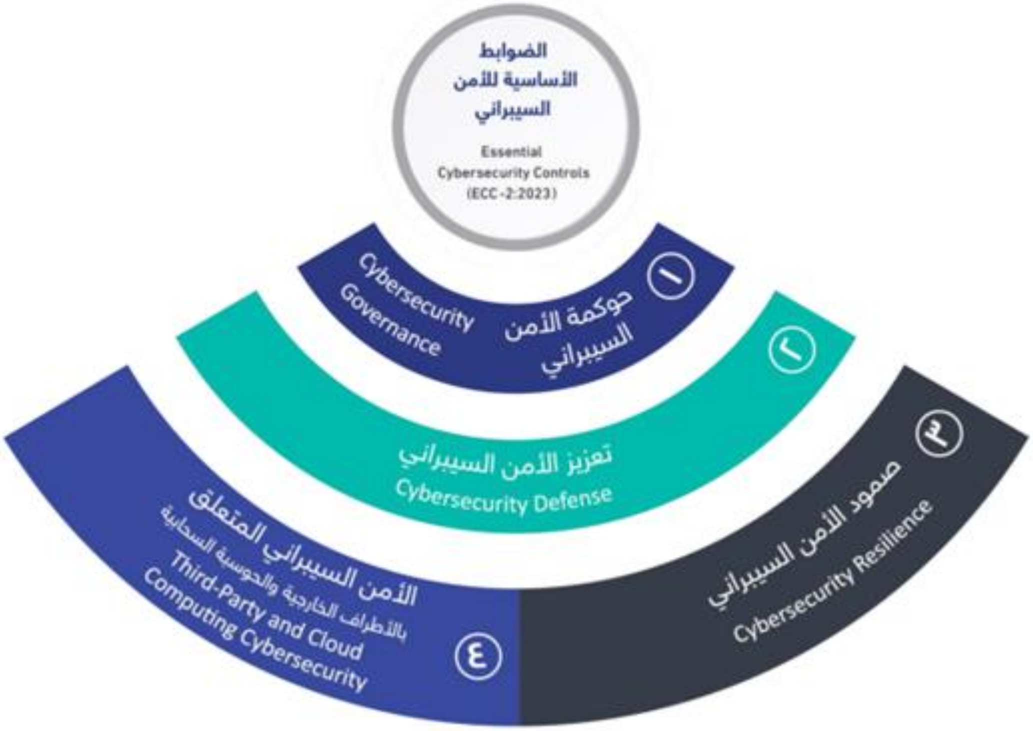

الضوابط الأساسية للأمن السيبراني
Essential Cybersecurity Controls (ECC -2:2023)
١
Cybersecurity Governance
حوكمة الأمن السيبراني
٢
تعزيز الأمن السيبراني
Cybersecurity Defense
٣
صمود الأمن السيبراني
Cybersecurity Resilience
٤
الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية
Third-Party and Cloud Computing Cybersecurity

FIGURE 1: MAIN DOMAINS OF ECC

Let's explore each domain, detailing what it entails and its importance in strengthening overall cyber security efforts.

1. Cyber security governance

This domain is essential for building a strong cyber security foundation in organizations. It focuses on creating clear strategies and policies that outline how to manage cyber security effectively. Its main goal is to ensure that everyone knows their roles and responsibilities and that there are effective plans in place to handle risks and comply with cyber security standards.

By fostering a culture of security awareness and training, organizations can better protect themselves against cyber threats. Overall, this domain helps organizations create a structured approach to managing cyber security risks, leading to a more resilient security posture.

2. Cyber security defense

The cyber security defense domain within the NCA ECC–2:2024 framework is vital for enhancing an organization's security posture. Comprising 15 critical subdomains and 60 controls, this domain helps strengthen defenses against cyber threats.

It focuses on essential areas such as asset management, Identity and Access Management (IAM), network security, and cryptography. Additionally, it includes processes for identifying and managing vulnerabilities. By implementing robust defense strategies, organizations can protect their digital assets, control access to sensitive information, and mitigate potential risks.

3. Cyber security Resilience

The cyber security resilience domain is dedicated to enhancing an organization's capability to endure and recover from cyber security incidents. This domain emphasizes integrating cyber security resilience requirements into business continuity management. With a single subdomain focused on "Cyber Security Resilience Aspects of Business Continuity Management (BCM)," it includes four essential controls.

This will help organizations minimize cyber incidents' impact on critical systems, information processing facilities, and e-services.

By focusing on resilience, organizations can better prepare for disruptions, ensuring they can swiftly recover and maintain essential operations even when faced with cyber security challenges.

4. Third-party and cloud computing cyber security

The third-party and cloud computing cyber security domain focuses on enhancing organizations' defenses against cyber security risks that come from working with external partners and using cloud services.

This domain includes two important subdomains: "Third-Party Cyber Security" and "Cloud Computing and Hosting Cyber Security," which collectively feature eight essential controls. By addressing these areas, organizations can better manage risks associated with third-party collaborations and ensure the security of their cloud-based operations.

Automate your NCA ECC–2:2024 implementation with Cyber Arrow GRC

Organizations can now automate the implementation of NCA ECC-2:2024 with Cyber Arrow, simplifying the process of adapting to new updates and requirements. Say goodbye to manual spreadsheets and the hassle of identifying security controls across multiple systems.

With Cyber Arrow, you can:

Ongoing NCA ECC-2:2024 monitoring: Automatically gather evidence across 50+ integrations and utilize auditor-approved document templates.

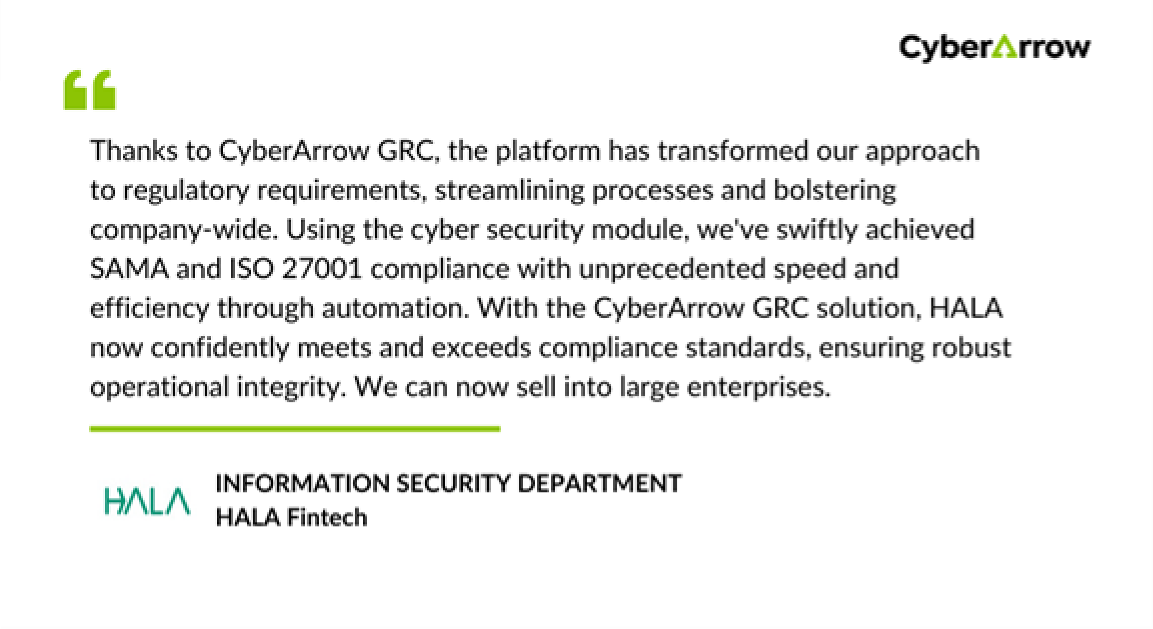
- **Security KPI monitoring:** Continuously assess your security posture and automate reporting for security control KPIs, allowing you to focus your time where it's truly needed.

- **Automated risk management:** Effortlessly manage risk assessments with pre-mapped controls and robust reporting dashboards.

- **Arabic language support:** Everything, from technical checks to documentation, is managed in both languages (English & Arabic).

Leverage Cyber Arrow's powerful features to ensure your organization meets NCA ECC-2:2024 requirements efficiently.

See what our clients say about Cyber Arrow GRC:



CyberArrow

"Thanks to CyberArrow GRC, the platform has transformed our approach to regulatory requirements, streamlining processes and bolstering company-wide. Using the cyber security module, we've swiftly achieved SAMA and ISO 27001 compliance with unprecedented speed and efficiency through automation. With the CyberArrow GRC solution, HALA now confidently meets and exceeds compliance standards, ensuring robust operational integrity. We can now sell into large enterprises.

HALA

INFORMATION SECURITY DEPARTMENT
HALA Fintech

Cybersecurity and National Security: The Role of NCA Compliance in Saudi Cybersecurity

Cybersecurity isn't just about protecting data; it's about safeguarding national security interests and economic prosperity. In Saudi Arabia, where Vision 2030 is driving digital transformation, cybersecurity compliance is more critical than ever. The National Cybersecurity Authority (NCA) is at the forefront of this effort, establishing regulations to ensure the security of critical infrastructure and sensitive data. Let's delve into the role of NCA compliance in Saudi cybersecurity and how it impacts businesses:

Role of NCA Compliance in Saudi Cybersecurity

NCA's Essential Cybersecurity Controls (ECC) set the standards for cybersecurity in Saudi Arabia. These controls cover various aspects, from data security to incident response, providing a comprehensive framework for safeguarding digital assets. Compliance with NCA regulations isn't just about avoiding penalties; it's about:

Protecting Critical Infrastructure:

Saudi Arabia's critical infrastructure, including energy grids and financial networks, relies on secure digital systems. NCA compliance ensures these systems are fortified against cyber threats, minimizing the risk of disruptions or attacks.

Safeguarding National Security:

Cyberattacks can have far-reaching consequences, impacting essential services and compromising sensitive information. NCA compliance helps mitigate these risks, contributing to the overall security and stability of the nation.

Building Trust in the Digital Economy:

In today's interconnected world, trust is paramount. NCA compliance demonstrates a commitment to cybersecurity, fostering trust in online transactions, e-commerce platforms, and government services. This trust is essential for attracting investment and driving economic growth.

Benefits of NCA Compliance for Businesses

Reduced Risk of Cyberattacks:

By implementing NCA's cybersecurity controls, organizations bolster their defenses, making them less vulnerable to cyber threats. This proactive approach reduces the likelihood of breaches or security incidents.

Enhanced Reputation:

NCA compliance isn't just about protecting data; it's about protecting trust. Demonstrating compliance signals to customers and partners that a business takes cybersecurity seriously, enhancing its reputation and credibility.

Improved Business Continuity:

A robust cybersecurity posture ensures that operations remain uninterrupted even in the face of cyber threats. By adhering to NCA regulations, businesses can minimize downtime and maintain continuity, safeguarding their productivity and profitability.

Competitive Advantage:

In today's digital landscape, cybersecurity is a differentiator. Businesses that priorities security gain a competitive edge, attracting partners and investors who value data protection and risk mitigation.

Challenges and Considerations

Staying Up-to-Date:

The cybersecurity landscape is dynamic, with new threats emerging regularly. NCA's regulations may evolve to address these threats, requiring businesses to stay informed and adapt their security strategies accordingly.

Integration with Existing Systems:

Implementing NCA controls may necessitate integrating new security tools and processes with existing IT infrastructure. This integration requires careful planning and resource allocation to ensure seamless operations.

Skilled Cybersecurity Workforce:

Building a skilled cybersecurity workforce is crucial for effective compliance. Businesses need trained professionals capable of implementing and managing NCA compliance measures effectively.

How Micro minder CS can Help:

In the context of ensuring NCA compliance and bolstering cybersecurity in Saudi Arabia, several Micro minder CS services would be invaluable for organizations:

1. **Cybersecurity Risk Assessments:** Micro minder offers comprehensive cybersecurity risk assessments that help organizations identify vulnerabilities and assess their current security posture. This service can assist businesses in understanding their compliance gaps concerning NCA regulations and implementing appropriate remediation measures.

2. **Compliance Services:** Micro minder provides tailored compliance services that align with NCA regulations and other cybersecurity frameworks. These services include assessing compliance readiness, developing compliance strategies, and implementing controls to meet regulatory requirements effectively.

3. **Cybersecurity Consultancy:** Micro minder's cybersecurity consultancy services offer expert guidance and advice on navigating the complexities of cybersecurity compliance. This includes interpreting NCA regulations, developing cybersecurity policies and procedures, and establishing effective cybersecurity governance structures.

4. **Outsourced DPO Services:** Micro minder offers outsourced Data Protection Officer (DPO) services, which can be particularly beneficial for organizations that lack the internal resources or expertise to fulfil this role effectively. A DPO plays a crucial role in ensuring compliance with data protection regulations like those mandated by NCA.

5. **Managed Security Services:** Micro minder's managed security services provide continuous monitoring, threat detection, and incident response capabilities, essential components of a robust cybersecurity strategy. By outsourcing these tasks to experts, organizations can enhance their cybersecurity posture and meet NCA compliance requirements more effectively.
Overall, Micro minder's suite of cybersecurity services offers comprehensive support for organizations seeking to achieve and maintain NCA compliance while strengthening their cybersecurity defenses to safeguard national security interests

FAQs

- What is NCA compliance, and why is it important?
- Who needs to comply with NCA regulations?
- What are the consequences of non-compliance with NCA regulations?
- How can organizations ensure NCA compliance?
- What are the common challenges faced by organizations in achieving NCA compliance?
- What is NCA compliance, and why is it important?

NCA compliance refers to adherence to the cybersecurity regulations established by the National Cybersecurity Authority (NCA) in Saudi Arabia. It's essential because it helps organizations protect critical infrastructure, sensitive data, and national security interests from cyber threats.

Lesson3 : What are the major ECC documents?

Your software is like a set of instructions for your device, consisting of thousands of lines of code. Sometimes, there are mistakes or weaknesses in these lines of code. Bad actors use these weaknesses to hack into your systems, similar to a burglar finding an open window. Is there a way to

Without cybersecurity, it’s hard for your company to keep your data, devices, networks, or systems safe from harmful attacks. A “cyber essentials” certification proves that your business has a formidable security posture and is trustworthy. Implementing cyber essential controls and staying on top of it is the way to go.

This article covers everything you need about cyber essentials and their benefits. We explain how cyber essentials work and outline the cyber essentials controls list.

Let’s dive in…

Table of Content

What are Cyber Essentials?

Cyber Essentials is a cybersecurity initiative implemented in 2014 by the government of the United Kingdom. The singular agenda of this is to offer basic cybersecurity for all organizations, big or small.

This certification helps businesses assure their customers that they prioritize securing IT assets and data against cyber-attacks. This, in turn, helps attract new business and foster relationships with trusted IT suppliers. Also, certain government contracts necessitate Cyber Essentials certification, and in this age of trust-less commerce, one you must stay ahead.

It is designed to be a starting point that introduces businesses to the essentials of cybersecurity principles and paves the path for adequate cybersecurity measures.

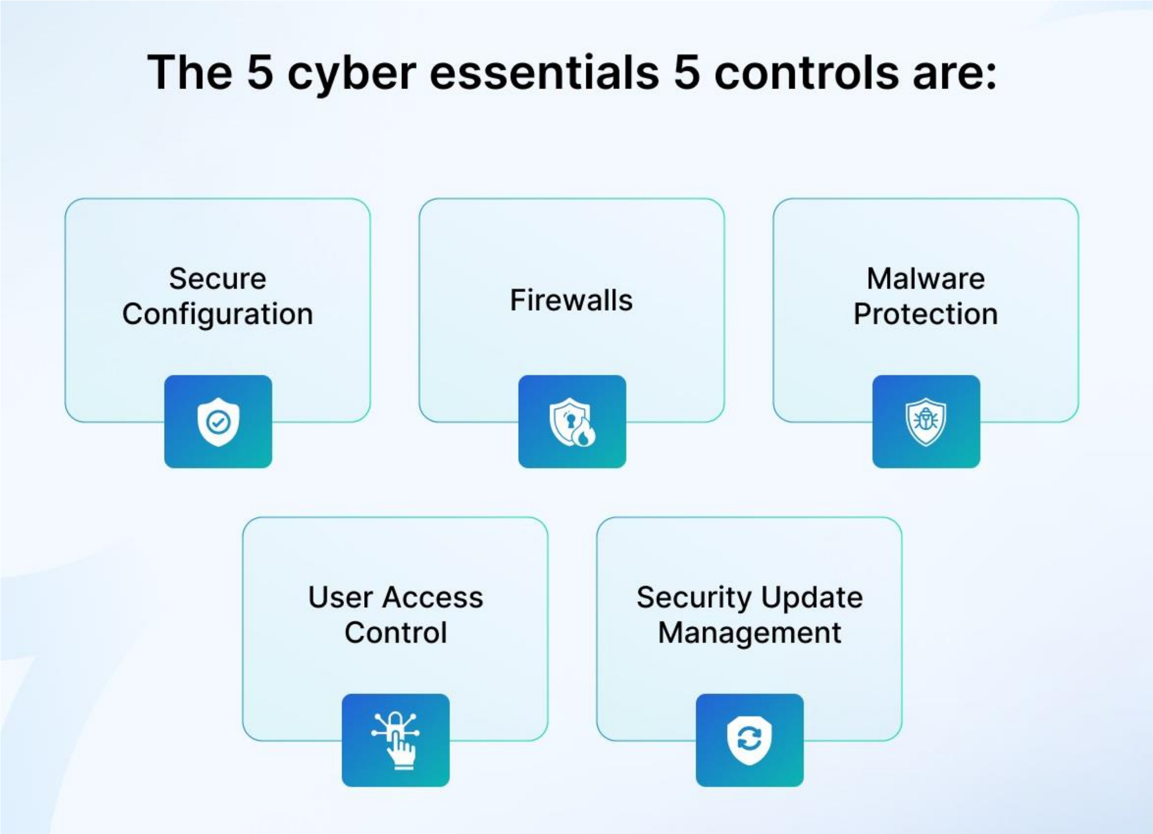
The essential cybersecurity controls list guides businesses through the technical and administrative controls listed in the initiative and their implementation process. Also, it hands out a baseline certification to show that companies are dead serious about keeping things secure.

5 Cyber Essentials Controls List

Cyber Essentials controls consist of five main essential controls, each with unique characteristics and requirements demands that must be addressed.

The 5 cyber essentials controls are:

- Firewalls
- Secure Configuration
- User Access Control
- Malware Protection
- Security Update Management



The 5 cyber essentials 5 controls are:

Secure Configuration

Firewalls

Malware Protection

User Access Control

Security Update Management

1. Firewalls

Firewalls have been around for more than 25 years, serving diligently as the first defense in network security. A software firewall is a physical security guard that checks your incoming and outgoing traffic to decide what to allow or block based on the given security rules.

Now, your company should regularly do a few things to improve the software firewall protection:

- Change any default passwords to strong passwords
- Disable remote administrative access if you don’t need it in your cloud services

- Only let people access the administrative part from the internet if there’s a good reason, and make sure it’s protected by a second multi-factor authentication factor or an IP whitelist that limits access to trusted addresses
- And as a rule of thumb, block any connections that aren’t authenticated

2. Security update management

In the Cyber Essentials scheme, patch management is one of the requirements that help keep your devices and software safeguarded from security vulnerabilities. This includes a sweep of activities within your infrastructure management:

- IT admins or managers must identify patching needs based on the severity of security issues
- Once identified, patches or fixes are obtained and tested to ensure they address the vulnerabilities without causing any adverse effects
- Successful patches are then deployed to improve existing device code

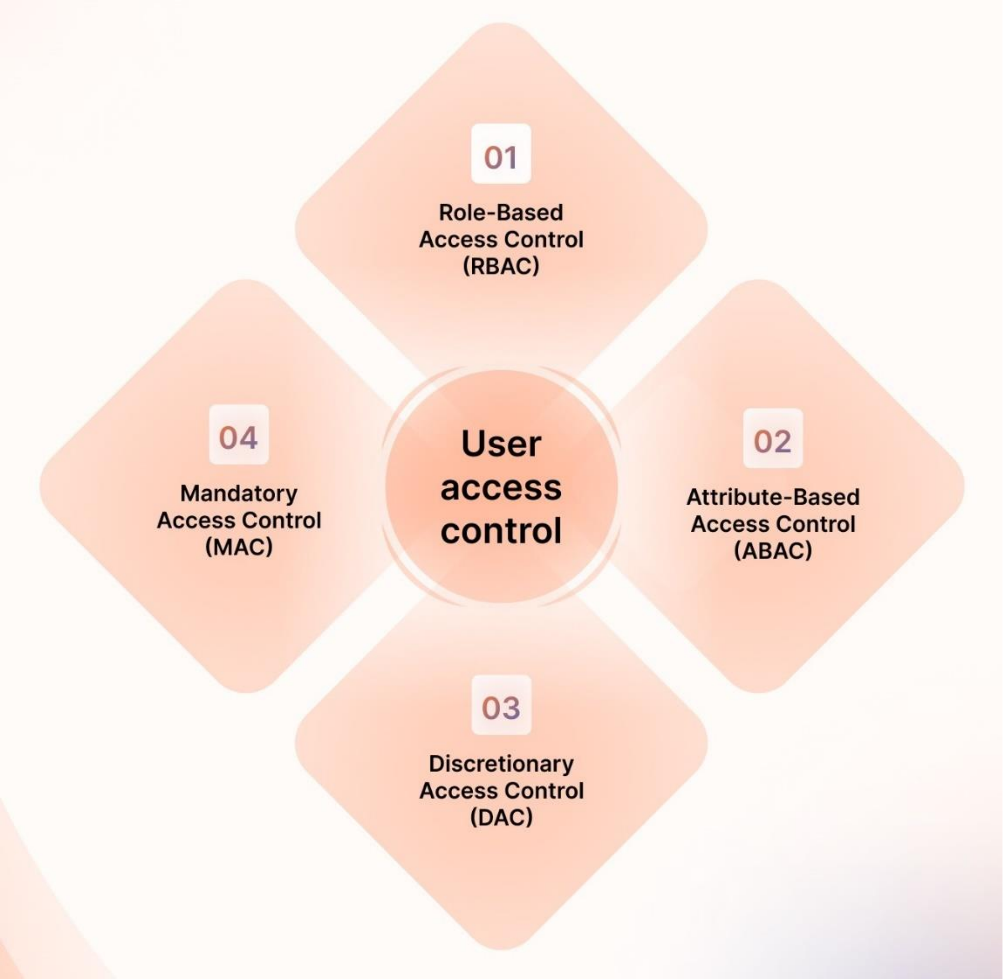
For effective security update management:

- Remove old, unsupported software from devices or prevent it from connecting to the internet
- Apply ‘critical’ or ‘high-risk’ updates within 14 days of release
- Enable automatic updates whenever possible
- Ensure that all software on devices is licensed and actively supported by the supplier
- Apply updates promptly for vulnerabilities with a CVSS v3 score of 7 or above or in the absence of severity information from the supplier

3. User access control

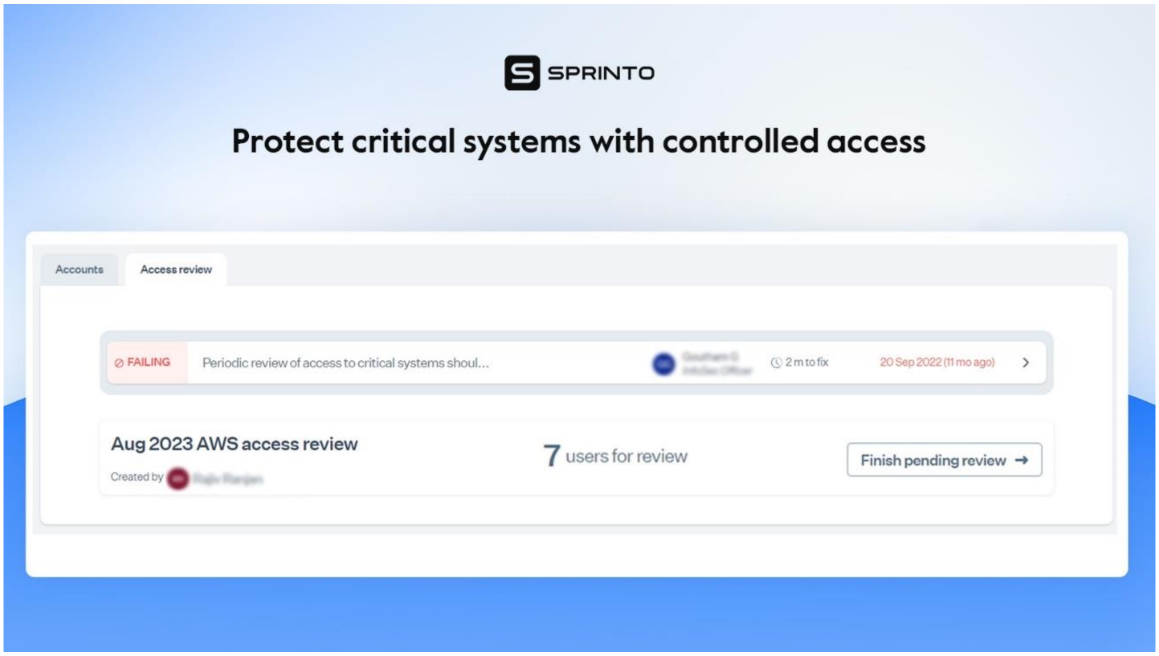
The other control that is very important to add is User access control this helps in ensuring the safety of your data and external services. This will restrict special access privileges, so no unauthorized people such as hackers.

You can choose the four main access control types based on your security and compliance needs:


01
Role-Based Access Control (RBAC)
02
Attribute-Based Access Control (ABAC)
User access control
03
Discretionary Access Control (DAC)
04
Mandatory Access Control (MAC)

- Role-Based Access Control (RBAC): It is also aimed at users having access only to the relevant data based on their roles in an organization.
- Attribute-Based Access Control (ABAC): different attributes and conditions are used in determining access.
- Discretionary Access Control (DAC): It is an open approach where access depends on the owner or admin
- Mandatory Access Control (MAC): Access rights at various security levels are managed by a central authority in non-discretionary ways.

Or, you might use Sprinto along with user access and technical controls.



SPRINTO

Protect critical systems with controlled access

Sprinto smoothly combines with ACLs and does more than work in favor of role-based access controls. It allows you to specify certain individuals for every role, automates the circulation of these policy documents and makes sure that they are followed through acknowledgments. Hiring evaluations and off boarding are easier to manage so that ACLs can be accurately implemented.

When it comes to compliance, Sprinto stands out as the #1 rated tool on G2 in its category, boasting a 100% audit success rate. Using Sprinto with ACLs, you can establish a great approach to cyber essentials key controls, policy enforcement, and continuous monitoring for airtight security.

4. Malware Protection

Malware is a blend of “malicious software” that poses various cyber threats like viruses, worms, Trojans, and spyware. These harmful programs are created in a way that infects your computer and causes harm in horrific ways.

One of the biggest security risks is cybercriminals stealing your users’ confidential information, especially online banking details, which they can exploit to drain their accounts or create fraudulent credit card bills.

This is why Cyber Essentials lays down rules to minimize the risk of malware :

- Use reliable anti-malware software to detect and remove cybersecurity risk programs actively
- Employ cyber security measures that block connections to malicious websites, reducing the risk of encountering harmful content
- Regularly update your software, ensuring that signature files are updated at least daily to defend against the latest cyber threats
- Configure your software to automatically scan files upon access, including those downloaded, opened, or accessed from network connections

- Ensure that your software scans web pages automatically when you access through a web browser, which adds an extra layer of protection

5. Secure Configuration

Insecure configurations are common pitfalls that criminal hackers exploit. And this is why secure configurations of web and application servers are an important requirement under Cyber Essentials. Failure to manage proper configurations properly can result in various security issues.

So, to improve your security regulations for computers and network devices, you should follow these routine practices :

- Make sure to review and eliminate unnecessary user accounts to minimize potential points of unauthorized access regularly (This has to be done regularly)
- Improve your security settings by removing any unnecessary software (This will reduce your attack surface and potential vulnerabilities)
- Change default or easily guessable account passwords to more complex and less predictable options
- Put your security first by authenticating users before granting Internet-based access to commercially or personally sensitive data
- Disable auto-run features that allow file execution without user authorization, preventing unauthorized access

How can Sprinto's reusable automation help?

Cyber Essentials certification is a need of the hour for your business' overall functionality. And achieving it is straightforward, with the right IT infrastructure maintenance suite. That said, often, businesses are required to deploy near-similar processes over and over for different requirements.

With Sprinto's reusable nodes, processes and functions can be reused without needing fresh implementation processes. This seamless functionality helps businesses save time and cost and is hassle-free.

Leveraging Sprinto's security compliance automation platform helps you automate the repetitive and time-consuming manual activities in setting the foundation while laying the path for future compliance regulatory laws and global compliance frameworks(ISO 27001, SOC 2, HIPAA, GDPR, PCI DSS).

You can use Sprinto for implementing technical controls, running checks, triggering workflows, and real-time compliance monitoring. You can also stay proactive in audits to ensure nothing slips through the cracks.

Upon signing up with Sprinto, you can access :

- A full-stack, automation-first compliance management platform that will scale with your business in no time

- Built-in and customizable compliance programs that align with your audit objectives and business goals
- Get access to on-demand expert advisory to help you move swiftly
- A trusted network of legal advisors, tooling vendors, and security auditors to complete the compliance loop
- Full access to continuous control monitoring

FAQs

1. Is Cyber Essentials Mandatory?

No, Cyber Essentials certification is not mandatory. It's a voluntary program guiding your security efforts, whether already in place or yet to be implemented. However, note that some government contracts may require this certification.

2. What does the certification process for Cyber Essentials look like?

The Cyber Essentials certification process comes in two types. The regular process starts with a simple self-assessment questionnaire. Cyber Essentials Plus involves a more technical and challenging test, including a vulnerability assessment.

3. What is the difference between Cyber Essentials and Cyber Essentials Plus?

The key difference lies in Cyber Essentials Plus going a step further with a technical audit of your IT systems, ensuring cyber security controls are in place for added compliance assurance. The pass bar is set slightly higher for Cyber Essentials Plus.

4. Does your business need Cyber Essentials?

The decision is yours. Cyber Essentials is a starting point to keep your security in check, providing a robust foundation to safeguard your systems against generic attacks and well-known external threats.

Unit Two : ECC and GRC

At the end of the unit, the trainee will be able to:

- To identify the features of cybersecurity controls

- To mention the importance of basic cybersecurity controls

- To explain governance and risk management

- To show the importance of governance for companies

Lesson1 : ECC

Essential Cybersecurity Controls (ECC-1:2018)

The Kingdom of Saudi Arabia is living now in a mutation of the level of the use of Information Technology and Digital Transformation in institutions and companies, and it is so obvious when looking at the huge and massive government investment in information technology. However, this technology may have risks that could lead to threats and shake the national security if the control is lost as a result of a breach or problem with a component of cyberspace.

The National Cybersecurity Authority NCA has developed and launched the Essential Cybersecurity Controls (ECC-1-2018) to avoid disasters that may results from cyber risks and to define the minimum requirements of cybersecurity in the national institutions that fall under the scope of implementation of these controls.

All national authorities must raise and improve their cybersecurity level to protect their networks, systems, and electronic data and comply to the national cybersecurity authority (NCA) policies, frameworks, standards, controls, and guidelines in this regard.

What are Essential Cybersecurity Controls?

They are organized practices and frameworks developed by national and international organizational authorities and they are containing of measures and countermeasures that institutions must to implement for discovering, preventing, or facing security risks that target the technology and information assets.

The Features of Essential Cybersecurity Controls

ECC-1-2018 are characterized by:

1. Focuses on the protection of key objectives, which are: confidentiality, integrity, and availability of information.

2. They’re built based on the best practices, standards, and organizational frameworks (international and local).

3. These controls give great interest to the pillars that cybersecurity focuses on (Strategy, people, procedures, and technology).

Importance of Essential Cybersecurity Controls

Regardless to the mandatory of implementing essential cybersecurity controls (ECC-1-2018) for some entities, they provide many benefits to the other organizations, and we mention some of them:

1. Assist in designing the cyber security strategy and the organization.
2. Ensure compliance from the tip manager of implementing and managing cybersecurity programs.
3. Determining and documenting the organizational structure, roles, and responsibilities of cybersecurity within the organization.
4. Editing, applying and reviewing cybersecurity policies and procedures.
5. Achieve the national legislative and organizational requirements that related to cybersecurity.
6. Processing cybersecurity risks that related to human resources.
7. Protecting the organization's information and technology assets from cybersecurity external and Internet the risks and threats.
8. Discover the technical vulnerabilities in the right time, and process them effectively.
9. Processing cybersecurity risks and the implementation of cybersecurity requirements for cloud computing and hosting appropriately and effectively.

The scope of Essential Cybersecurity Controls (ECC-1-2018)

These controls are prepared to fit the needs of cybersecurity in all organizations and sectors regardless to the business type and size. But these controls are specially implemented in the national organizations on the Kingdom of Saudi Arabia, and they include:

1. All ministries, authorities, and the national companies, industries, and establishments and their affiliates.
2. Private sector companies that provide their services to the national authorities.
3. Companies and organizations that operate and host the critical national infrastructure (CNI).
4. Other organizations can benefit of these controls, even if compliance is not necessary.

Notice: All organizations within the scope of work of essential cybersecurity controls (ECC-1-2018) must implement what's achieve permanent and continuous compliance with these controls.

And the National Cybersecurity Authority (NCA) evaluates the range of compliance of the national authorities of these controls.

How can Renad AL Majed for Information Technology (RMG) company helps you?

our special services design according to the Essential Cybersecurity Controls to help you to assure your institution while achieving compliance to the national legislation at the same time, some of our services are:

1. Make Gap analysis and maturity assessment.
2. Implementing the appropriate essential controls to your institution.
3. Design and develop a cybersecurity strategy
4. Designing And developing cybersecurity policies and the procedures.
5. Providing training programs, transferring knowledge, and raising the awareness of the human factor.
6. Document review and internal audit.

Why do you choose Renad AL Majed for information technology company (RMG)?

- Would you ask Renad AL Majed services, you are allowed do benefit from more than 60 experts and consultants to improve and develop your business.
- The company is characterized by flexibility, the accuracy of implementation and showing results quickly, Because of the company awareness to the deep dimensions of the pillars and indicators that mentioned in these controls.
- The company has an expert in implementing a vulnerability assessment.
- Long experience in implementing a penetration test.
- The company has an operations center works 24/ 7.
- The company's ability to cover all cybersecurity fields, where the company has a previous business in digital transformation, governance, business continuity, ISO standards and Backup, data recovery, and network security.

Frequently asked questions (FAQ)

Does not implementing the requirements of Essential cyberse**curity cont**rols (ECC-1-2018) expose the entity to legal accountability ?

What does it take for my organization to implement and comply with Essential Cybersecurity Controls ?

How can I get started with Renad AL Majed for information technology (RMG) company ?

Saudi Arabia Essential Cybersecurity Controls (ECC)

The Kingdom of Saudi Arabia, as part of the Saudi Vision 2030, has developed and promulgated the Essential Cybersecurity Controls (ECC). These measures aim to help government and government-affiliated organizations enhance their cybersecurity posture.

Thales can help your organization comply with the Kingdom's ECC.

The Kingdom of Saudi Arabia, as part of the Saudi Vision 2030, has developed and promulgated the Essential Cybersecurity Controls (ECC). These measures aim to help government and government-affiliated organizations enhance their cybersecurity posture.

Thales can help your organization comply with the Kingdom's ECC.

Thales' guide to Saudi Arabia ECC

The development of the ECCs is a crucial and vital step towards increasing the cybersecurity posture of the Kingdom of Saudi Arabia. Organizations subject to the Controls can take advantage of top-level industry solutions and use existing frameworks such as the NIST Cybersecurity Framework as guidelines.

Thales, a global leader in cybersecurity solutions and services, can help the Saudi Arabian organizations become compliant with the Essential Cybersecurity Controls.

Cybersecurity Governance Domain

Thales offers a variety of data protection professional services designed to help you effectively take your investment and ensure a successfully deployment. These services include:

- Best practices and awareness workshops for learning about the latest security trends and practices, managing governance risk and compliance and implementing data protection
- Strategy and design for identifying stakeholders and assigning roles and responsibilities
- Implementation and operations such as on-site product training, installation and customization of Thales products.
- Assessment to help your organization prepare for upcoming security audits while reviewing existing environment and business needs.

Best practice security solutions

Best practice for securing the integrity and confidentiality of sensitive data against loss, damage, unauthorized destruction, and unlawful access is strong access management and authentication combined with transparent encryption, integrated cryptographic key management, and security intelligence. Thales provides the following solutions to help organizations comply with Saudi Arabia's Essential Cybersecurity Controls.

Data discovery and classification

The first step in protecting sensitive data is finding the data wherever it is in the organization, classifying it as sensitive, and typing it (e.g. PII, financial, IP, HHI, customer-confidential, etc.) so you can apply the most appropriate data protection techniques. It is also important to monitor and assess data regularly to ensure new data isn't overlooked and your organization does not fall out of compliance.

Thales' Cipher Trust Data Discovery and Classification efficiently identifies structured as well as unstructured sensitive data on-premises and in the cloud. Supporting both agentless and agent-based deployment models, the solution provides built-in templates that enable rapid identification of regulated data, highlight security risks, and help you uncover compliance gaps. A streamlined workflow exposes security blind spots and reduces remediation time. Detailed reporting supports compliance programs and facilitates executive communication.

Protection of sensitive data at rest

Separation of privileged access users and sensitive user data

With the Cipher Trust Data Security Platform, administrators can create strong separation of duties between privileged administrators and data owners. Cipher Trust Transparent Encryption encrypts files, while leaving their metadata in the clear. In this way, IT administrators - including hypervisor, cloud, storage, and server administrators - can perform their system administration tasks, without being able to gain privileged access to the sensitive data residing on the systems they manage.

Separation of administrative duties

Strong separation of duties policies can be enforced to ensure one administrator does not have complete control over data security activities, encryption keys, or administration. In addition, the Cipher Trust Manager supports two-factor authentication for administrative access.

Granular privileged access controls

The Cipher Trust Data Security Platform can enforce very granular, least-privileged-user access management policies, enabling protection of data from misuse by privileged users and APT attacks. Granular privileged-user-access management policies can be applied by user, process, file type, time of day, and other parameters. Enforcement options can control not only permission to access clear-text data, but what file-system commands are available to a user.

Strong access management and authentication

Thales Access Management and Authentication solutions provide both the security mechanisms and reporting capabilities organizations need to comply with data security regulations. Our solutions protect sensitive data by enforcing the appropriate access controls when users log into applications that store sensitive data. By supporting a broad range of authentication methods and policy driven role-based access, our solutions help enterprises mitigate the risk of data breach due to compromised or stolen credentials or through insider credential abuse.

Support for smart single sign on and step-up authentication allows organizations to optimize convenience for end users, ensuring they only have to authenticate when needed. Extensive reporting allows businesses to produce a detailed audit trail of all access and authentication events, ensuring they can prove compliance with a broad range of regulations.

Protection of Sensitive Data in Motion

Thales High Speed Encryptors (HSEs) provide network independent data-in-motion encryption (Layers 2,3 and 4) ensuring data is secure as it moves from site-to-site, or from on-premises to the cloud and back. Our HSE solutions allow customers to better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception-all at an affordable cost and without performance compromise.

10 Essential Cybersecurity Controls

Cyber incidents-including data breaches, ransomware attacks, and social engineering scams-have become increasingly prevalent, impacting organizations of all sizes and industries. Such incidents have largely been brought on by additional cyber threat vectors and growing attacker sophistication. As these incidents continue to rise in both cost and frequency, organizations must take steps to address their cyber exposures and bolster their digital security defenses.

Doing so not only helps organizations prevent cyber incidents and associated insurance claims from happening but can also help them secure adequate cyber coverage in the first place. After all, the heightened severity of cyber incidents has motivated most cyber insurers to increase their premiums and be more selective regarding which organizations they will insure and the types of losses they will cover. As such, many underwriters have begun leveraging organizations' documented cybersecurity practices to determine whether they qualify for coverage-a new policy or a renewal-and how expensive their premiums will be.

With this in mind, here are ten essential cybersecurity controls that organizations can implement to help manage their cyber exposures.

1. Multifactor Authentication (MFA)

While complex passwords can help deter cybercriminals, they can still be cracked. To help prevent cybercriminals from gaining access to employees' accounts and using such access to launch potential attacks, MFA is key. MFA is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify their identity for login. Through MFA, employees must confirm their identities by providing extra information (e.g., a phone number or unique security code) in addition to their passwords when attempting to access corporate applications, networks, and servers.

This additional login hurdle means that cybercriminals won't be able to easily unlock accounts, even if they have employees' passwords in hand. It's best practice for organizations to enable MFA for remote access to their networks, the administrative functions within their networks, and any enterprise-level cloud applications.

2. Endpoint Detection and Response (EDR) Solutions

EDR solutions continuously monitor security-related threat information to detect and respond to ransomware and other kinds of malware. They provide visibility into security incidents occurring on various endpoints-such as smartphones, desktop computers, laptops, servers, tablets, and other devices that communicate back and forth with the networks in which they are connected-to help prevent digital damage and minimize future attacks.

Specifically, EDR solutions offer advanced threat detection, investigation, and response capabilities-including incident data search and investigation triage, suspicious activity validation, threat hunting, and malicious activity detection and containment-by constantly analyzing events from endpoints to identify suspicious activity. Further, these solutions provide continuous and comprehensive visibility into what is happening in real-time by recording activities and events taking place on all endpoints and workloads. Upon receiving alerts regarding possible threats, organizations and their IT departments can uncover, investigate and remediate related issues.

As a whole, implementing EDR solutions is a critical step in helping organizations enhance their network visibility, conduct more efficient cybersecurity investigations, leverage automated remediation amid potential incidents, and promote more contextualized threat hunting through ongoing endpoint data analysis.

3. Patch Management

Patches modify operating systems and software to enhance security, fix bugs, and improve performance. They are created by vendors and address key vulnerabilities cybercriminals may target. Patch management refers to the process of acquiring and applying software updates to a variety of endpoints.

The patch management process can be carried out by organizations' IT departments, automated patch management tools, or a combination of both. The patch management process includes identifying IT assets and their locations, assessing critical systems and vulnerabilities, testing and applying patches, tracking progress, and maintaining records of such progress. Patch management is necessary to ensure overall system security, maintain compliance with applicable software standards set by regulatory bodies and government agencies, leverage system features and functionality improvements that may become available over time, and decrease downtime that could result from outdated, inefficient software.

A consistent approach to patching and updating software and operating systems from a cybersecurity standpoint helps limit exposure to cyber threats. Accordingly, organizations should establish patch management plans that include frameworks for prioritizing, testing, and deploying software updates.

4. Network Segmentation and Segregation

When organizations' networks lack sufficient access restrictions and are closely interconnected, cybercriminals can easily hack into such networks and cause more widespread operational disruptions and damage. That's where network segmentation and segregation can help.

Network segmentation refers to dividing larger networks into smaller segments (also called subnetworks) through switches and routers, permitting organizations to better monitor and control traffic flow between these segments. Such segmentation may also boost network performance and help organizations localize technical issues and security threats. Network segregation, on the other hand, entails isolating crucial networks (i.e., those containing sensitive data and resources) from external networks, such as the internet. Such segregation allows organizations to leverage additional security protocols and access restrictions within their most critical networks, making it more difficult for cybercriminals to penetrate these networks laterally.

Both network segmentation and segregation allow organizations to take a granular approach to cybersecurity, limiting the risk of cybercriminals gaining expansive access to their IT infrastructures (and the vital assets within them) and causing significant losses. When implementing network segmentation and segregation, organizations must uphold the principle of least privilege-only allowing employees access to the networks they need to perform their job duties-and separate hosts from networks based on critical business functions to ensure maximum infrastructure visibility.

5. End-of-Life (EOL) Software Management

At some point, all software will reach the end of its life. This means manufacturers will no longer develop or service these products, discontinuing technical support, upgrades, bug fixes, and security improvements. As a result, EOL software will have vulnerabilities that cybercriminals can easily exploit.

Organizations may be hesitant to transition away from EOL software for several reasons, such as limited resources, a lack of critical features among new software, or migration challenges. This is especially true when EOL systems are still functioning. However, continuing to use EOL software also comes with many risks, including heightened cybersecurity exposures, technology incompatibilities, reduced system performance levels, elevated operating costs, and additional data compliance concerns.

As such, it's clear that proactive EOL software management is necessary to prevent unwelcome surprises and maintain organizational cybersecurity. In particular, organizations should adopt life cycle management plans that outline ways to introduce new software and provide methods for phasing out unsupported software; utilize device management tools to push software updates, certifications, and other necessary upgrades to numerous devices simultaneously; and review the EOL status of new software before selecting it for current use to avoid any confusion regarding when it will no longer be supported and plan for replacements as needed.

6. Remote Desk Protocol (RDP) Safeguards

RDP-a network communications protocol developed by Microsoft-consists of a digital interface that allows users to connect remotely to other servers or devices. Users can easily access and operate these servers or devices through RDP ports from any location. RDP has become an increasingly useful business tool—permitting employees to retrieve files and applications stored on their organizations' networks while working from home and allowing IT departments to identify and fix employees' technical problems remotely.

Unfortunately, RDP ports are also frequently leveraged as a vector for launching ransomware attacks, particularly when these ports are left exposed to the internet. In fact, a recent report from Kaspersky found that nearly 1.3 million RDP-based cyber events occur each day, with RDP reigning as the top attack vector for ransomware incidents. To safeguard their RDP ports, organizations need to keep these ports turned off whenever they aren't in use, ensure such ports aren't left open to the internet, and promote overall interface security through the use of a virtual private connection (VPN) and MFA.

7. Email Authentication Technology/Sender Policy Framework (SPF)

Many ransomware attacks and social engineering scams start with employees receiving deceiving emails, such as those from fraudulent senders claiming to be trustworthy parties and providing malicious attachments or asking for sensitive information. To protect against potentially harmful emails, it's paramount that organizations utilize email authentication technology.

This technology monitors incoming emails and determines the validity of these messages based on specific sender verification standards that organizations have in place. Organizations can choose from several different verification standards, but the most common is SPF-which focuses on verifying senders' IP addresses and domains.

Upon authenticating emails, this technology permits them to pass through organizations' IT infrastructures and into employees' inboxes. When emails can't be authenticated, they will either appear as flagged in employees' inboxes or get blocked from reaching inboxes altogether. With SPF, unauthenticated emails may be filtered directly into employees' spam folders. Ultimately, email authentication technology can make all the difference in keeping dangerous emails out of employees' inboxes and stopping cybercriminals' tactics before they can begin.

8. Secure Data Backups

One of the best ways for organizations to protect their sensitive information and data from cybercriminals is by conducting frequent and secure backups. First and foremost, organizations should determine safe locations to store critical data, whether within cloud-based applications, on-site hard drives, or external data centers. From there, organizations should establish concrete schedules for backing up this information and outline data recovery procedures to ensure swift restoration amid possible cyber events.

9. Incident Response Planning

Cyber incident response plans can help organizations establish protocols for detecting and containing digital threats, remaining operational and mitigating losses promptly amid cyber events. Successful incident response plans should outline potential attack scenarios, ways to identify signs of such scenarios, methods for maintaining or restoring key functions during these scenarios, and the individuals responsible for doing so.

These plans should be routinely reviewed through various activities, such as penetration testing and tabletop exercises, to ensure effectiveness and identify ongoing security gaps. Penetration testing refers to the simulation of actual attacks that target specific workplace technology or digital assets (e.g., websites, applications, and software) to analyze organizations' cybersecurity strengths and weaknesses. In contrast, tabletop exercises are drills that allow organizations to utilize mock scenarios to walk through and test the efficiency of their cyber incident response plans. Based on the results of these activities, organizations should adjust their response plans when necessary.

10. Employee Training

Employees are widely considered organizations' first line of defense against cyber incidents, especially since all it takes is one staff mistake to compromise and wreak havoc on an entire workplace system. In light of this, organizations must offer cybersecurity training. This training should center around helping employees properly identify and respond to common cyber threats. Additional training topics may include organizations' specific cybersecurity policies and methods for reporting suspicious activities.

Because digital risks are everchanging, this training shouldn't be a standalone occurrence. Rather, organizations should provide cybersecurity training regularly and update this training when needed to reflect the latest threats, attack trends, and workplace changes.

Conclusion

In today's evolving digital risk landscape, it's vital for organizations to take cybersecurity seriously and utilize effective measures to decrease their exposures. By leveraging proper cybersecurity controls, organizations can help safeguard their operations from a wide range of losses and reduce the likelihood of related insurance claims. Furthermore, documenting these controls can allow organizations to demonstrate to cyber insurers that they consider cybersecurity a top priority, potentially increasing their ability to secure coverage.

For more risk management guidance, **contact Bates Hewett & Floyd today.**

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice. © 2022 Zywave, Inc. All rights reserved.

Lesson2 : GRC

What is GRC?

Governance, Risk, and Compliance (GRC) is a structured way to align IT with business goals while managing risks and meeting all industry and government regulations. It includes tools and processes to unify an organization's governance and risk management with its technological innovation and adoption. Companies use GRC to achieve organizational goals reliably, remove uncertainty, and meet compliance requirements.

What does GRC stand for?

GRC stands for governance, risk (management), and compliance. Most businesses are familiar with these terms but have practiced them separately in the past. GRC combines governance, risk management, and compliance in one coordinated model. This helps your company reduce wastage, increase efficiency, reduce noncompliance risk, and share information more effectively.

Governance

Governance is the set of policies, rules, or frameworks that a company uses to achieve its business goals. It defines the responsibilities of key stakeholders, such as the board of directors and senior management. For example, good corporate governance supports your team in including the company's social responsibility policy in their plans.

Good governance includes the following :

- Ethics and accountability
- Transparent information sharing
- Conflict resolution policies
- Resource management

Risk management

Businesses face different types of risks, including financial, legal, strategic, and security risks. Proper risk management helps businesses identify these risks and find ways to remediate any that are found. Companies use an enterprise risk management program to predict potential problems and minimize losses. For example, you can use risk assessment to find security loopholes in your computer system and apply a fix.

Compliance

Compliance is the act of following rules, laws, and regulations. It applies to legal and regulatory requirements set by industrial bodies and also for internal corporate policies. In GRC, compliance involves implementing procedures to ensure that business activities comply with the respective regulations. For example, healthcare organizations must comply with laws like HIPAA that protect patients' privacy.

Why is GRC important?

By implementing GRC programs, businesses can make better decisions in a risk-aware environment. An effective GRC program helps key stakeholders set policies from a shared perspective and comply with regulatory requirements. With GRC, the entire company comes together in its policies, decisions, and actions.

The following are some benefits of implementing a GRC strategy at your organization.

Data-driven decision-making

You can make data-driven decisions within a shorter time frame by monitoring your resources, setting up rules or frameworks, and using GRC software and tools.

Responsible operations

GRC streamlines operations around a common culture that promotes ethical values and creates a healthy environment for growth. It guides strong organizational culture development and ethical decision-making in the organization.

Improved cybersecurity

With an integrated GRC approach, businesses can employ data security measures to protect customer data and private information. Implementing a GRC strategy is essential for your organization due to increasing cyber risk that threatens users' data and privacy. It helps organizations comply with data privacy regulations like the General Data Protection Regulation (GDPR). With a GRC IT strategy, you build customer trust and protect your business from penalties.

What drives GRC implementation?

Companies of all sizes face challenges that can endanger revenue, reputation, and customer and stakeholder interest. Some of these challenges include the following :

- Internet connectivity introducing cyber risks that might compromise data storage security
- Businesses needing to comply with new or updated regulatory requirements
- Companies needing data privacy and protection
- Companies facing more uncertainties in the modern business landscape
- Risk management costs increasing at an unprecedented rate
- Complex third-party business relationships increasing risk

These challenges create demand for a strategy to navigate businesses toward their goals. Conventional third-party risk management and regulatory compliance methods are not enough. Hence, GRC was introduced as a unified approach to help stakeholders make accurate decisions.

How does GRC work?

GRC in any organization works on the following principles:

Key stakeholders

GRC requires cross-functional collaboration across different departments that practices governance, risk management, and regulatory compliance. Some examples include the following:

- Senior executives who assess risks when making strategic decisions
- Legal teams who help businesses mitigate legal exposures
- Finance managers who support compliance with regulatory requirements
- HR executives who deal with confidential recruitment information
- IT departments that protect data from cyber threats

GRC framework

A GRC framework is a model for managing governance and compliance risk in a company. It involves identifying the key policies that can drive the company toward its goals. By adopting a GRC framework, you can take a proactive approach to mitigating risks, making well-informed decisions, and ensuring business continuity.

Companies implement GRC by adopting GRC frameworks that contain key policies that align with the organization's strategic objectives. Key stakeholders base their work on a shared understanding from the GRC framework as they devise policies, structure workflows, and govern the company. Companies might use software and tools to coordinate and monitor the success of the GRC framework.

GRC maturity

GRC maturity is the level of integration of governance, risk assessment, and compliance within an organization. You achieve a high level of GRC maturity when a well-planned GRC strategy results in cost efficiency, productivity, and effectiveness in risk mitigation. Meanwhile, a low level of GRC maturity is unproductive and keeps business units working in silos.

How does GRC work?

GRC in any organization works on the following principles:

Key stakeholders

GRC requires cross-functional collaboration across different departments that practices governance, risk management, and regulatory compliance. Some examples include the following:

- Senior executives who assess risks when making strategic decisions
- Legal teams who help businesses mitigate legal exposures
- Finance managers who support compliance with regulatory requirements
- HR executives who deal with confidential recruitment information
- IT departments that protect data from cyber threats

GRC framework

A GRC framework is a model for managing governance and compliance risk in a company. It involves identifying the key policies that can drive the company toward its goals. By adopting a GRC framework, you can take a proactive approach to mitigating risks, making well-informed decisions, and ensuring business continuity.

Companies implement GRC by adopting GRC frameworks that contain key policies that align with the organization's strategic objectives. Key stakeholders base their work on a shared understanding from the GRC framework as they devise policies, structure workflows, and govern the company. Companies might use software and tools to coordinate and monitor the success of the GRC framework.

GRC maturity

GRC maturity is the level of integration of governance, risk assessment, and compliance within an organization. You achieve a high level of GRC maturity when a well-planned GRC strategy results in cost efficiency, productivity, and effectiveness in risk mitigation. Meanwhile, a low level of GRC maturity is unproductive and keeps business units working in silos.

What is the GRC Capability Model ?

The GRC Capability Model contains guidelines that help companies implement GRC and achieve principled performance. It ensures a common understanding of communication, policies, and training. You can take a cohesive and structured approach to incorporate GRC operations across your organization.

Learn

You learn about the context, values, and culture of your company so you can define strategies and actions that reliably achieve objectives.

Align

Ensure that your strategy, actions, and objectives are in alignment. You do so by considering opportunities, threats, values, and requirements when making decisions.

Perform

GRC encourages you to take actions that bring results, avoid those that hinder goals, and monitor your operations to detect sudden changes.

Review

You revisit your strategy and actions to ensure they align with the business goals. For example, regulatory changes could require a change of approach.

What are common GRC tools?

GRC tools are software applications that businesses can use to manage policies, assess risk, control user access, and streamline compliance. You might use some of the following GRC tools to integrate business processes, reduce costs, and improve efficiency.

GRC software

GRC software helps automate GRC frameworks by using computer systems. Businesses use GRC software to perform these tasks:

- Oversee policies, manage risk, and ensure compliance
- Stay updated about various regulatory changes that affect the business
- Empower multiple business units to work together on a single platform
- Simplify and increase the accuracy of internal auditing

You can also combine GRC frameworks on one platform. For example, you can use AWS Cloud Operations to govern cloud and on-premises resources.

User management

You can give various stakeholders the right to access company resources with user management software. This software supports granular authorization, so you can precisely control who has access to what information. User management ensures that everyone can securely access the resources they need to get their work done.

Security information and event management

You can use security information and event management (SIEM) software to detect potential cybersecurity threats. IT teams use SIEM software like AWS CloudTrail to close security gaps and comply with privacy regulations.

Auditing

You can use auditing tools like AWS Audit Manager to evaluate the results of integrated GRC activities in your company. By running internal audits, you can compare actual performance with GRC goals. You can then decide if the GRC framework is effective and make necessary improvements.

What are the challenges of GRC implementation?

Businesses might face challenges when they integrate GRC components into organizational activities.

Change management

GRC reports provide insights that guide businesses to make accurate decisions, which helps in a fast-changing business environment. However, companies need to invest in a change management program to act quickly based on GRC insights.

Data management

Companies have long been operating by keeping departmental functions separated. Each department generates and stores its own data. GRC works by combining all the data within an organization. This results in duplicate data and introduces challenges in managing information.

Lack of a total GRC framework

A complete GRC framework integrates business activities with GRC components. It serves the changing business environment, particularly when you are dealing with new regulations. Without a seamless integration, your GRC implementation is likely to be fragmented and ineffective.

Ethical culture development

It takes great effort to get every employee to share an ethically compliant culture. Senior executives must set the tone of transformation and ensure that information is passed through all layers of the organization.

Clarity in communication

The success of GRC implementation depends on seamless communication. Information sharing must be transparent between GRC compliance teams, stakeholders, and employees. This makes activities like creating policies, planning, and decision-making easier.

How do organizations implement an effective GRC strategy?

You must bring different parts of your business into a unified framework to implement GRC. Building an effective GRC requires continuous evaluation and improvement. The following tips make GRC implementation easier.

Define clear goals

Start by determining what goals you want to accomplish with the GRC model. For example, you might want to address the risk of noncompliance to data privacy laws.

Assess existing procedures

Evaluate current processes and technologies in your company that you use to handle governance, risk, and compliance. You can then plan and choose the right GRC frameworks and tools.

Start from the top

Senior executives play a leading role in the GRC program. They must understand the benefits of implementing GRC for policies and how it helps them make decisions and build a risk-aware culture. Top leaders set clear GRC-driven policies and encourage acceptance within the organization.

Use GRC solutions

You can use GRC solutions to manage and monitor an enterprise GRC program. These GRC solutions give you a holistic view of the underlying processes, resources, and records. Use the tools to monitor and meet regulatory compliance requirements. For example, Netflix uses AWS Config to make sure its AWS resources meet security requirements. Symetra uses AWS Control Tower to quickly provision new accounts that fully adhere to their corporate policy.

Test the GRC framework

Test the GRC framework on one business unit or process, and then evaluate whether the chosen framework aligns with your goals. By conducting small-scale testing, you can make helpful changes to the GRC system before you implement it in the entire organization.

Set clear roles and responsibilities

GRC is a collective team effort. Although senior executives are responsible for setting key policies, legal, finance, and IT personnel are equally accountable for GRC success. Defining the roles and responsibilities of each employee promotes accountability. It allows employees to report and address GRC issues promptly.

How can AWS help with GRC?

AWS Cloud Operations optimizes cloud resources with business agility and governance control. You can manage dynamic resources on a massive scale and reduce costs.

For example, with AWS Cloud Operations, you can perform the following tasks:

- Govern, grow, and scale AWS workloads in one place
- Ensure your risk management process stands up to an audit
- Automate compliance management to remove human error

Read more about AWS Management and Governance services or get started by creating an AWS account today.

The meaning and importance of GRC software in today’s business landscape

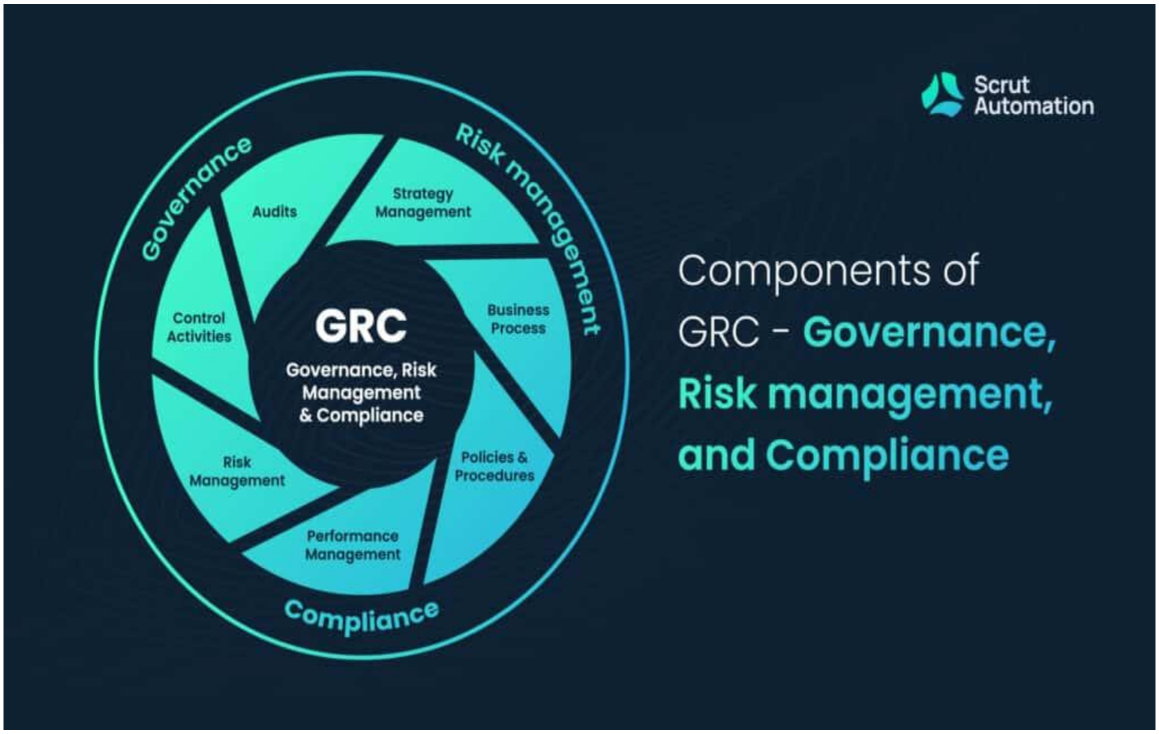
Overnance, risk, and compliance, or GRC, means an organization’s comprehensive risk management approach to align its IT and business goals. Understanding the GRC meaning is crucial for businesses aiming to establish effective governance, manage risks, and ensure compliance within their operations. In the first scholarly research published in 2007, GRC is formally defined as “the integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty, and act with integrity.”

The GRC means governance, risk management, and compliance. This approach is a combination of

Governance: Governance is the sum of procedures established and implemented by the top management, or the board of directors, demonstrated in the organization’s structure and management to achieve its business objectives.

Risk management: This facet of GRC focuses on predicting, mitigating, and responding to risks that can hamper the organization in achieving its business objectives.

Compliance: Compliance is adherence to mandatory laws and regulations and voluntary frameworks to achieve an elevated level of security posture.



A robust cybersecurity posture in today's business landscape mandates a comprehensive GRC approach. One is almost impossible to achieve without the other. GRC is one of the more recent concepts in the cybersecurity landscape; nonetheless, it is becoming the pillar on which the organization's cyber resilience is based.

The evolution of GRC

GRC was a pretty neglected concept until recent years. It lacked standardization. Therefore, every organization had a different perspective towards it. The primary focus was compliance and regulatory issues. Organizations compiled rules and regulations to avoid penalties and fines.

2001- The Enron scandal

Some events changed the GRC landscape forever. In 2001, the world saw one of the biggest scandals in human history – the Enron scandal. SOX was passed in 2002 to protect investors by improving the accuracy and reliability of corporate disclosures.

2008- The global financial crisis

Again in 2008, the global financial crisis begged for financial controls over listed companies. These events changed the perception of GRC and gave it a more modern approach.

Current state of GRC

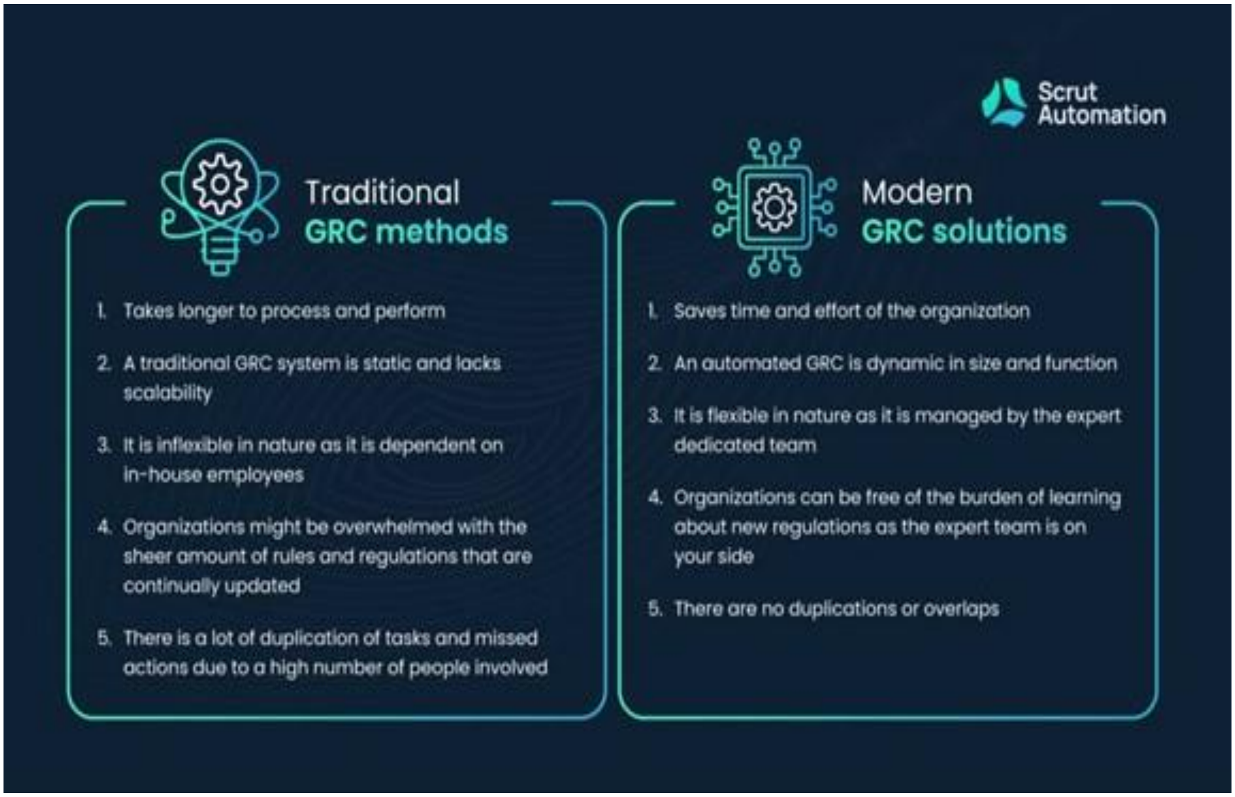
As opposed to the past, today, organizations are willing to invest more in GRC as they have realized the importance of GRC in today's business landscape.

Today some regulations are mandatory, and frameworks are voluntary to carry out compliance. Instead of an isolated area, GRC is becoming mainstream as more consumers prefer organizations with a modern GRC policy in place instead of those that don’t.

However, there are still some issues with the successful implementation of GRC. There are numerous rules and regulations to be followed for compliance in an organization, and some of them overlap. So, the tasks take longer and become complicated.

To be able to add value to business activities, organizations should be able to comply with GRC requirements with less time and expertise. The only befitting way out of the situation is to partner with an outside counsel to guide the organization about the relevant requirements and help it follow them.

Automating the GRC process can reduce the time spent on repetitive tasks, evidence collection, and policy formation. Below is a detailed breakdown depicting how using an automated GRC platform is different from following traditional GRC methods.



Scrut Automation

Traditional GRC methods

1. Takes longer to process and perform
2. A traditional GRC system is static and lacks scalability
3. It is inflexible in nature as it is dependent on in-house employees
4. Organizations might be overwhelmed with the sheer amount of rules and regulations that are continually updated
5. There is a lot of duplication of tasks and missed actions due to a high number of people involved

Modern GRC solutions

1. Saves time and effort of the organization
2. An automated GRC is dynamic in size and function
3. It is flexible in nature as it is managed by the expert dedicated team
4. Organizations can be free of the burden of learning about new regulations as the expert team is on your side
5. There are no duplications or overlaps

A truly competent GRC solution integrates governance, risk management, and compliance seamlessly with an organization’s business goals. There are many such GRC automation tools available in the market today.

Today we will take a deep dive into how to select the right GRC platform while focusing on smart GRC, which is a modern approach that helps organizations accelerate compliance and risk monitoring while ensuring reliability, speed, and security.

What does a GRC platform do?

A typical GRC structure encompasses corporate governance, enterprise risk management (ERM), and compliance with applicable laws and regulations.

It is crucial to align all three components of GRC with the organization's business goals to avoid overlaps and promote effective information security. With the growth in the organization, GRC becomes a taxing task and takes a back burner leading to dire consequences.

The organization often faces issues in training the employees to follow policies and procedures, finding gaps in the systems and designing ways to fill them, keeping pace with the upcoming regulations, and ensuring that controls are maintained throughout the organization.

On the other hand, independently taking up the three facets can lead to a lot of duplication and overlaps. These issues call for a tool that can manage your compliance posture with relative ease and simplicity. In this case, that tool is a smart GRC platform.

What are the benefits of using a modern GRC solution?

A GRC tool can help the organization establish and maintain IT policies and procedures, comply with regulations, and manage cyber risks while achieving business goals. GRC tools or solutions are designed to automate your manual processes and help you achieve your GRC goals effortlessly. The benefits of a modern GRC solution make it a preferable option over traditional GRC. Here are some of the benefits that cannot be overlooked.

Improved risk management

GRC tools help the organization to identify and manage risks effectively. Typically, a GRC tool features risk assessment and threat monitoring modules. These modules help the organization in improving the overall risk management posture of the organization. As the risks and threats are monitored and reported to the management in real-time, they can take quick actions to secure the organization's IT systems.

Strengthened compliance

As the compliance procedures are becoming more stringent and the scope of standards is also widening, organizations often face gaps in compliance. GRC software provides organizations with a centralized repository of policies, controls, regulations, and frameworks. It provides a comprehensive guide to the organization and assists in following them. Ultimately, strengthened compliance is one of the most important features of a reliable GRC tool.

Improved efficiency

With a GRC tool, an organization can reduce manual tasks by automating them, thereby improving efficiency. It provides standardized workflows, approval process, and notifications that reduces the need for manual intervention. In addition to that, GRC tools provide real-time data analytics, helping organizations make well-informed decisions and detect areas for improvement.

Assisted decision-making

GRC tool assists decision-makers by providing a wealth of information and analytics. With real-time risk assessment, the decision-makers can take quick actions if needed. Real-time data and analytics also help the organization make effective decisions that can prevent a breach or penalty. GRC tool can also identify the areas where improvements are needed by continually monitoring the data. This can update the organization's systems as soon as the vulnerability is detected.

Enhanced transparency

A GRC tool is equipped with data, analytics, and reports on its dashboard. The management can review the organization's governance, risk management, and compliance posture at any time with a click of a button. Moreover, the organization can showcase the compliance and risk strategies to its stakeholders, including present and prospective consumers, shareholders, and vendors. Sharing this information can accentuate trust among stakeholders. If the need arises, the governing bodies can review the state of the organization's affairs on the platform.

Reduced cost

A GRC tool should be considered to be an investment rather than an expenditure. This means the benefits of the GRC tool costs are available for considerably longer periods of time. Firstly, it decreases human resource costs by automating repetitive tasks. The time and effort spent on such tasks can be spent on profit-generating activities. Additionally, it reduces the chances of errors – so the cost of human errors is reduced. If the organization faces fines and penalties for non-compliance, it can tune-up to a significant sum denting the resources of the organization. A well-maintained GRC tool can nullify the chances of fines and penalties for non-compliance

Audit assistance

A robust GRC solution can not only integrate with all your apps and software but also automatically collect evidence from them. It can reduce human involvement by 70%. The auditor can be on the same platform, and the organization can share the information with them without much effort. Communication with the auditor about the audit process is well-documented to reduce the time taken in passing the information back and forth.

Now that we have discussed the benefits of a modern GRC solution, let's move on to discuss the factors to be considered while evaluating the GRC software for your organization.

Factors to consider while evaluating GRC software for your organization

Most organizations start searching for a GRC solution when they realize that their in-house efforts are inadequate and unsustainable to maintain security in the long run. And it is during this search that they overlook several critical factors that can either make or break their GRC program.

Investing a large amount of money in a tool that is not right for your organization can cause havoc for your organization. Not only finances but the reputation of your organization can be in question because of one wrong step.

The right GRC tool can make the tasks in an organization much simpler. It helps employees adapt to security requirements without intensive training, and the compliance requirements can be fulfilled with little effort. But that all depends on whether you select the right tool for your organization or not.

Here are a few steps you can follow while evaluating a GRC tool for your organization:

Identify the pain points

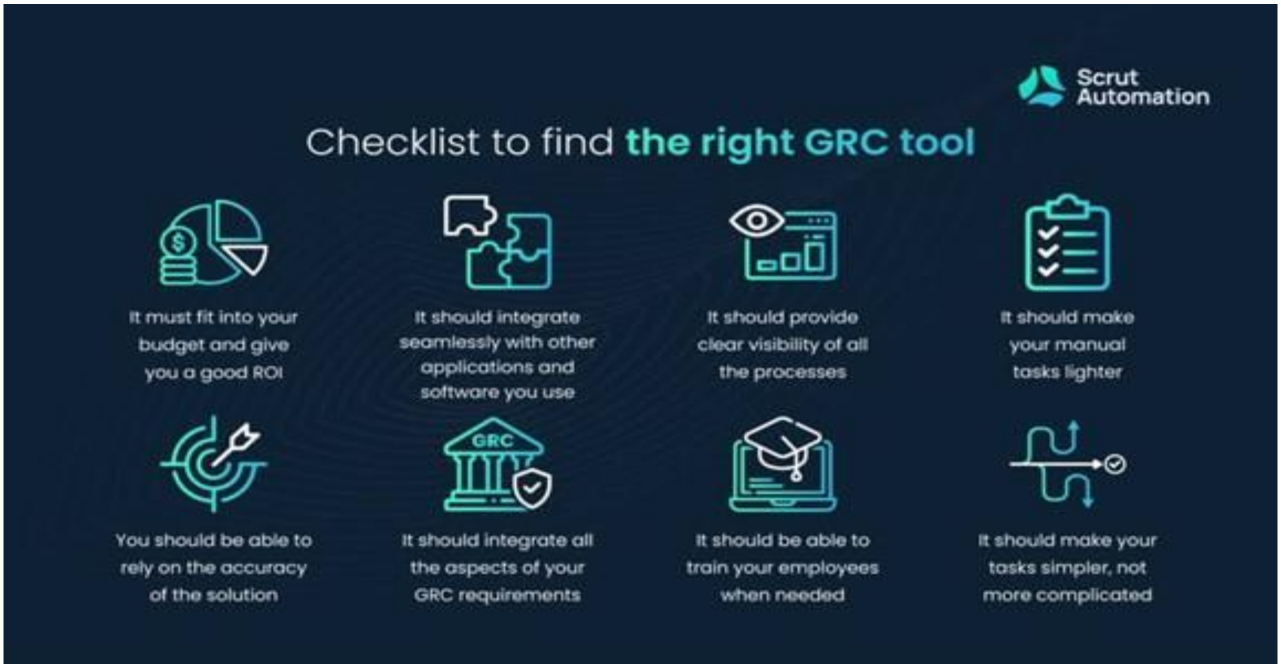
The first step is to list the problems you need to address with a GRC tool. Which are the pain points, if not addressed, can create bigger losses to your organization? Ask yourself the following questions.

Different GRC tools have been developed to solve different pain points of the clients. When you select your solution, you must know what exactly you are looking for in the solution.

Assess different GRC vendors

Focus on your budget and the solutions available to you in the market. Compare and contrast different GRC tools on the basis of what your organization needs. Take the example of the following checklist to see how fitting the tool is for your organization.

GRC tool checklist



Scrut Automation

Checklist to find **the right GRC tool**

It must fit into your budget and give you a good ROI

It should integrate seamlessly with other applications and software you use

It should provide clear visibility of all the processes

It should make your manual tasks lighter

You should be able to rely on the accuracy of the solution

It should integrate all the aspects of your GRC requirements

It should be able to train your employees when needed

It should make your tasks simpler, not more complicated

After comparing a few vendors, you should check with your selected vendor about the pre-launching requirements and the time needed to implement the governance, risk management, and compliance. You should confirm the non-functional requirements with your GRC vendor too. Also check out our article on how to choose GRC Software/Tools?

Assess non-functional requirements of GRC

Non-functional requirements of GRC include all the expectations from the solution over and above the basic requirements. These requirements are

- **Scalability** – Your GRC platform should be able to handle your organization's growth. It should also be able to include all the new laws and regulations that are relevant to your organization in the future.
- **Security** – Your GRC vendor must secure your data adequately from unauthorized access.
- **Integration** – You should be able to integrate your existing software and applications into the GRC software without having to make major changes.
- **Usability** – The GRC platform you choose should be simple enough to use. Training your employees about the solution should be aided by the vendor.
- **Customer support** – The GRC vendor should provide customer support when you need it. The customer support team should be able to guide you through difficult situations.
- **Customer reviews** – Check the customer reviews of the GRC software to know what the existing customers have to say about the product.

Checklist to find **the right GRC tool**

It must fit into your budget and give you a good ROI

It should integrate seamlessly with other applications and software you use

It should provide clear visibility of all the processes

It should make your manual tasks lighter

You should be able to rely on the accuracy of the solution

It should integrate all the aspects of your GRC requirements

It should be able to train your employees when needed

It should make your tasks simpler, not more complicated

Manage pre-launch

Some of the pre-launch steps that need to be taken before implementing the GRC solution are

- Take information from the vendor about pre-launch requirements
- Appoint an in-house team to collaborate with the GRC vendor team
- Determine how the new tool will be configured at the launch
- Ensure the user training by the vendor is scheduled
- Evaluate the vendor system documentation

- Ensure all the IT assets required by the vendor are in place on the D-day

Manage the launch

After a solid pre-launch preparation, the launch can be smooth and event-free. The launch event should be done in coordination with the vendor. The following points should be taken into mind at the time of launch.

- Form a data recovery plan in case something goes wrong
- Coordinate with the vendor team for implementation
- Set up real-time indicators to test the performance of the solution
- Notify all the stakeholders about the implementation of the GRC software

Now you know how to successfully choose and integrate a GRC platform into your system. Let's look at **Scrut's smart GRC** to know how it helps organizations streamline their GRC processes.

Framing governance policies with smartGRC

Every organization has its unique needs for the formation of a comprehensive plan based on its industry, business, and size. Governance policies must be well aligned with the business goals for overall organizational growth.

Scrut's smart GRC is a modern GRC tool that lets you take control of your organization's governance policies in a much simpler and smarter way. It features a library of policies the client can choose from. These pre-built policies are vetted thoroughly by industry experts and aligned with popular industry frameworks.

Moreover, with Scrut, you have the option to customize your governance policies from templates or build your own policies. You can get these policies verified by industry experts to ensure compliance with well-accepted frameworks and governance principles. Also check out our article on why Scrut is the best GRC software?

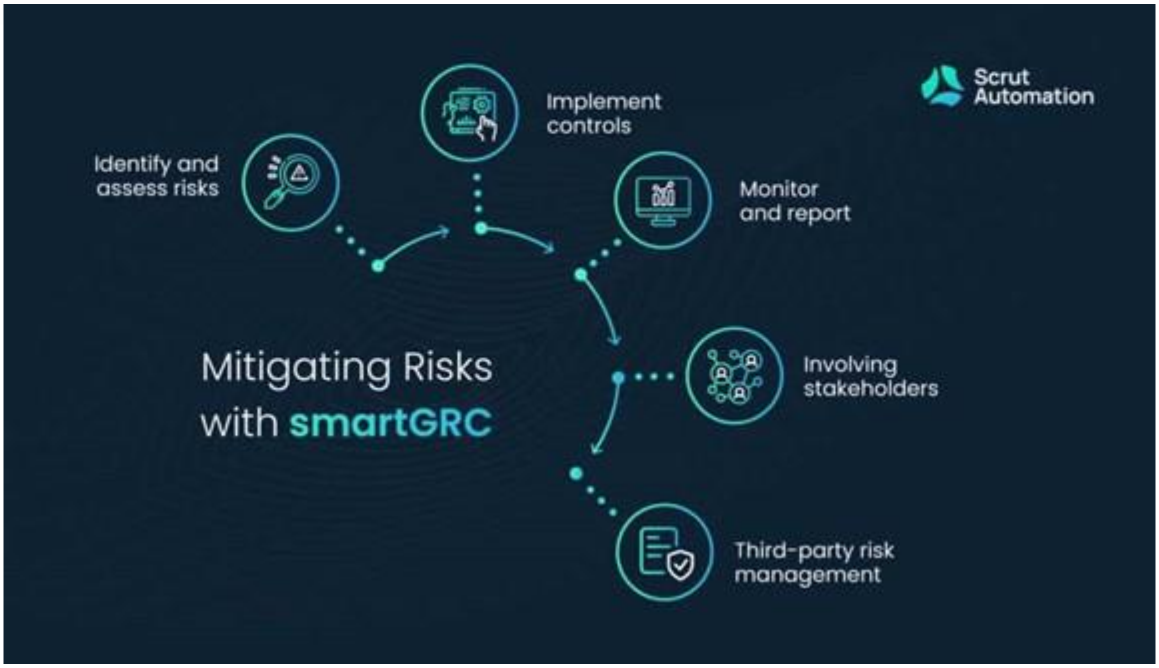
Unleashing the power of AI with GPT Policy Builder

Scrut has launched a new feature that helps you to team up with ChatGPT, which can hasten the process of policy formation called GPT Policy Builder. It can help you create policies regardless of your knowledge level. It will ask you simple questions like the size, industry, and location of your organization and build policies customized for you.

The organization can create tailor-made policies by entering minimum information via prompts and questions. The integration of AI-powered GPT can make policy building faster and easier and help you achieve compliance with the leading industry standards. It offers a continually evolving solution for your governance policies.

This level of customization ensures that your policies and procedure are in sync with your business goals. There are neither overlaps nor duplications of efforts in the workflow, nor are any activities neglected – helping you accelerate your compliance procedure significantly. Also check out our article on how you can use Scrut's GPT Policy Builder for policy generation.

Mitigating Risks with smart GRC


Scrut Automation
Implement controls
Identify and assess risks
Monitor and report
Mitigating Risks with smartGRC
Involving stakeholders
Third-party risk management

Identify and assess risks

Risk management starts with the collection of evidence from various sources in the organization. One of the first steps taken after you register your organization with Scrut is risk assessment and gap analysis done by collecting evidence. A team of experts will review your organization's controls to verify whether they are adequate to mitigate the risks in the present world. If not, the team will guide you to form a more suitable policy to ensure cybersecurity.

Implement controls

The next step is to implement controls to mitigate the risks assessed. This includes training the employees and implementing and reporting mechanisms. Scrut provides an excellent feature to help you train and assess your employees. Monitoring and reporting the control activities can help the organization know the pitfalls in the systems and devise ways to mitigate them.

Monitor and report

A typical organization uses different applications and software, cloud services, communication channels, and platforms to carry out its functions. An organization should monitor and report the effectiveness of controls on every function it performs. Scrut's smart GRC tool can monitor and report on compliance and risk management activities, assisting the organization in identifying and addressing the risks quickly.

Moreover, the organization should regularly update its policies to suit the requirements of the laws and regulations. Also, regular updation can fortify the organization from emerging threats and risks. Smart GRC can help the organization stay ahead of the new rules and regulations along with evolving risks.

Involving stakeholders

Engaging stakeholders, such as employees, customers, and regulators, is critical to the success of GRC. By involving stakeholders in the risk management process, organizations can gain valuable insights and feedback, improve risk awareness, and build trust and credibility. It improves the transparency between stakeholders and the organization's management, thereby increasing trust.

Third-party risk management

When cybercriminals attack an organization, its stakeholders also face the risk of secondary cyber-attacks. Therefore, any organization must be vigilant in choosing its vendors. Scrut offers vendor risk assessment options to all its customers. It helps you to assess the security posture of your vendor or third parties via simple questionnaires.

You can collect the vendor security data, assess it, and share it with the auditors to verify whether they have implemented adequate safeguards for your data. You can also compare the risks presented by different vendors on a single platform in a visual manner before you finalize your vendor.

Maintain compliance with smart GRC

Compliance includes adherence to mandatory and recommendatory regulations, policies, and standards to be followed by an organization for improved cybersecurity. Compliance can help the organization take greater control over its cybersecurity posture.

Some compliance requirements are mandatory to be adhered to, such as GDPR, HIPAA, and SOX. Failing to adhere to these compliance standards can result in penalties and fines to regulatory bodies. It can also lead to legal suits wrecking the reputation of the organization.

Voluntary frameworks like ISO 27001 or SOC 2 are crucial in establishing trust with potential clients. These standards ensure that the organization is following stringent practices to protect the information of its clients.

Both standards and frameworks can enhance the governance policies of the organization. The management gets a clear view of the loopholes in the security process and develops ways to eradicate them.

Thanks to Scrut, your organization can streamline the compliance processes for all the standards and frameworks applicable to your organization. It also helps you in the audit processes, including getting your systems for audit and coordinating with the auditors for a smoother assessment.

Having an integrated platform for compliance standards, risk management, and governance is convenient and cost-effective. It eliminates overlaps and duplication of functions. The management can access all the facets of GRC from a single platform.

What do Scrut clients have to say about smartGRC?

Client testimonials are the most reliable way to know the truth about products and services. So, what better way to know how Scrut smartGRC works than to hear from our customers? Here is what they have to say!

Summing up

To sum up, governance, risk assessment, and compliance are three of the most important aspects of a modern business landscape. It improves the cybersecurity posture of the business, increases customer trust, and saves the organization from non-compliance issues. Overall, the organization can increase its business turnover by demonstrating to its customers that it has formal policies in place.

A modern GRC solution can automate manual tasks, collect evidence for the auditors, and also help in collaborating with the auditors during audits. While looking for an appropriate solution, you must first assess your requirements and the GRC software available in the market to decide which one is best suited for you.

Scrut provides customers with an excellent governance, compliance, and risk management solution called smartGRC, which enables them to manage all security requirements from a single dashboard.

To learn more about smartGRC's ability to streamline your security program, reach out to us today.

FAQs

What is GRC?

Governance, risk management, and compliance or GRC means the integrated approach organizations take to manage their business processes, risks, and compliance requirements.

What are some benefits of implementing GRC in an organization?

Implementing GRC in an organization can help improve risk management practices, increase compliance with regulations, streamline business processes, enhance transparency, and foster a culture of accountability and responsibility.

Who is responsible for implementing GRC in an organization?

GRC is the responsibility of the entire organization, from the board of directors to individual employees. However, many organizations have a designated GRC officer or team who is responsible for overseeing and coordinating GRC activities.

Is smartGRC a better way to govern compliance and risk management?

smartGRC is certainly a better way to govern compliance and risk management than any other GRC tools. smartGRC provides a comprehensive solution for policy formation and implementation, risk management, and compliance. It helps you manage and showcase your compliance certificates and reports on a single dashboard.

How can I evaluate the best GRC platforms?

You can evaluate the top GRC platform based on its functionality, performance, price, and ease of use. You should also consider the reviews of its users and the knowledge of the vendor team before entering into a contract.

Unit Three : ECC to ISO 27001 Control Mapping

At the end of the unit, the trainee will be able to:

- To understand governance and its main importance

- To explain what compliance is and its importance

- To feel the importance of network security management

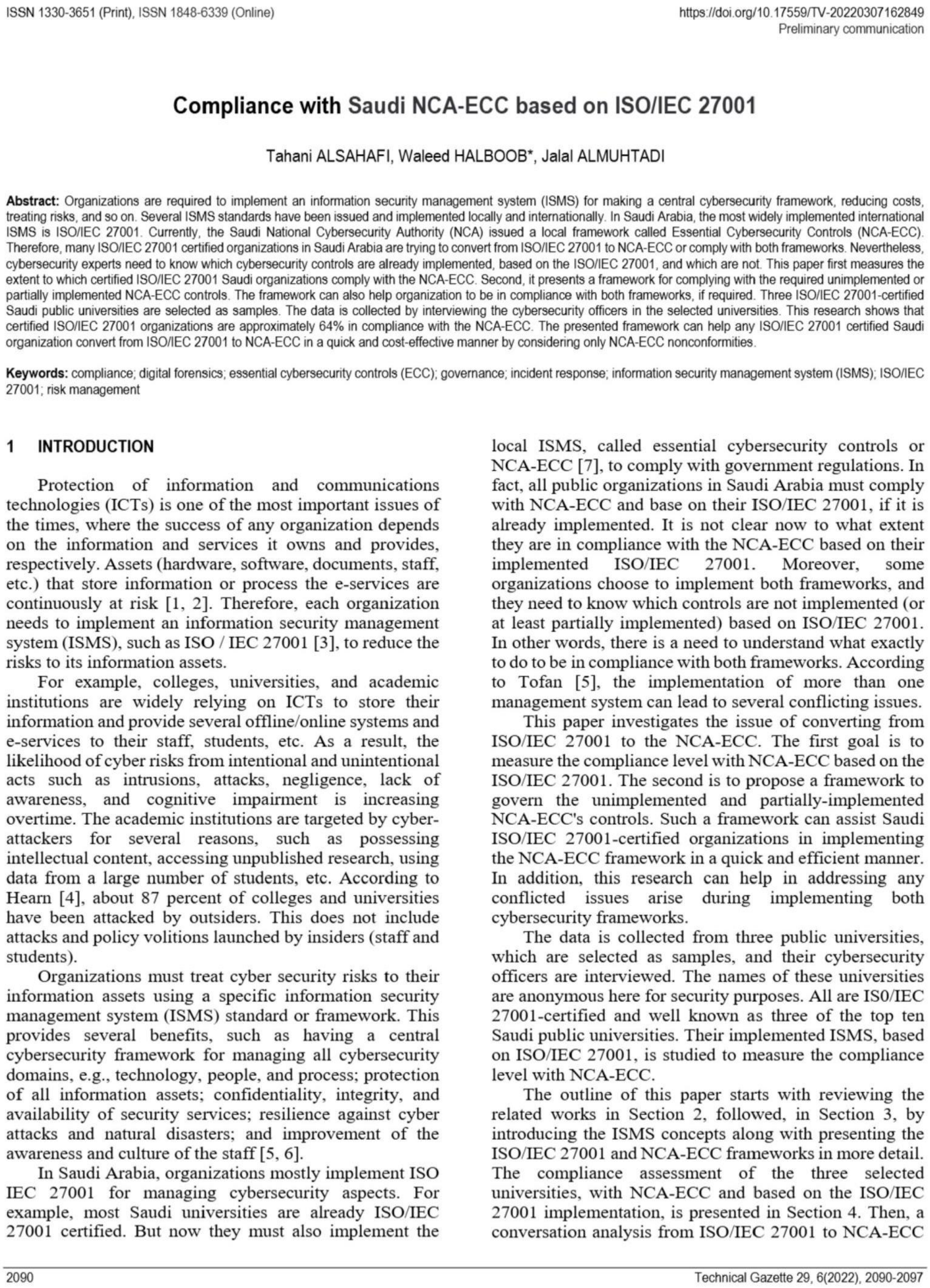
- To understand the management of incidents and threats related to cyber security

- To feel the importance of protecting data and information

- To explain what's basic vulnerability management

- To discover the importance of secure records storage and archiving.

Lesson1 : ECC to ISO 27001 Control Mapping



ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)

https://doi.org/10.17559/TV-20220307162849
Preliminary communication

Compliance with Saudi NCA-ECC based on ISO/IEC 27001

Tahani ALSAHAFI, Waleed HALBOOB*, Jalal ALMUHTADI

Abstract: Organizations are required to implement an information security management system (ISMS) for making a central cybersecurity framework, reducing costs, treating risks, and so on. Several ISMS standards have been issued and implemented locally and internationally. In Saudi Arabia, the most widely implemented international ISMS is ISO/IEC 27001. Currently, the Saudi National Cybersecurity Authority (NCA) issued a local framework called Essential Cybersecurity Controls (NCA-ECC). Therefore, many ISO/IEC 27001 certified organizations in Saudi Arabia are trying to convert from ISO/IEC 27001 to NCA-ECC or comply with both frameworks. Nevertheless, cybersecurity experts need to know which cybersecurity controls are already implemented, based on the ISO/IEC 27001, and which are not. This paper first measures the extent to which certified ISO/IEC 27001 Saudi organizations comply with the NCA-ECC. Second, it presents a framework for complying with the required unimplemented or partially implemented NCA-ECC controls. The framework can also help organization to be in compliance with both frameworks, if required. Three ISO/IEC 27001-certified Saudi public universities are selected as samples. The data is collected by interviewing the cybersecurity officers in the selected universities. This research shows that certified ISO/IEC 27001 organizations are approximately 64% in compliance with the NCA-ECC. The presented framework can help any ISO/IEC 27001 certified Saudi organization convert from ISO/IEC 27001 to NCA-ECC in a quick and cost-effective manner by considering only NCA-ECC nonconformities.

Keywords: compliance; digital forensics; essential cybersecurity controls (ECC); governance; incident response; information security management system (ISMS); ISO/IEC 27001; risk management

1 INTRODUCTION

Protection of information and communications technologies (ICTs) is one of the most important issues of the times, where the success of any organization depends on the information and services it owns and provides, respectively. Assets (hardware, software, documents, staff, etc.) that store information or process the e-services are continuously at risk [1, 2]. Therefore, each organization needs to implement an information security management system (ISMS), such as ISO / IEC 27001 [3], to reduce the risks to its information assets.

For example, colleges, universities, and academic institutions are widely relying on ICTs to store their information and provide several offline/online systems and e-services to their staff, students, etc. As a result, the likelihood of cyber risks from intentional and unintentional acts such as intrusions, attacks, negligence, lack of awareness, and cognitive impairment is increasing overtime. The academic institutions are targeted by cyber-attackers for several reasons, such as possessing intellectual content, accessing unpublished research, using data from a large number of students, etc. According to Hearn [4], about 87 percent of colleges and universities have been attacked by outsiders. This does not include attacks and policy volitions launched by insiders (staff and students).

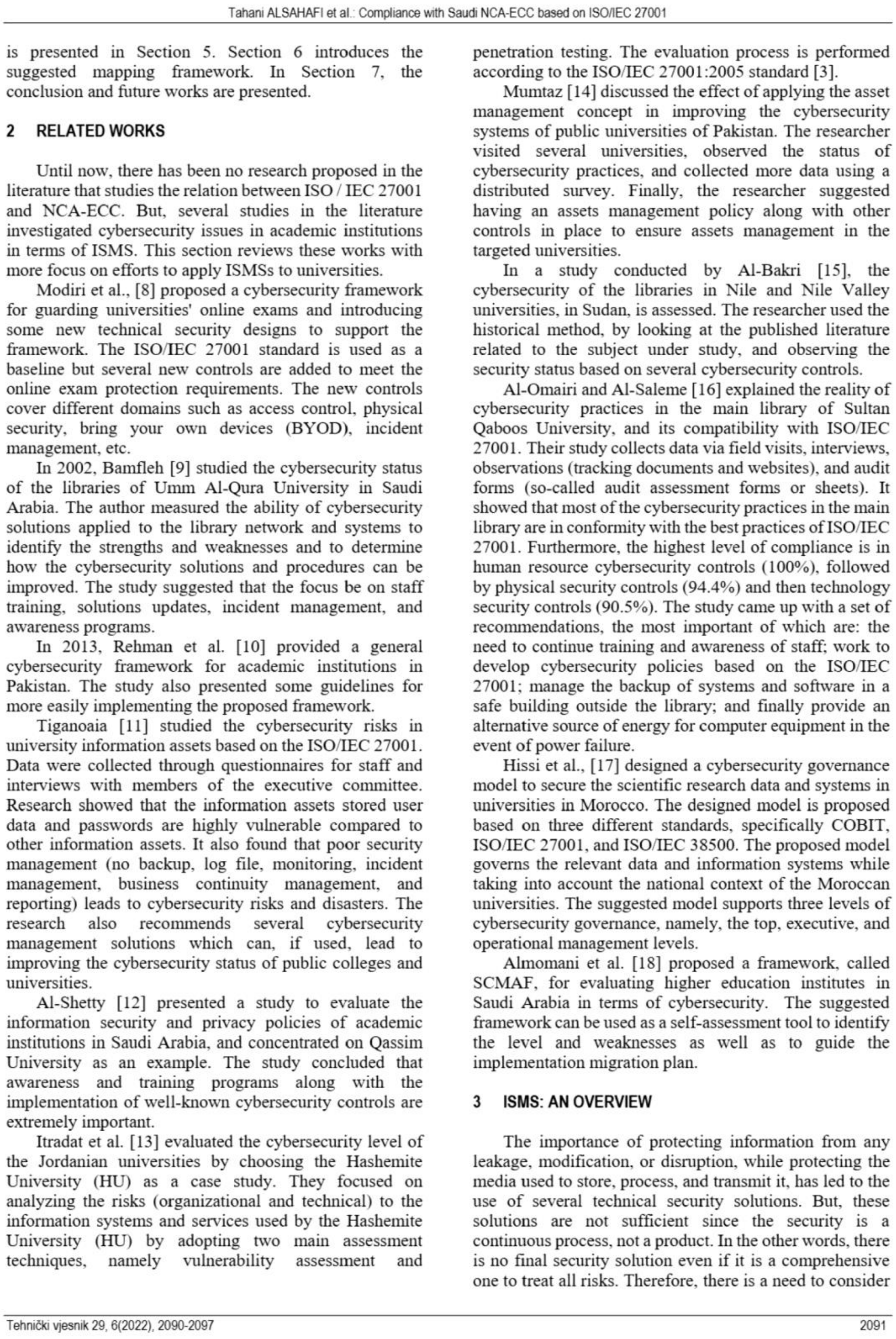
Organizations must treat cyber security risks to their information assets using a specific information security management system (ISMS) standard or framework. This provides several benefits, such as having a central cybersecurity framework for managing all cybersecurity domains, e.g., technology, people, and process; protection of all information assets; confidentiality, integrity, and availability of security services; resilience against cyber attacks and natural disasters; and improvement of the awareness and culture of the staff [5, 6].

In Saudi Arabia, organizations mostly implement ISO IEC 27001 for managing cybersecurity aspects. For example, most Saudi universities are already ISO/IEC 27001 certified. But now they must also implement the local ISMS, called essential cybersecurity controls or NCA-ECC [7], to comply with government regulations. In fact, all public organizations in Saudi Arabia must comply with NCA-ECC and base on their ISO/IEC 27001, if it is already implemented. It is not clear now to what extent they are in compliance with the NCA-ECC based on their implemented ISO/IEC 27001. Moreover, some organizations choose to implement both frameworks, and they need to know which controls are not implemented (or at least partially implemented) based on ISO/IEC 27001. In other words, there is a need to understand what exactly to do to be in compliance with both frameworks. According to Tofan [5], the implementation of more than one management system can lead to several conflicting issues.

This paper investigates the issue of converting from ISO/IEC 27001 to the NCA-ECC. The first goal is to measure the compliance level with NCA-ECC based on the ISO/IEC 27001. The second is to propose a framework to govern the unimplemented and partially-implemented NCA-ECC's controls. Such a framework can assist Saudi ISO/IEC 27001-certified organizations in implementing the NCA-ECC framework in a quick and efficient manner. In addition, this research can help in addressing any conflicted issues arise during implementing both cybersecurity frameworks.

The data is collected from three public universities, which are selected as samples, and their cybersecurity officers are interviewed. The names of these universities are anonymous here for security purposes. All are IS0/IEC 27001-certified and well known as three of the top ten Saudi public universities. Their implemented ISMS, based on ISO/IEC 27001, is studied to measure the compliance level with NCA-ECC.

The outline of this paper starts with reviewing the related works in Section 2, followed, in Section 3, by introducing the ISMS concepts along with presenting the ISO/IEC 27001 and NCA-ECC frameworks in more detail. The compliance assessment of the three selected universities, with NCA-ECC and based on the ISO/IEC 27001 implementation, is presented in Section 4. Then, a conversation analysis from ISO/IEC 27001 to NCA-ECC



is presented in Section 5. Section 6 introduces the suggested mapping framework. In Section 7, the conclusion and future works are presented.

2 RELATED WORKS

Until now, there has been no research proposed in the literature that studies the relation between ISO / IEC 27001 and NCA-ECC. But, several studies in the literature investigated cybersecurity issues in academic institutions in terms of ISMS. This section reviews these works with more focus on efforts to apply ISMSs to universities.

Modiri et al., [8] proposed a cybersecurity framework for guarding universities' online exams and introducing some new technical security designs to support the framework. The ISO/IEC 27001 standard is used as a baseline but several new controls are added to meet the online exam protection requirements. The new controls cover different domains such as access control, physical security, bring your own devices (BYOD), incident management, etc.

In 2002, Bamfleh [9] studied the cybersecurity status of the libraries of Umm Al-Qura University in Saudi Arabia. The author measured the ability of cybersecurity solutions applied to the library network and systems to identify the strengths and weaknesses and to determine how the cybersecurity solutions and procedures can be improved. The study suggested that the focus be on staff training, solutions updates, incident management, and awareness programs.

In 2013, Rehman et al. [10] provided a general cybersecurity framework for academic institutions in Pakistan. The study also presented some guidelines for more easily implementing the proposed framework.

Tiganoaia [11] studied the cybersecurity risks in university information assets based on the ISO/IEC 27001. Data were collected through questionnaires for staff and interviews with members of the executive committee. Research showed that the information assets stored user data and passwords are highly vulnerable compared to other information assets. It also found that poor security management (no backup, log file, monitoring, incident management, business continuity management, and reporting) leads to cybersecurity risks and disasters. The research also recommends several cybersecurity management solutions which can, if used, lead to improving the cybersecurity status of public colleges and universities.

Al-Shetty [12] presented a study to evaluate the information security and privacy policies of academic institutions in Saudi Arabia, and concentrated on Qassim University as an example. The study concluded that awareness and training programs along with the implementation of well-known cybersecurity controls are extremely important.

Itradat et al. [13] evaluated the cybersecurity level of the Jordanian universities by choosing the Hashemite University (HU) as a case study. They focused on analyzing the risks (organizational and technical) to the information systems and services used by the Hashemite University (HU) by adopting two main assessment techniques, namely vulnerability assessment and penetration testing. The evaluation process is performed according to the ISO/IEC 27001:2005 standard [3].

Mumtaz [14] discussed the effect of applying the asset management concept in improving the cybersecurity systems of public universities of Pakistan. The researcher visited several universities, observed the status of cybersecurity practices, and collected more data using a distributed survey. Finally, the researcher suggested having an assets management policy along with other controls in place to ensure assets management in the targeted universities.

In a study conducted by Al-Bakri [15], the cybersecurity of the libraries in Nile and Nile Valley universities, in Sudan, is assessed. The researcher used the historical method, by looking at the published literature related to the subject under study, and observing the security status based on several cybersecurity controls.

Al-Omairi and Al-Saleme [16] explained the reality of cybersecurity practices in the main library of Sultan Qaboos University, and its compatibility with ISO/IEC 27001. Their study collects data via field visits, interviews, observations (tracking documents and websites), and audit forms (so-called audit assessment forms or sheets). It showed that most of the cybersecurity practices in the main library are in conformity with the best practices of ISO/IEC 27001. Furthermore, the highest level of compliance is in human resource cybersecurity controls (100%), followed by physical security controls (94.4%) and then technology security controls (90.5%). The study came up with a set of recommendations, the most important of which are: the need to continue training and awareness of staff; work to develop cybersecurity policies based on the ISO/IEC 27001; manage the backup of systems and software in a safe building outside the library; and finally provide an alternative source of energy for computer equipment in the event of power failure.

Hissi et al., [17] designed a cybersecurity governance model to secure the scientific research data and systems in universities in Morocco. The designed model is proposed based on three different standards, specifically COBIT, ISO/IEC 27001, and ISO/IEC 38500. The proposed model governs the relevant data and information systems while taking into account the national context of the Moroccan universities. The suggested model supports three levels of cybersecurity governance, namely, the top, executive, and operational management levels.

Almomani et al. [18] proposed a framework, called SCMAF, for evaluating higher education institutes in Saudi Arabia in terms of cybersecurity. The suggested framework can be used as a self-assessment tool to identify the level and weaknesses as well as to guide the implementation migration plan.

3 ISMS: AN OVERVIEW

The importance of protecting information from any leakage, modification, or disruption, while protecting the media used to store, process, and transmit it, has led to the use of several technical security solutions. But, these solutions are not sufficient since the security is a continuous process, not a product. In the other words, there is no final security solution even if it is a comprehensive one to treat all risks. Therefore, there is a need to consider all cybersecurity aspects (namely technology, processes, people, etc.) and manage all controls such as authentication, encryption, incident management, digital forensics, staff awareness and training, business continuity, etc.

As a consequence, having several ISMSs are issues being discussed by international bodies and government agencies. An ISMS can be defined as a set of policies, and procedures that define security controls - called also requirements. These policies and procedures are interrelated, and coordinated [19]. Once defined, they need to be implemented. In the end, the whole process is audited at least once a year.

To manage an ISMS task and to achieve best security practices, an organization must identify the targeted ISMS first. The following sub-sections discuss the most well-known and implemented international and local ISMSs in Saudi Arabia.

3.1 International ISMSs

Many organizations around the world are seeking to implement international standards for managing cybersecurity. The most internationally recognized cybersecurity standards or ISMSs are [3, 20]:

- ISO/IEC 27001: It is part of the ISO 27000 series of standards issued by the International Organization for Standardization (ISO), and it can be implemented by both public and private organizations in any country.
- Best Practice Standard: Published by the Information Security Forum in 1992, covering best practices in cybersecurity, but it is less well-known than the ISO/IEC 27001.
- Payment Card Industry-Data Security Standard (PCI-DSS): A standard used by financial organizations, such as banks, to protect credit card data, online payments, client data, etc.

As discussed earlier, the most well-known and implemented international standard is ISO / IEC 27001 [3], which specifies several requirements (called clauses) that must be documented and implemented to ensure the organization to be certified in the ISO/IEC 27001. These clauses are categorized into ten main ones which are scope, normative references, terms and conditions, context of the organization establishment, leadership, planning, support, operation, performance evaluation, and improvements requirements. The sub-clauses will be listed and discussed in the next section.

ISO/IEC 27000 serious includes ISO/IEC 27002 which identifies the security controls. However, also in ISO/IEC 27001 standard an annex (called Annex A) is provided to list all security controls. These controls are in fact taken from the ISO/IEC 27002 standard.

3.2 Saudi Arabia ISMSs

In Saudi Arabia, the following cybersecurity standards have been issued so far [7, 21]:

- SAMA Cybersecurity Framework: Issued by the Saudi Arabian Monetary Authority (SAMA) and applied to all financial organizations in the Kingdom.
- Essential Cybersecurity Controls (NCA-ECC): Issued in October 2018, by National Cybersecurity Authority (NCA) to be implemented by all public organizations and private ones that provide services, specifically IT services, to the public ones. The authority also issued another standard for critical systems, which is outside the scope of this research.

The NCA-ECC controls are distributed into five main domains, which are:

- Cybersecurity Governance.
- Cybersecurity Defence.
- Cybersecurity Resilience.
- Third-party and cloud computing security.
- Cybersecurity of industrial control systems.

The above five domains have 29 main controls, which then have 114 sub-controls. However, these main domains will be listed in the next section.

Compared to ISO/IEC 27001: 2013, the NCA-ECC combines requirements and controls. In ISO/IEC 27000 serious, the requirements are defined in ISO/IEC 27001 while the controls are specified in ISO/IEC 27002. However, the ISO/IEC 27001: 2013 document refers to the list of controls (described in ISO/IEC 27002) in an annex (called Annex A), as mentioned earlier. Also, unlike ISO/IEC 27001 which focus only on three cybersecurity pillars (people, process, and technology), NCA-ECC focus also on the strategy as a fourth pillar. Many of the differences between these two standards will be discussed in this paper successively when the compliance assessment and framework are presented.

4 COMPLIANCE WITH NCA-ECCBASED ON ISO/IEC 27001

This section studies the compliance of the three universities with NCA-ECC based on their implemented ISO/IEC 27001 standard. The names of these universities are kept private here. For the interview, all ISO/IEC 27001 clauses, and their sub-clauses, are listed in an interview table and their data are collected based on answers to questions. Finally, the interview questions for each clause are prepared and written in the same interview table. The entire interview table cannot be presented here due to the limited space provided. Instead, the result of only the main clauses and its immediate sub-clauses is presented. The interviews are made with cybersecurity officers in all three universities. The answer to each control can be one of the following three statuses:

- Implemented: The clause is completely documented and implemented.
- Partially implemented: The clause is not documented or implemented. For instance, it can be documented but not implemented. Another reason the clause can have many sub-clauses, and only some of them are documented and/or implemented.
- Not implemented: The clause and its sub-clauses are not documented and implemented at all.
- Non-applicable: The clause is not applicable to the specific organization.

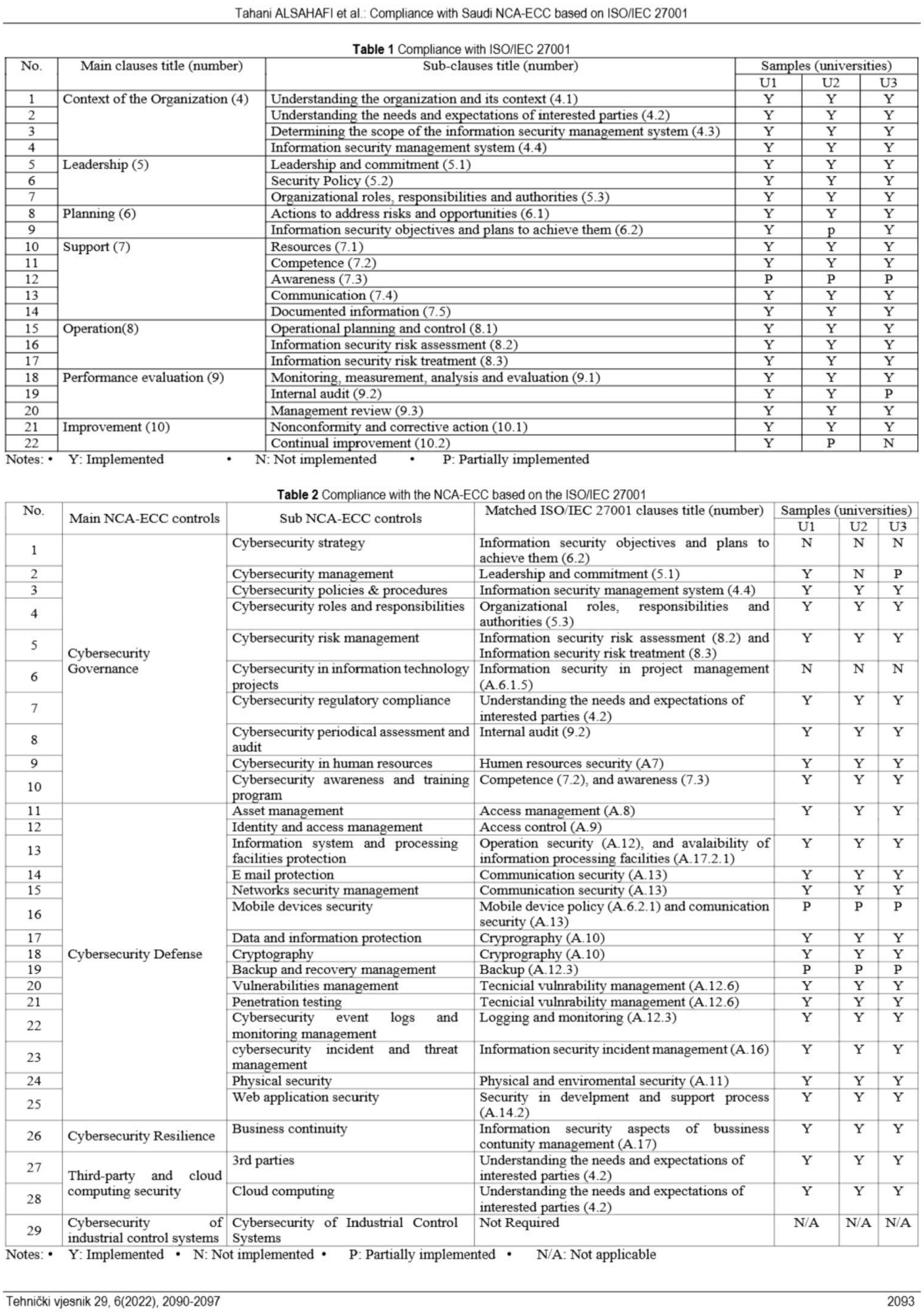


Table 1 Compliance with ISO/IEC 27001

No.	Main clauses title (number)	Sub-clauses title (number)	Samples (universities)		
			U1	U2	U3
1	Context of the Organization (4)	Understanding the organization and its context (4.1)	Y	Y	Y
2		Understanding the needs and expectations of interested parties (4.2)	Y	Y	Y
3		Determining the scope of the information security management system (4.3)	Y	Y	Y
4		Information security management system (4.4)	Y	Y	Y
5	Leadership (5)	Leadership and commitment (5.1)	Y	Y	Y
6		Security Policy (5.2)	Y	Y	Y
7		Organizational roles, responsibilities and authorities (5.3)	Y	Y	Y
8	Planning (6)	Actions to address risks and opportunities (6.1)	Y	Y	Y
9		Information security objectives and plans to achieve them (6.2)	Y	p	Y
10	Support (7)	Resources (7.1)	Y	Y	Y
11		Competence (7.2)	Y	Y	Y
12		Awareness (7.3)	P	P	P
13		Communication (7.4)	Y	Y	Y
14		Documented information (7.5)	Y	Y	Y
15	Operation(8)	Operational planning and control (8.1)	Y	Y	Y
16		Information security risk assessment (8.2)	Y	Y	Y
17		Information security risk treatment (8.3)	Y	Y	Y
18	Performance evaluation (9)	Monitoring, measurement, analysis and evaluation (9.1)	Y	Y	Y
19		Internal audit (9.2)	Y	Y	P
20		Management review (9.3)	Y	Y	Y
21	Improvement (10)	Nonconformity and corrective action (10.1)	Y	Y	Y
22		Continual improvement (10.2)	Y	P	N

Notes: • Y: Implemented • N: Not implemented • P: Partially implemented

Table 2 Compliance with the NCA-ECC based on the ISO/IEC 27001

No.	Main NCA-ECC controls	Sub NCA-ECC controls	Matched ISO/IEC 27001 clauses title (number)	Samples (universities)		
				U1	U2	U3
1	Cybersecurity Governance	Cybersecurity strategy	Information security objectives and plans to achieve them (6.2)	N	N	N
2		Cybersecurity management	Leadership and commitment (5.1)	Y	N	P
3		Cybersecurity policies & procedures	Information security management system (4.4)	Y	Y	Y
4		Cybersecurity roles and responsibilities	Organizational roles, responsibilities and authorities (5.3)	Y	Y	Y
5		Cybersecurity risk management	Information security risk assessment (8.2) and Information security risk treatment (8.3)	Y	Y	Y
6		Cybersecurity in information technology projects	Information security in project management (A.6.1.5)	N	N	N
7		Cybersecurity regulatory compliance	Understanding the needs and expectations of interested parties (4.2)	Y	Y	Y
8		Cybersecurity periodical assessment and audit	Internal audit (9.2)	Y	Y	Y
9		Cybersecurity in human resources	Humen resources security (A7)	Y	Y	Y
10		Cybersecurity awareness and training program	Competence (7.2), and awareness (7.3)	Y	Y	Y
11	Cybersecurity Defense	Asset management	Access management (A.8)	Y	Y	Y
12		Identity and access management	Access control (A.9)			
13		Information system and processing facilities protection	Operation security (A.12), and avalaibility of information processing facilities (A.17.2.1)	Y	Y	Y
14		E mail protection	Communication security (A.13)	Y	Y	Y
15		Networks security management	Communication security (A.13)	Y	Y	Y
16		Mobile devices security	Mobile device policy (A.6.2.1) and comunication security (A.13)	P	P	P
17		Data and information protection	Cryprography (A.10)	Y	Y	Y
18		Cryptography	Cryprography (A.10)	Y	Y	Y
19		Backup and recovery management	Backup (A.12.3)	P	P	P
20		Vulnerabilities management	Tecnicial vulnrability management (A.12.6)	Y	Y	Y
21		Penetration testing	Tecnicial vulnrability management (A.12.6)	Y	Y	Y
22		Cybersecurity event logs and monitoring management	Logging and monitoring (A.12.3)	Y	Y	Y
23		cybersecurity incident and threat management	Information security incident management (A.16)	Y	Y	Y
24		Physical security	Physical and enviromental security (A.11)	Y	Y	Y
25		Web application security	Security in develpment and support process (A.14.2)	Y	Y	Y
26	Cybersecurity Resilience	Business continuity	Information security aspects of bussiness contunity management (A.17)	Y	Y	Y
27	Third-party and cloud computing security	3rd parties	Understanding the needs and expectations of interested parties (4.2)	Y	Y	Y
28		Cloud computing	Understanding the needs and expectations of interested parties (4.2)	Y	Y	Y
29	Cybersecurity of industrial control systems	Cybersecurity of Industrial Control Systems	Not Required	N/A	N/A	N/A

Notes: • Y: Implemented • N: Not implemented • P: Partially implemented • N/A: Not applicable

Tab. 1 shows the result of data collection and analysis. In other words, the result of assessing the three universities in terms of their compliance with ISO/IEC 27001. However, the names of all universities are ignored and U1, U2, and U3 samples are used instead. All universities are ISO/IEC 27001-certified. But and in general, there is a need for implementing stronger awareness programs. Awareness programs in universities help not only protect university information assets, but also provide students and researchers with a greater awareness of cybersecurity, which can help improve it wherever they work. At the time of this writing, the cybersecurity awareness in the interviewed universities relies only on regular email messages sent to faculty, staff, and students. There are no scheduled awareness training sessions. Secondly, the continual improvement of such ISMSs in all universities is not taken seriously. For example, one university did not recertify itself after the first year of certification process. Therefore, in terms of ISO/IEC 27001, all universities are already certified and are already in compliance with most of the requirements, except for security awareness and continual improvement, which require more efforts.Tab. 2 shows the extent to which ISO / IEC 27001 certified universities are in compliance with NCA-ECC. The three universities are assessed based on the NCA-ECC controls (called clauses in the ISO/IEC 27001). The assessment process uses the NCA's assessment tool [22] and covers all domains along with their main controls and sub-controls. However, due to the limited space provided here, only the results of the main controls (total 29 controls) are discussed. Based on the result presented in Tab. 2, it is clear that implementing the ISO/IEC 27001 standard is not sufficient to be in compliance with the NCA-ECC as many main controls are only partially implemented or not implemented at all. Fig. 1 shows that among 29 main controls, only 12 (41%) main controls are implemented, 13 partially implemented (45%), 3 not implemented, and finally (4%) are not applicable for universities. It can be concluded that the ISO/IEC 27001-certified organizations are only 64 present (as 41% controls are totally implemented and 45% controls are partially implemented, counted as 23%, so 64% on average) in compliance with the NCA-ECC.

5 CONVERTING FROM ISO/ECC 27001 NCA-ECC: ANALYSIS

For developing the converting framework, the results of implementing the ISO/IEC 27001 clauses (listed in Tab. 1) are discussed and linked to their relevant controls, if any, in the NCA-ECC.

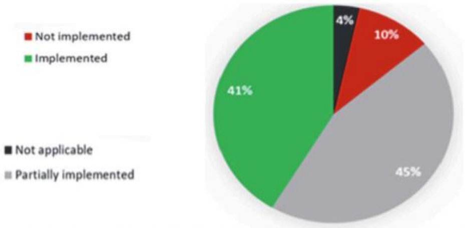


Figure 1 Compliance with the NCA-ECC based on the ISO/IEC 27001

5.1 Clauses Mapping

First, for implementing the ISO/IEC 27001 standard, a document called ISMS manual is prepared. This document lists all clauses and highlights how they are implemented briefly inside the ISMS manual or, mostly, by referring to another document (e.g., policy, procedure, record, etc.) for details. However, having such manual is not required when implementing the NCA-ECC framework. The clauses 0 (introduction) just introduce the standard and its implementation within an organization, and such introduction cannot be reused while implementing the NCA-ECC framework.

Clause 1 (scope) sets the purpose of implementing the ISO/IEC 27001 standard, the type of organization, and finally in which departments in the organization the standard is implemented. Based on our study, all investigated three universities apply the ISO/IEC 27001 standard to their IT department/deanship only. Most public and private organizations do the same to reduce implementation cost (in terms of staff, resources, and time). All three universities refer in their ISMS manual to a document called ISMS scope to explain in more detail the scope of implementing the ISO/IEC 27001 standard. To be more specific, the ISMS scope document explains the departments that are managed by the standards, the description and organizational chart of these departments, geographical locations, relevant third parties, personnel included in the scope, etc. However, the scope of applying the NCA-ECC is for all of an organization and the cybersecurity team cannot exclude any department. So, there is no need for identifying the scope at all. Therefore, the ISO/IEC 27001 scope document is not helpful here and never assists in addressing any NCA-ECC controls.

The clause 2 (normative references) refers to the related ISO documents (namely ISO/IEC 27001 and 2700) inside the ISMS manual. Finally, clause 3 (terms and definitions) requires listing or referring to the terms used in the implemented ISMS. Like clause 2, the clause 3 is also documented inside the ISMS manual and not required by the NCA-ECC framework.

It can be concluded that the ISO/IEC 27001 first four clauses (0 - 3) are not useful for implementing the NCA-ECC framework. The other clauses are discussed in details in the next sub-sections.

5.2 Clauses 4 (Context of the Organization)

This clause requires documenting several ISO/IEC 27001 requirements, whereas all of them are required during implementing the NCA-ECC frameworks but in a different manner. Tab. 3 shows these requirements and how and where they can be applied in the NCA-ECC framework.

5.3 Clauses 6 (Planning)

This clause has two main sub-clauses, which are: actions to address risks and opportunities; and Information security objectives and planning to achieve them. For the first sub-clause, the organization has to develop a risk management policy, and procedures along with a risk management sheet. The sheet must be used to identify, asset, evaluate, and treat all risks associated with information assets. The same risk management policy, procedure, and sheet can be used in the NCA-ECC framework with the following new sub-controls:

- The risk management process needs to be re-executed in many cases, e.g., delivering new services, major changes in the IT infrastructure, and contacting new third parts.
- The risk management process needs to be reexecuted at least every six months, unlike the ISO/IEC 27001 in which reexecuting the risk management process every year is an acceptable procedure.

Table 3 Mapping the context of the organization

No.	ISO/IEC 27001 clauses	ISO/IEC 27001 implementation	Relevant NCA-ECC implementation
1	Clause 4.1 (Understanding the Organization and its context)	Determine the internal and external issues that are relevant to the ISMS	Not mandatory but they can also be determined inside the cybersecurity strategy as challenges.
2	Clause 4.2 (Understanding the needs and expectations of interested parties)	Th expectation of the internal and external parties including the Legal & regulatory requirements	Not required in the NCA-ECC but it is better to list all 3rd parties in the risk assesemnt sheet as well as treat the risks associtaed with them.
3	Clause 4.3 (Determining the scope of the information security management system)	Here, ISMS objectives and boundaries are identified. The objectives must be supported by action plans. The boundaries mean listing all exclusive clauses that are not applicable.	The objectives are identified inside the cybersecurity strategy and need to be supported with initiatives, projects, and budgets. The exclusive controls are marked inside the NCA assessment tool, which is used normally for assessing and auditing the progress.
4	Clause 4.4 (Information security management system)	Confirming, in a statement inside the ISMS manual, the implementation, monitoring, and improving the ISMS.	The organization must implement, monitor, and improve its compliance with the NCA-ECC.

5.4 Clauses 7 (Support)

This clause has five sub-clauses, practical resources, competence, awareness, communication, and documented information. Tab. 4 presents how this clause can be mapped to the implementation of the NCA-ECC.

Table 4 Mapping the support clause implementation into the NCA-ECC

No	ISO/IEC 27001 clauses	ISO/IEC 27001 implementation	Relevant NCA-ECC implementation
1	Clause 5.1 (Leadership and commitment)	The commitment of the top management is documented in a management review procedure.	Many main controls must be reviewed periodically. The ISO/IEC 27001 management review procedure can be used.
2	Clause 5.2 (Policy)	A general policy must be documented, approved, and communicated.	A policy called cooperate cybersecurity policy is prepared as a main policy for all other policies.
3	Clause 5.3 (Organizational roles, responsibilities and authorities)	The roles and responsibilities are recorded in a document called the roles and responsibilities document.	Beside documenting the roles and responsibilities, you need also another document called cybersecurity steering committee regulating.

5.5 Clauses 8 (Operation)

This clause is about executing the security controls that were documented while complying with the previous clauses. These security controls include solutions required for securing the organization's assets and based on the documented policies, procedures, and risk management. However, the controls listed in the ISO/IEC 27002 document are used for this purpose. But, with the NCA-ECC, the security controls are listed as sub-controls in each control. This means that the NCA-ECC did not provide a separate specification for security controls. For most NCA-ECC controls, the sub-controls have to be documented and then implemented. So, converting from the ISO/IEC 27001 to NCA-ECC requires analyzing all existing security policies and procedures to ensure that all NCA-ECC's sub-controls are documented, and implemented.

5.6 Clauses 8 (Performance Evaluation)

In ISO/IEC 27001, the organization must evaluate the performance and effectiveness of its ISMS. This is done through executing the following tasks:

- An internal audit process (every six months or annually) followed by an annual external audit executed by a certification body.
- Frequently, holding a management review meeting to evaluate the status of the ISO/IEC 27001.

With the NCA-ECC, the above processes can be followed with few changes such as the following:

- In terms of internal audit, it is mandatory to be executed every six months, the auditing plan is not mandatory, and the NCA assessment tool is the most preferred.
- For management review, most controls must be periodically reviewed by the cyber security steering committee. Falling to do that will lead to non-compliance with about 21 sub-controls over 114 sub-controls.

5.7 Clauses 9 (Improvements)

In the ISO/IEC 27001, the organization must ensure the continued improvement of its ISMS through correcting all noncompliance found during the internal and external audits. The whole ISMS should be improved over time by targeting new objectives, applying more secure controls, etc. With the NCA-ECC, it is observed that the improvement is granted through auditing and targeting new objectives in each new strategy. But the improvement in the NCA-ECC is widely measured and evaluated through several KPIs linked to the cybersecurity strategy.

6 THE FRAMEWORK

Fig. 2 summarizes the suggested framework. The framework steps are as follows:

1. Developing and implementing a cybersecurity strategy: The NCA-ECC requires a cybersecurity strategy that includes objectives, initiatives, projects, budgets, etc. The NCA website offers a template for cybersecurity strategies that can help Saudi organizations develop their strategies.

2. Cybersecurity Management: The NCA-ECC requires all Saudi organizations to establish a cybersecurity department separated from the IT department and linked directly to the top management.

3. Risk management: The NCA-ECC requires more sub-controls to ensure running the risk management process during launching new IT projects, delivering new e-services, changing the IT infrastructure, and contracting a new third party. Therefore, the execution of the risk management process in these four cases will ensure the compliance of the risk management process with the NCA-ECC requirements.

4. Cybersecurity in information technology projects: In ISO/IEC 27001, this control is not mandatory, but it must be implemented according to NCA-ECC by having a documented, approved, implemented and reviewed cybersecurity in technology projects policy and/or procedure.

5. Periodical assessment and audit: Periodical assessment and audit in the NCA-ECC must be executed every six months, while, in the ISO/IEC 27001, it can be executed annually. So, to meet the NCA-ECC requirements, the auditing process must be scheduled twice a year.

6. Email protection: A two-factor authentication (2FA) is required for authenticating email's users if accessed remotely.

7. National Cybersecurity Authority of Saudi Arabia. (2018). Essential cybersecurity controls (ECC 1: 2018). Available at https://nca.gov.sa/files/ecc-en.pdf (accessed 25 October 2021).

8. Cryptograph: The NCA-ECC also published a national cryptography standards document that defines some criteria for cryptography algorithms, systems, and protocols.

9. Event logs and monitoring management: Similarly, both standards require this control as an email protection control. However, in the ECC, a security information and event management (SIEM) solution must be used as well.

10. Incident response and digital forensics: With the ECC, all Saudi organizations have to comply with more controls compared to the ISO/IEC 27001. They need to register with the NCA and receive all security intelligence alerts, report any security incident to the NCA, and finally, their level of security in some aspects and in different times as directed by the NCA.

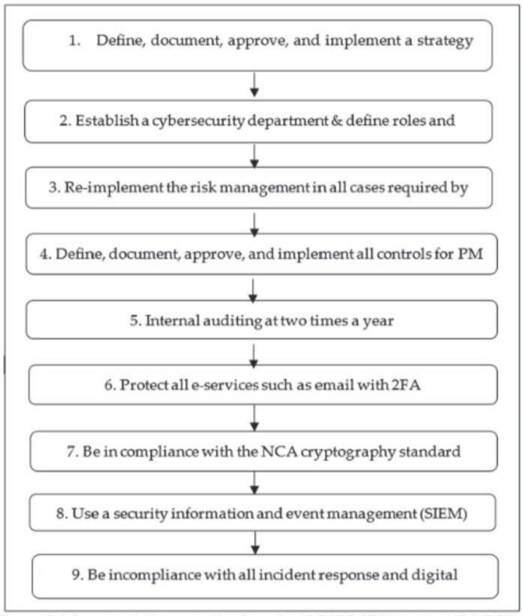

1. Define, document, approve, and implement a strategy
2. Establish a cybersecurity department & define roles and
3. Re-implement the risk management in all cases required by
4. Define, document, approve, and implement all controls for PM
5. Internal auditing at two times a year
6. Protect all e-services such as email with 2FA
7. Be in compliance with the NCA cryptography standard
8. Use a security information and event management (SIEM)
9. Be incompliance with all incident response and digital

Figure 3 A framework for converting from the ISO/IEC 27001 to the NCA-ECC

Another finding that is worth noting is that we typically found that the implementation of the ISO/IEC 27001 tends to be lenient and relaxed, since it is not a requirement for Saudi organizations, and some controls can be partially implemented or delayed to a later date, depending on management decision and risk acceptance. On the other hand, the NCA-ECC controls are implemented in a stricter fashion, with clearly less risk appetite, because the NCA-ECC is mandatory on all government sectors, including public universities.

7 CONCLUSIONS

This research paper investigates compliance of Saudi organizations with the NCA-ECC framework based on their ISO/IEC 27001 implementation. The study found that complying with ISO/IEC 27001 ensures only a partial compliance with the NCA-ECC. Three ISO/IEC 27001 certified Saudi public universities are chosen as samples and their NCA-ECC compliance is evaluated based on their ISO/IEC implementation. Then, all ISO/IEC 27001 clauses implemented are mapped with the relevant controls in the NCA-ECC. A framework for converting ISO/IEC 27001 to the NCA-ECC is presented. This framework can help not only universities but any Saudi organization in converting from the ISO/IEC 27001 to the NCA-ECC quickly and with less time and effort.

Acknowledgements

The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through research group no (RG-1441-531).

The authors declare that they have no conflicts of interest.

8 REFERENCES

[1] Fernandez, A. & Garcia, D. F. (2016). Complex Vs. Simple Asset Modeling Approaches for Information Security Risk Assessment. Evaluation with MAGERIT Methodology. *6th International Conference on Innovative Computing Technology (INTECH)*. https://doi.org/10.1109/intech.2016.7845064

[2] Partheeban P. & Kavitha V. (2015). A Study with Security Concerns in Service Delivery Models of Cloud Computing. *Journal of Information Security Researc*h, *8*(4), 129-145.

[3] ISO/IEC 27001. (2013). https://www.iso.org/isoiec-27001-information-security.html

[4] Hearn, T. (2019). University Challenge: Cyber Attacks in Higher Education.

[5] Tofan, D. C. (2011). Information security standards. *Journal of Mobile, Embedded and Distributed Systems*, *3*(3), 128-135.

[6] Bourekkache, S., Kazar, O., & Aloui, A. (2019). Computer and Network Security: Ontological and Multi-agent System for Intrusion Detection. *Journal of digital information management*, *17*(3), 133-144.

[7] National Cybersecurity Authority of Saudi Arabia. 2018. Essential cybersecurity controls (ECC-1: 2018). https://nca.gov.sa/files/ecc-en.pdf.

[8] Modiri, N., Farahi, A., & Ketabi, S. (2011). Providing Security Framework for Holding Electronic Examinations in Virtual Universities. *7th International Conference on Networked Computing and Advanced Information Management*, Gyeongju, Korea (South), 73-79.

[9] Bamfleh, F. (2002). Information Security Protection in the Main Library of Om Al Qora University. *Future Directions in Libraries and Information*, *9*(18), 1-13.

[10] Rehman, H., Masood, A., & Cheema, A. R. (2013). Information Security Management in Academic Institutes of Pakistan. *2nd NCIA*, 47-51.

[11] Tiganoaia, B. (2013). Some Aspects Regarding the Information Security Management System within Organizations-Adopting the ISO/IEC 27001:2013 Standard. *Studies in Informatics and Control*, *24*(2), 201-210.

[12] Al- Shetty, E. (2014). Privacy Policies Evaluation in Saudi Arabia: Al-Qasim University as Case Study. *Egypt Information Journal*, *13*(14), 11-24.

[13] Itradat, S., Sulatn, M., Al-Junaidi, S., & Qaffaf, R. (2014). Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study. *Jordan Journal of Mechanical & Industrial Engineering*, *8*(2), 102-118.

[14] Mumtaz, N. (2015). Analysis of Information Security Through Asset Management in Academic Institutes of Pakistan. *6th International Conference on Information and Communication Technologies (ICICT)*, 1-4.

[15] Al-bakri, Y. (2017). Information security in Sudan Public Universities. *23rd Annual Conference and Exhibition of Special Libraries Association/Arabian Gulf Chapter*, Manamah, Bahrain, 1-11.

[16] Al-Omeri, M. & Al-Saleme, J. (2017). The Status and Practice of Information Security in the Libraries of Sultan Qabous in Oman. *23rd Annual Conference and Exhibition of Special Libraries Association/Arabian Gulf Chapter*, Manamah, Bahrain, 33-41.

[17] Hissi, Y. E., Arezki, S., & Haqiq, A. (2018). Conceptualization of an Information System Governance Model Dedicated to the Governance of Scientific Research in the Moroccan University. *4th ICCTA*, 54-58.

[18] Almomani, I., Ahmed, M., & Maglaras, L. (2021). Cybersecurity Maturity Assessment Framework for Higher Education Institutions in Saudi Arabia. *Peer J Comput. Sci*.

[19] Dexter, J. (2002). The Cyber Security Management System: A Conceptual Mapping. https://www.sans.org/white-papers/591/

[20] PCI Security Standards Council. (2019). Payment Card Industry (PCI) Data Security Standard. https://www.pcisecuritystandards.org/

[21] Saudi Arabian Monetary Authority (SAMA). (2017). Cyber Security Framework. https://www.sama.gov.sa/en-US/Laws/BankingRules/SAMA%20Cyber%20Security%20Framework.pdf

[22] NCA-ESS Assessment Tool. (2018). https://nca.gov.sa/pages/ecc.html

Contact information:

Tahani ALSAHAFI
Department of Administration and Educational,
Arab East College for Graduate Studies,
Riyadh, Saudi Arabia
Al Qirawan, Riyadh 13544
E-mail: tahanialsahafi@hotmail.com

Waleed HALBOOB
(Corresponding author)
Center of Excellence in Information Assurance,
King Saud University,
Riyadh, Saudi Arabia
P.O Box 92144 Riyadh, 11653, Saudi Arabia
E-mail: Wmohammed.c@ksu.edu.sal

Jalal ALMUHTADI
Center of Excellence in Information Assurance,
King Saud University,
Riyadh, Saudi Arabia &College of Computer and Information Sciences,
King Saud University, Riyadh, Saudi Arabia
PJF9+5XV, King Saud University, Riyadh 12372
E-mail: jalal@ksu.edu.sal

Lesson2 : How to assess current state of ECC compliance

What is ECC compliance?

ECC compliance refers to adherence to the Essential Cybersecurity Controls (ECC), a framework developed to establish fundamental measures and practices for cybersecurity. The ECC provides a structured set of guidelines and controls essential for organizations to protect their systems and data from various cyberthreats. These controls typically cover areas such as access control, incident response, network security, and data protection. This compliance involves implementing and maintaining these essential controls to fortify an organization's cybersecurity posture and mitigate potential risks associated with cyberthreats.

How do I ensure that my organization is ECC compliant?

To ensure ECC compliance, organizations need to assess their current systems and controls and identify and address any gaps in relation to ECC requirements. Event Log Analyzer provides detailed reports that will help ensure your organization is compliant and audit-ready.

Why is ECC compliance important and what does it involve?

Ensuring compliance with ECC is pivotal in fortifying an organization's cybersecurity posture. It involves implementing fundamental controls across access, network security, incident response, and data protection domains. It not only mitigates risks associated with cyberthreats but also aligns with regulatory standards, ensuring trust among stakeholders. Overall, ECC compliance plays a crucial role in proactively addressing vulnerabilities, enhancing incident response, and fostering a secure operational environment amid evolving cyber risks.

Discover how Event Log Analyzer streamlines the process of demonstrating ECC compliance:

- Collect, store, and retain logs from various sources, ensuring that organizations meet ECC's requirements for logging and retaining data for analysis and investigation.
- The file integrity monitoring (FIM) module will track changes to critical files and configurations, helping to identify unauthorized modifications and maintain the integrity of sensitive data.
- Create new reports and customize existing reports to facilitate compliance management. With a wide range of reporting options, organizations can tailor reports according to their specific compliance requirements.

Effortlessly showcase ECC compliance throughout your network

- **Network security management**

Leverage the sophisticated network security management capabilities of Event Log Analyzer to effectively monitor and track network device logins, configurations, and account management activities. This comprehensive solution allows for detailed tracking of various facets within your network infrastructure. This ensures comprehensive control and visibility over activities such as logins, configurations, and account management procedures.

- **Cybersecurity incident and threat management**

Event Log Analyzer's advanced threat analytics feature helps in identifying potential threats promptly and meets ECC's directives for incident response and threat detection. Event Log Analyzer utilizes data from threat feeds by correlating it with the collected log information. This guarantees that administrators receive alerts when a connection is established by a malicious IP address or URL identified in the feed.

- **Access management**

Monitor and track user activities and access rights, addressing ECC's focus on ensuring access control monitoring. The solution offers robust access monitoring to help implement strong security measures, monitor unauthorized access, and maintain compliance with data protection and privacy regulations.

- **Data and information protection**

EventLog Analyzer provides robust data and information protection capabilities to safeguard sensitive information and ensure compliance to ECC. With comprehensive log management and SIEM features, organizations can detect and mitigate security threats, monitor user activities, and maintain data integrity. To protect sensitive data, EventLog Analyzer offers role-based access control (RBAC) and secure log storage to prevent unauthorized access and ensure data confidentiality.

- **Vulnerability management**

EventLog Analyzer can collect log data from various vulnerability scanners like Nessus, Qualys, OpenVAS, and Nmap into its correlation engine, enabling the detection of intricate attack patterns. With over 50 comprehensive out-of-the-box reports to help detect vulnerabilities, organizations can adhere to ECC's vulnerability management requirement.

What additional features does EventLog Analyzer provide?

- **Secure log storage and archiving** EventLog Analyzer ensures that all stored log data is tamper proof and secure. The solution collects and archives log data from the moment of deployment, and the data can be archived for as long as needed.

- **Event log correlation** EventLog Analyzer's correlation engine allows the creation of custom correlation rules, the management of existing rules, and provides correlation reports to help administrators understand complex incidents happening across the network and the sequence in which they unfold. The solution also allows for easy access to the ten most recent correlation incidents that occurred on the network, providing a swift overview in the event of an incident.

- **Privileged user activity monitoring** EventLog Analyzer offers privileged user activity monitoring capabilities to enhance security and compliance. With real-time log collection and analysis, gain visibility into privileged user actions across the network. Track user authentication, authorization, and activity in order to effectively detect and respond to unauthorized access and insider threats.

- **Incident management** Get automated incident response through real-time alerts, automated workflows, and scheduled, customizable reports. Streamline the process of identifying, responding to, and recovering from security incidents.

ECC: Key requirements to consider

ECC compliance requirements	What is it?	Predefined reports in EventLog Analyzer
Identity and access management	To ensure the secure and restricted logical access to information and technology assets in order to prevent unauthorized access and allow only authorized access for users which are necessary to accomplish assigned tasks.	• AD Logon Reports • User Auditing Reports • OU Management • GPO Auditing Reports
Asset management	To ensure that the organization has an accurate and detailed inventory of information and technology assets in order to support the organization's cybersecurity and operational requirements to maintain the confidentiality,	Computer Management Reports

ECC compliance requirements	What is it?	Predefined reports in EventLog Analyzer
	integrity, and availability of information and technology assets.	
Networks security management	To ensure the protection of organization's network from cyber risks.	• Network Device Logon Reports • Network Device Configuration Reports • Network Device Attack Reports • Network Device Security Reports

ECC compliance requirements	What is it?	Predefined reports in EventLog Analyzer
Vulnerability management	To ensure timely detection and effective remediation of technical vulnerabilities to prevent or minimize the probability of exploiting these vulnerabilities to launch cyberattacks against the organization.	• Qualys Vulnerability Reports • Nexpose Vulnerability Reports
Cybersecurity event logs and monitoring management	To ensure timely collection, analysis and monitoring of cybersecurity events for early detection of potential cyberattacks in order to prevent or minimize the negative impacts on the organization's operations.	• Windows Logon Reports • Windows Logoff Reports • Windows Failed Logon Reports • Windows Failed Logon Reports • Windows User Account Changes • Windows Computer Account Changes • Windows User Group Changes

ECC compliance requirements	What is it?	Predefined reports in EventLog Analyzer
Cybersecurity incident and threat management	To ensure timely identification, detection, effective management and handling of cybersecurity incidents and threats to prevent or minimize negative impacts on organization's operation taking into consideration the Royal Decree number 37140, dated 14/8/1438H.	• Symantec reports • FireEye Reports • Malwarebytes Reports • CEF Format Reports • Trend Micro Policy Management • Trend Micro User Account Management

What is NCA compliance?

The National Cybersecurity Authority (NCA) of Saudi Arabia is responsible for safeguarding the country's cybersecurity landscape. The NCA plays an important role in setting policies, standards, and guidelines to protect the nation’s information and communication technology (ICT) infrastructure.

Here's an overview of the NCA's major controls:

- **Essential Cybersecurity Controls(ECC):**These controls are fundamental measures that organizations should implement to protect their systems and data against common cyberthreats.
- **Cloud Cybersecurity Controls (CCC):** These controls focus on securing cloud computing environments and addressing specific risks and challenges associated with cloud services.
- **Telework Cybersecurity Controls (TCC):** These controls are designed to secure remote work environments, ensuring that employees working from remote locations are adequately protected.

- **Critical Systems Cybersecurity Controls (CSCC):** These controls aim to safeguard critical infrastructure and systems that are essential for the functioning of key sectors and services.
- **Operational Technology Cybersecurity Controls (OTCC):** These controls focus on securing operational technology systems, which include industrial control systems (ICS) and other technologies used in industrial settings.
- **Data Cybersecurity Controls (DCC):** These controls are specifically geared towards protecting sensitive data from unauthorized access, modification, or disclosure.

These controls are tailored to address specific cybersecurity risks and requirements within Saudi Arabia, ensuring a comprehensive approach to cybersecurity across its different operational environments and sectors.

Consequence of noncompliance

Noncompliance with the NCA's regulations can have severe consequences for organizations. These include substantial fines, legal action, and loss of operating licenses. Furthermore, failure to adhere to cybersecurity regulations increases an organization's vulnerability to cyberattacks, which can result in data breaches, loss of sensitive information, operational disruptions, and significant recovery costs. The combined impact of these factors can be devastating, affecting not only the organization’s financial stability but also its market position and operational continuity.

What is CCC compliance?

The NCA of Saudi Arabia has developed the CCC to minimize cybersecurity risks associated with cloud computing. The CCC sets out specific requirements for both Cloud Service Providers (CSPs) and Cloud Service Tenants (CSTs) to ensure the secure usage of cloud services and mitigate potential cyberthreats.

The CCC addresses the complexities of cloud environments, offering specific guidelines on data privacy, identity management, encryption, and compliance. These measures are designed to protect the confidentiality, integrity, and availability of cloud-hosted data and services. Adherence to the CCC not only mitigates cybersecurity risks but also ensures alignment with national and international regulations, promoting a secure and resilient digital environment for all stakeholders in the country .

Components of the CCC

The CCC consists of four main domains and 24 subdomains, each designed with specific controls and sub-controls for CSPs and CSTs. The framework is an extension of the ECC and focuses on four main pillars:

Strategy: Ensuring that cloud security strategies are aligned with organizational goals and national cybersecurity objectives.

People: Fostering a skilled workforce capable of managing and securing cloud environments.

Procedures: Implementing robust processes and policies to maintain cloud security.

Technology: Leveraging advanced technologies and practices to protect cloud infrastructures and data.

Benefits of implementing the CCC

Implementing the CCC offers significant advantages for both CSPs and CSTs operating in Saudi Arabia.

For CSPs

- **Enhanced reputation:** Compliance with the CCC demonstrates a strong commitment to security, boosting trust and credibility among customers.
- **Competitive advantage:** Being CCC compliant positions CSPs as preferred partners for government agencies and other regulated industries.
- **Risk mitigation:** By adhering to the CCC, CSPs can proactively identify and address potential security vulnerabilities, reducing the risk of data breaches and financial losses.
- **Business continuity:** Robust security measures as outlined in the CCC ensure uninterrupted service delivery and minimize business disruptions due to cyberattacks.
- **Compliance with regulations:** The CCC aligns with international cybersecurity standards, simplifying compliance efforts for CSPs operating in a global market.

For CSTs

- **Data protection:** The CCC safeguards sensitive data stored in the cloud, protecting critical business information from unauthorized access.
- **Risk reduction:** By ensuring their CSP is CCC compliant, CSTs can mitigate the risk of data breaches and other cyber incidents.
- **Regulatory compliance:** Organizations can demonstrate compliance with data protection regulations by partnering with CCC compliant CSPs.
- **Cost savings:** Preventing data breaches and associated recovery costs can lead to significant financial savings for CSTs.

CCC: Key requirements to consider

CCC compliance requirements	What is it?	Predefined reports in EventLog Analyzer
2-4 Networks Security Management	To ensure the protection of networks managed by CSPs and CSTs from cyber risks.	• Network Device Logon Reports • Network Device Configuration Reports • Network Device Attack Reports • Network Device Security Reports
2-8 Backup and Recovery Management	To ensure the protection of CSPs' data and information, including information systems and software configurations, from cyber risks as per organizational policies and procedures and related laws and regulations.	Exchange Online Backup
2-11 Cybersecurity Event Logs and Monitoring Management	Ensure timely collection, analysis, and monitoring of cybersecurity event logs for the proactive detection and effective management of cyberattacks to prevent or minimize the impact on CSPs' and CSTs' businesses.	• Windows Logon Reports • Windows Logoff Reports • Windows Failed Logon Reports • Windows Failed Logon Reports

		• Windows User Account Changes • Windows Computer Account Changes • Windows User Group Changes
2-12 Cybersecurity Incident and Threat Management	Ensure timely collection, analysis, and monitoring of cybersecurity event logs for the proactive detection and effective management of cyberattacks to prevent or minimize the impact on the CSPs' and CSTs' business.	• Symantec reports • FireEye Reports • Malwarebytes Reports • CEF Format Reports • Trend Micro Policy Management • Trend Micro User Account Management

What is TCC compliance?

The TCC is a comprehensive framework designed to safeguard organizations in Saudi Arabia as they transition to remote work environments. Recognizing the increasing reliance on technology and the potential cyber risks associated with remote work, the NCA developed the TCC to mitigate these threats. Building upon the ECC, the TCC provides specific guidelines for securing telework operations. For examples, these controls may involve secure VPN access, MFA, endpoint security for remote devices, and policies for secure handling of sensitive information outside the corporate network.

The framework encompasses three primary domains, encompassing 21 main controls and 42 sub-controls, to address various aspects of remote work security. These controls aim to protect organizational data and systems, enhance cybersecurity resilience, and contribute to the overall cybersecurity posture of the country. Compliance with the TCC is mandatory for government entities, critical infrastructure organizations, and strongly encouraged for other businesses in Saudi Arabia. To ensure ongoing adherence, the NCA employs self-assessments and external compliance evaluations.

Objectives of the TCC

The primary goals of the TCC are:

Enabling secure remote work: To equip organizations with the necessary cybersecurity measures to conduct business operations remotely without compromising security.

Enhancing cybersecurity resilience: To strengthen organizations' ability to withstand cyberattacks and recover quickly from incidents in a telework environment.

Contributing to national cybersecurity: To elevate the overall cybersecurity posture of the country by promoting standardized security practices.

Implementing the TCC is essential for safeguarding organizations from the growing cyberthreats associated with remote work. By following these controls, businesses can significantly bolster their cybersecurity defenses, reduce the risk of data breaches and financial losses, and ensure a smooth transition to remote operations. Moreover, aligning with international cybersecurity standards through TCC compliance demonstrates a strong commitment to protecting sensitive information and maintaining trust with stakeholders.

Benefits of implementing the TCC

Implementing the TCC is crucial for several reasons:

- **Enhanced cybersecurity resilience:** By adhering to the TCC, organizations can significantly improve their ability to defend against cyberthreats and protect sensitive information.
- **Mitigated cyber risks:** The TCC addresses common vulnerabilities associated with remote work, reducing the risk of data breaches, unauthorized access, and other cyberattacks.
- **Seamless remote operations:** The framework facilitates a smooth transition to remote work while maintaining security standards.
- **Cost reduction**: Preventing cyber incidents through TCC compliance can save organizations significant financial losses due to data breaches, downtime, and reputational damage.
- **Alignment with global standards:** The TCC is based on international cybersecurity best practices, ensuring compatibility with global security standards.

TCC: Key requirements to consider

TCC compliance requirements	What is it?	Predefined reports in Event Log Analyzer
2-4 Networks Security Management	To ensure the protection of the organization's network from cyber risks.	• Network Device Logon Reports • Network Device Configuration Reports • Network Device Attack Reports • Network Device Security Reports
2-8 Backup and Recovery Management	To ensure the protection of the organization's data and information, including information systems and software configurations, from cyber risks as per organizational policies, procedures, and related laws and regulations.	Exchange Online Backup
2-11 Cybersecurity Event Logs and Monitoring Management	To ensure timely collection, analysis, and monitoring of cybersecurity events for early detection of potential cyber-attacks	• Windows Logon Reports • Windows Logoff Reports • Windows Failed Logon Reports

	in order to prevent or minimize the negative impacts on the organization’s operations.	• Windows Failed Logon Reports • Windows User Account Changes • Windows Computer Account Changes • Windows User Group Changes
2-12 Cybersecurity Incident and Threat Management	To ensure timely identification, detection, effective management and handling of cybersecurity incidents and threats to prevent or minimize negative impacts on organization’s operation taking into consideration the Royal Decree number 37140, dated 14/8/1438H.	• Symantec reports • FireEye Reports • Malwarebytes Reports • CEF Format Reports • Trend Micro Policy Management • Trend Micro User Account Management

What is CSCC compliance?

The CSCC is a comprehensive framework designed to bolster the security of critical systems within organizations operating in Saudi Arabia. It complements the ECC by providing more stringent requirements specifically tailored for systems deemed crucial to the country's infrastructure and operations. The CSCC comprises 32 main controls and 73 sub controls, offering a detailed roadmap for securing critical systems.

Components of the CSCC

The CSCC recognizes that critical systems are composed of various elements:

- **Technical components:** Network infrastructure (e.g., routers, switches, firewalls), databases, storage, middleware, servers, applications, encryption devices, and peripherals.
- **Human element:** Individuals involved in critical system operations, including users, technical staff, and operators.
- **Supporting documentation:** Documentation related to all system components.

Objectives of the CSCC

The primary goals of the CSCC are:

- **Enabling secure remote work:** To equip organizations with the necessary cybersecurity measures to conduct business operations remotely without compromising security.
- **Enhancing cybersecurity resilience:** To strengthen organizations' ability to withstand cyberattacks and recover quickly from incidents in a telework environment.
- **Contributing to national cybersecurity:** To elevate the overall cybersecurity posture of the country by promoting standardized security practices.

Organizations that should comply with the CSCC Here are some entities that should comply with these guidelines:

- Government organizations, including ministries, authorities, and embassies.
- Government subsidiaries.
- Private sector entities operating critical systems.

Importance of compliance

Adhering to the CSCC is paramount for organizations operating critical systems. It offers several benefits:

- **Enhanced cybersecurity resilience:** Strengthens defenses against cyberthreats.
- **Protection of critical assets:** Safeguards vital systems and sensitive information.
- **Legal and regulatory compliance:** Aligns with NCA mandates and avoids potential penalties.
- **Reputation enhancement:** Demonstrates a commitment to cybersecurity best practices.
- **Risk mitigation:** Reduces the likelihood of significant losses due to cyber incidents.

CSCC: Key requirements to consider

CSCC compliance requirements	What is it?	Predefined reports in Event Log Analyzer
2-4 Networks Security Management	To ensure the protection of the organization's network from cyber risks.	• Network Device Logon Reports • Network Device Configuration Reports • Network Device Attack Reports • Network Device Security Reports
2-8 Backup and Recovery Management	To ensure the protection of the organization's data and information, including information systems and software configurations, from cyber risks as per organizational policies, procedures, and related laws and regulations.	Exchange Online Backup
2-11 Cybersecurity Event Logs and	To ensure timely collection, analysis, and monitoring of	• Windows Logon Reports • Windows Logoff Reports • Windows Failed Logon Reports

Monitoring Management	cybersecurity events for early detection of potential cyber-attacks in order to prevent or minimize the negative impacts on the organization’s operations.	• Windows Failed Logon Reports • Windows User Account Changes • Windows Computer Account Changes • Windows User Group Changes

What is OTCC compliance?

The OTCC is a specialized cybersecurity framework designed to protect critical infrastructure systems. It recognizes the unique challenges posed by Operational Technology (OT) environments, such as ICSs, and provides tailored security measures to mitigate risks.

Objectives of the OTCC

The primary goals of the OTCC are:

- **Enhancing the protection of critical infrastructure:** To safeguard essential systems and services from cyberattacks.
- **Improving organizational preparedness for cyberthreats:** To equip organizations with the necessary tools and training to respond effectively to cyber incidents.
- **Contributing to overall national cybersecurity:** To strengthen the nation's resilience against cyberthreats and protect critical assets.

The OTCC focuses on securing ICSs within critical facilities, including those in both the government and private sectors. It applies to organizations that own, operate, or host critical national infrastructures (CNIs).

Potential OTCC control areas

Given the nature of OT environments, the OTCC likely addresses the following areas.

Network security:

- Segmentation of OT networks from IT networks
- Use of firewalls and intrusion detection systems
- Secure remote access protocols

Device hardening:

- Patch management for OT devices
- Configuration management and change control
- Vulnerability management

Data protection:

- Data classification and protection
- Backup and recovery procedures

Access control:

- Role-based access control
- Strong authentication mechanisms

Incident response and recovery:

- Incident response planning and procedures
- Business continuity and disaster recovery

Importance of the OTCC

Implementing the OTCC is crucial for organizations operating critical infrastructure. Key benefits include:

Securing critical infrastructure: Protects vital systems from cyberattacks and disruptions.

Compliance: Aligns with national cybersecurity mandates and regulations.

Risk mitigation: Reduces the likelihood of cyber incidents and their consequences.

Strengthening ICS: Enhances the security of industrial control systems, a critical component of operations.

OTCC: Key requirements to consider

OTCC compliance requirements	**What is it?**	**Predefined reports in Event Log Analyzer**
2-4 Networks Security Management	To ensure the protection of the organization’s OT/ICS networks from cyber risks.	• Network Device Logon Reports • Network Device Configuration Reports • Network Device Attack Reports • Network Device Security Reports
2-8 Backup and Recovery Management	To ensure the protection of the organization’s data and information, including information systems and software configurations, from cyber risks as per organizational policies, procedures, and related laws and regulations.	Exchange Online Backup

2-11 Cybersecurity Event Logs and Monitoring Management	To ensure timely collection, analysis, and monitoring of cybersecurity events for early detection of potential cyber-attacks in order to prevent or minimize the negative impacts on the organization’s operations.	• Windows Logon Reports • Windows Logoff Reports • Windows Failed Logon Reports • Windows Failed Logon Reports • Windows User Account Changes • Windows Computer Account Changes • Windows User Group Changes
2-12 Cybersecurity Incident and Threat Management	To ensure timely identification, detection, effective management, and handling of cybersecurity incidents and threats to prevent or minimize negative impacts on organization’s OT/ICS operation.	• Symantec reports • FireEye Reports • Malwarebytes Reports • CEF Format Reports • Trend Micro Policy Management • Trend Micro User Account Management

What is DCC compliance?

The primary purpose of the DCC is to bolster the cybersecurity defenses of organizations across various sectors within Saudi Arabia. This framework was developed in response to growing cybersecurity threats and aims to protect the country's critical infrastructure, national security, and vital interests.

Structure of the DCC

The NCA DCC is organized into a hierarchical structure designed to cover various aspects of cybersecurity:

- The framework is divided into three main domains. These domains represent broad areas of cybersecurity control that encompass various aspects of data protection and management.
- Within each domain, there are 11 subdomains. These subdomains further break down the domains into more specific areas of focus, allowing for detailed management and oversight of cybersecurity practices.
- There are 19 core controls within the framework. These controls provide specific directives and practices that organizations must implement to safeguard their data.
- The controls are further divided into 47 sub-controls. These sub controls offer detailed guidelines and procedures to ensure comprehensive implementation of the core controls.

Objectives of the DCC

The primary goals of the DCC are:

- **Enhance cybersecurity standards:** Elevate the standards for protecting national data to safeguard against threats and breaches.
- **Support organizations:** Provide continuous support to entities in securing their data throughout its life cycle, helping to mitigate cybersecurity threats and risks.
- **Increase awareness:** Foster a better understanding of secure data handling practices across various organizations.

Scope and applicability

The NCA DCC is applicable to:

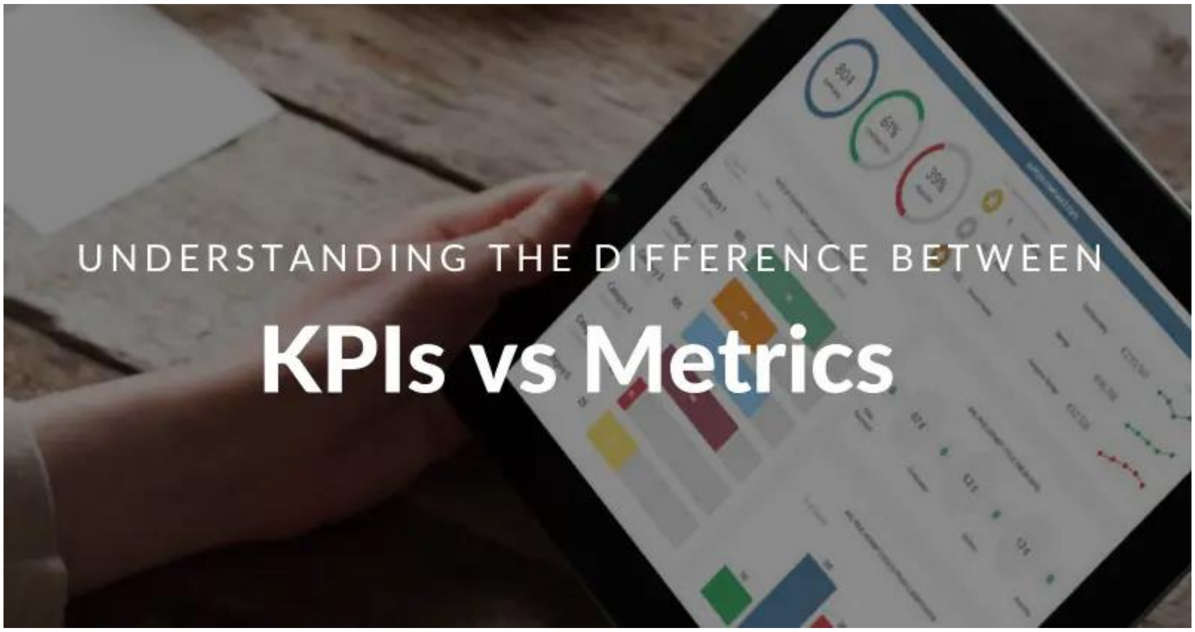
- **Government organizations:** This includes ministries, authorities, and affiliated entities within the Saudi government.
- **Private sector organizations:** Entities involved in critical national infrastructure must adhere to these controls. This includes private organizations that own, operate, or host such infrastructures.
- **General organizations:** While the primary focus is on government and critical infrastructure entities, NCA encourages all organizations in the Kingdom to adopt these controls. Doing so will help improve their cybersecurity posture and ensure robust data protection.

DCC: Key requirements to consider

DCC compliance requirements	What is it?	Predefined reports in Event Log Analyzer
2-6 Secure Data Disposal	To ensure a secure data disposal as per organizational policies and procedures and related to laws and regulations.	• File integrity monitoring • Log archiving
2-7 Cybersecurity for Printers, Scanners, and Copy machines	To ensure secure handling of data when using Printers, scanners, and copy machines.	Print server log monitoring

Lesson3 : How to develop ECC metrics and KPIs

KPIs vs Metrics: Understanding the Differences with Tips & Examples



Performance tracking has never been easier. With the rise of modern self-service BI tools, everyone can monitor relevant performance indicators in a matter of seconds. But this is not without problems. Having the ability to analyze your data fast and efficiently doesn't always mean you are doing it correctly. Businesses extract data from several internal and external sources, which makes it difficult but necessary to filter this data and only keep what's relevant for the company. This is done with the help of KPIs and metrics.

KPIs and metrics are often considered the same thing in day-to-day business contexts. However, while they work similarly, they are not used for the same purposes. Just memorize this statement for later: all KPIs are metrics, but not all metrics are KPIs.

This post will cover the main difference between metrics and KPIs and provide examples and tips for efficient performance tracking.

Let's kick it off with the answer to the famous question: are metrics and KPIs the same?

What Are KPIs?

Key performance indicators, or KPIs, measure performance or progress based on specific business goals and objectives. A pivotal element to consider is the word "key," meaning they only track what is truly relevant to the company's strategic decisions.

A good KPI should help you and your team understand if you are making the right decisions. They act as a map of business outcomes and are the strategic indicators that will move the company forward. Examples of KPIs can be sales growth, customer retention, or customer lifetime value. Companies usually visualize these measurements with the help of interactive KPI reports.

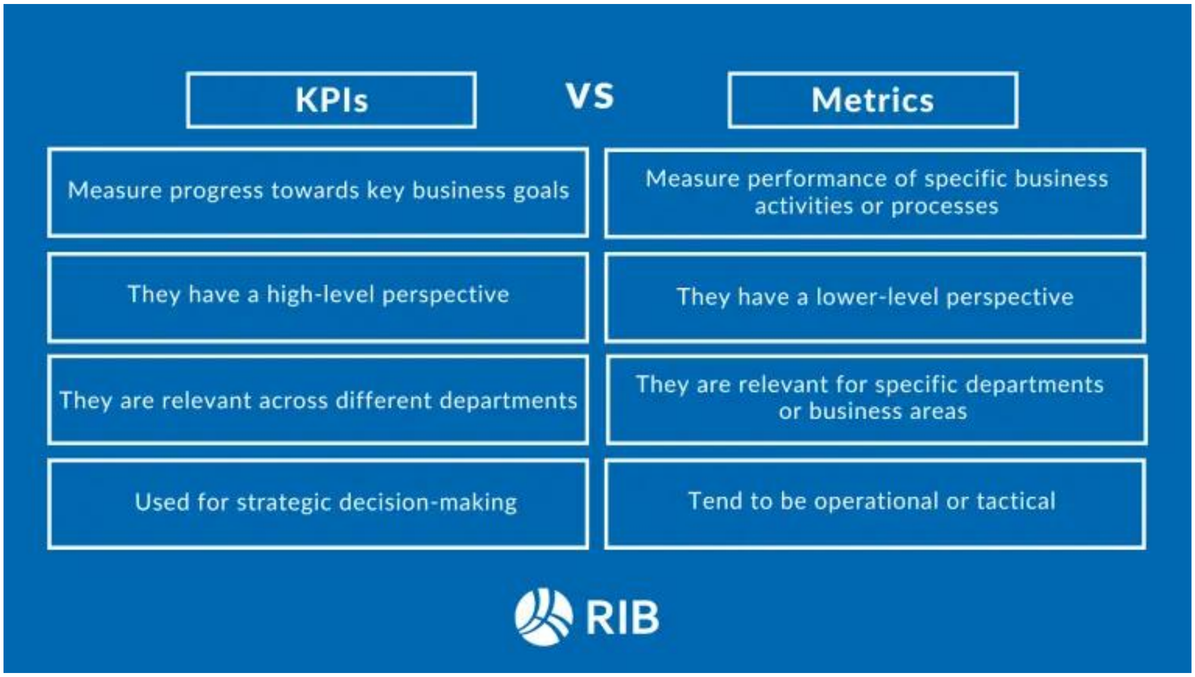
What Are Metrics?

Metrics are quantitative measurements used to track the performance of specific business processes at an operational and tactical level. They help provide context for the performance of key business goals but are not critical to their success like KPIs are.

While some might be tight to objectives, metrics are not the most important indicators for monitoring strategic actions. However, they are still relevant to informing businesses about the progress of their different activities. Some examples of metrics include the lead-to-conversion ratio, return rate, and acquisition costs by marketing channel.

Now that we have a basic understanding of the definitions of both indicators, let’s explore the difference between KPIs and metrics further.

KPIs vs Metrics: What Is the Difference?



KPIs	Metrics
Measure progress towards key business goals	Measure performance of specific business activities or processes
They have a high-level perspective	They have a lower-level perspective
They are relevant across different departments	They are relevant for specific departments or business areas
Used for strategic decision-making	Tend to be operational or tactical

Differences Between KPIs vs Metrics

KPIs and metrics are often considered synonyms. But this is not how it actually works. While they are both quantitative measurements, they are used for different purposes. Simply put, KPIs need to be exclusively linked to targets or goals to exist, and metrics just measure the performance of specific business actions or processes. Let’s see some of the differences between the KPI and metrics in more detail.

- **Communication:** The first difference between KPIs and metrics is what they communicate. As mentioned above, KPIs are strategic indicators exclusively used to convey the progress of your business goals, and metrics are used to track specific areas or processes that might be working towards that goal. For example, if you want to sell 20% more next year, your main KPI would be the number of products or subscriptions sold to date. Now, to monitor the progress of that goal in detail, you would need to track various metrics such as the number of website visitors, best-performing sales channels, the performance of your sales agents, and any others that help you understand which actions are contributing to achieving your goals and what could be improved. In summary, a KPI can be seen as a collection of metrics that impact your journey toward achieving your goals.

- **Objective:** Another vital difference between a metric and KPI is the objective. A good KPI is always tied to the outcome. You expect it to go up or down to reach its target. Metrics, on the other hand, measure the impact of the day-to-day performance of different business areas, and as seen with the sales example, only some of them help you track the success of your strategic actions. The important takeaway is that metrics and KPIs are not mutually exclusive and are often taken as the same thing. A KPI will need a collection of metrics to track its success; you just need to ensure you are using the right ones. Remember: while all KPIs are metrics, not all metrics are KPIs.

- **Focus:** Another critical difference between metrics and KPIs is their level of focus. KPIs have a high-level perspective. They represent key business goals that are relevant for various departments. Conversely, metrics are considered lower-level indicators, and they track activities or processes specific to a department or business area. Following the example of increasing sales by 20%, each department will likely play a role in achieving that goal. For instance, the marketing department might need to focus on boosting promotions, the sales team might need to focus on developing strategies to efficiently turn leads into paying customers, the logistics team can focus on improving the shipping experience, and the product team can focus on finding strengths and weaknesses in production. Consequently, each department must track different metrics to achieve that general business goal.

KPIs vs Metrics Examples

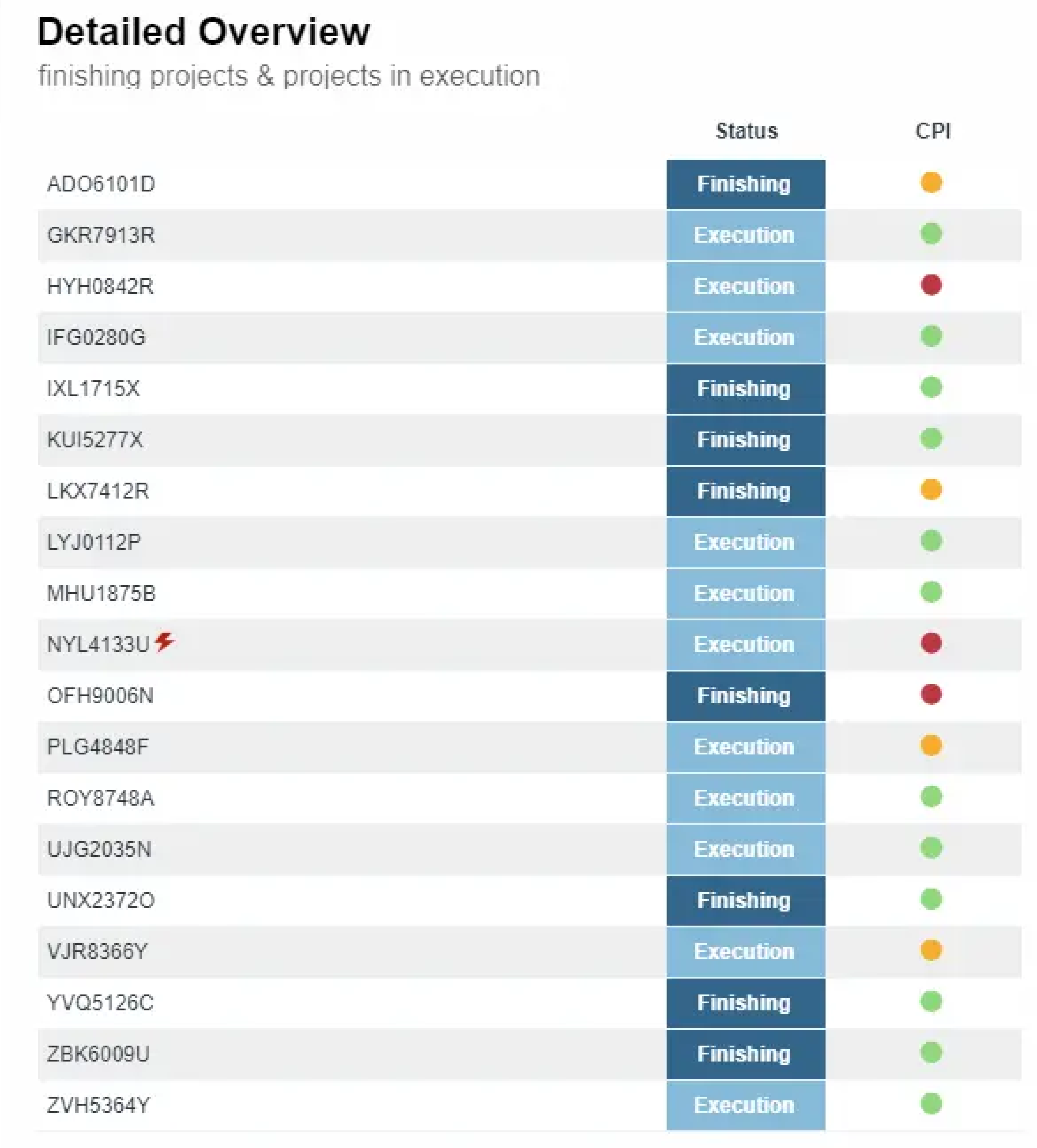
Let's put these differences into perspective with some metrics vs KPI examples!

1) Construction KPI vs. metrics

Delivering projects on time and, most importantly, within budget is one of a construction company's most relevant strategic goals. To do so, project managers must plan and schedule the tasks correctly and anticipate multiple challenges or potential issues to ensure the work is completed on time and with the expected quality. For our first example, we will discuss increasing the cost-efficacy of a company's construction projects. For this purpose, we will take the CPI as our main KPI. Let's explore it in more detail below!

- **KPI: Cost Performance Index (CPI)**

The CPI has become one of the most relevant KPIs for assessing project performance. It measures a project's cost and financial efficiency by comparing the value of the work completed to the actual costs. It is calculated using the following formula: CPI = earned value (EV) / actual cost (AC). A CPI higher than 1 means the project is cost-effective, and a CPI lower than 1 shows the project is over budget. The image below shows a table chart displaying the CPIs of different projects. The colors following each project show the status of the CPI, with green being over 1, yellow being risky, and red being negative.



Detailed Overview

finishing projects & projects in execution

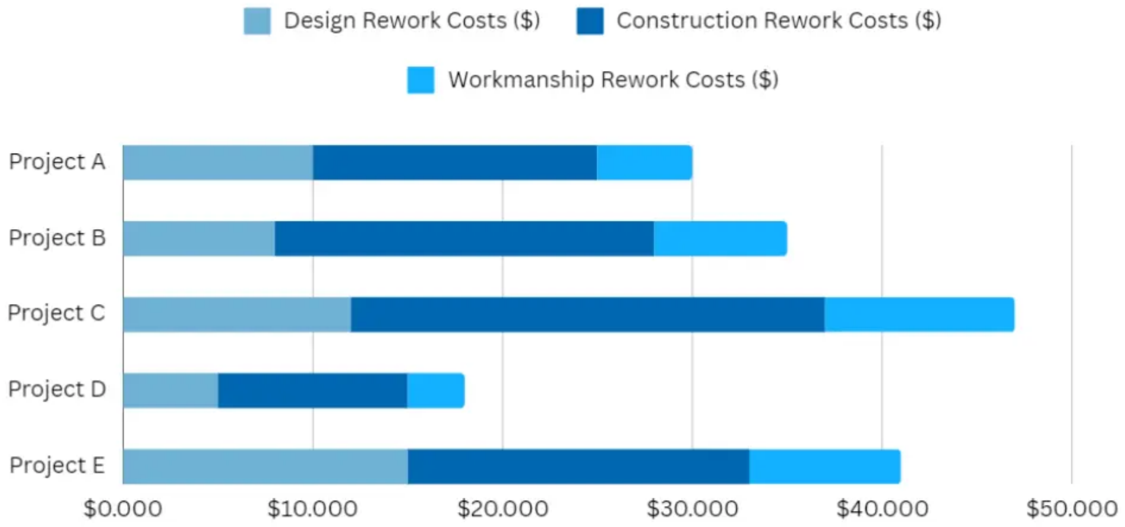
	Status	CPI
ADO6101D	Finishing	🟠
GKR7913R	Execution	🟢
HYH0842R	Execution	🔴
IFG0280G	Execution	🟢
IXL1715X	Finishing	🟢
KUI5277X	Finishing	🟢
LKX7412R	Finishing	🟠
LYJ0112P	Execution	🟢
MHU1875B	Execution	🟢
NYL4133U ⚡	Execution	🔴
OFH9006N	Finishing	🔴
PLG4848F	Execution	🟠
ROY8748A	Execution	🟢
UJG2035N	Execution	🟢
UNX2372O	Finishing	🟢
VJR8366Y	Execution	🟠
YVQ5126C	Finishing	🟢
ZBK6009U	Finishing	🟢
ZVH5364Y	Execution	🟢

Construction CPI Overview for Multiple Projects

If you know anything about construction, you know that building projects are never static. Many factors can impact on your CPI. Some are external, such as a rise in material or labor costs, weather conditions, or economic conditions, while others are internal, like overlooked risks, low labor productivity, or mistakes during preconstruction planning and design, which leads us to our metric example.

- **Metric: Rework Costs**

Reworks are common in construction projects. They refer to any work that needs to be done again or adapted due to a mistake or an unforeseen situation. In most cases, reworks can be avoided with efficient planning and risk management. However, issues with construction communication and collaboration can lead to mistakes in the project's early stages, which can then impact the following stages.



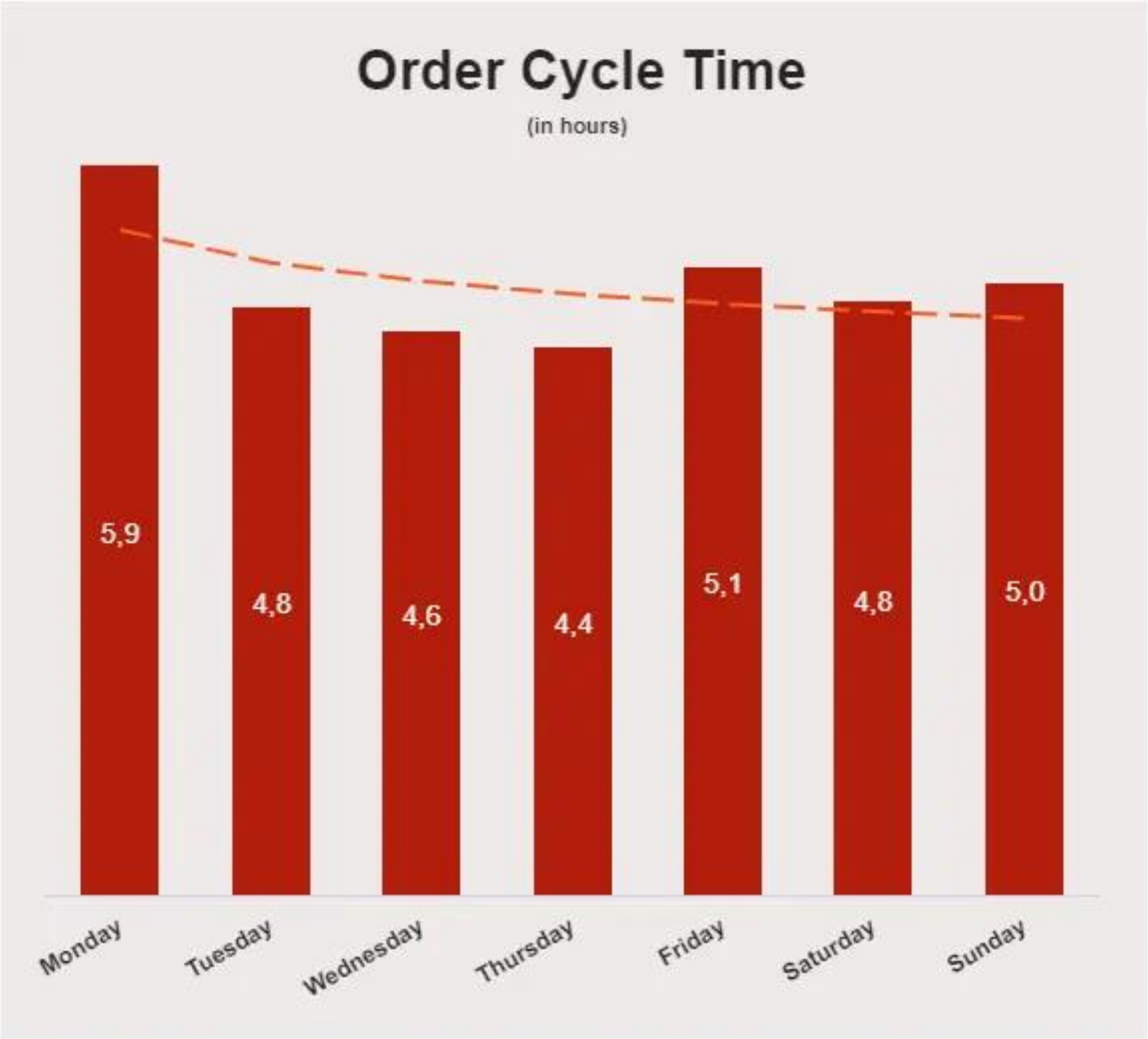
Rework Costs for A Construction Project

Reworks can directly affect a project's CPI because they increase costs beyond the budgeted amounts for that specific work, meaning the value earned from that work does not align with its costs. Therefore, tracking it closely is of the utmost importance. In this case, the rework costs are tracked for multiple projects and categories. Project C has the highest rework costs in all categories, meaning issues in design probably affected the rest of the project. This needs to be analyzed further to extract insights and learn from them.

2) Logistics KPIs vs metrics

Ensuring the entire supply chain is efficient in logistics and warehouse management is paramount to success. One of the most popular KPIs to measure success is order cycle time, which measures the time it takes a company to ship an order from the moment it was placed until it leaves the warehouse, without considering shipping time. Naturally, businesses want to keep this KPI as low as possible, as it means all areas of the supply chain, including inventory management, picking, and packing, and transportation, are working as expected. Let's explore this in more detail below.

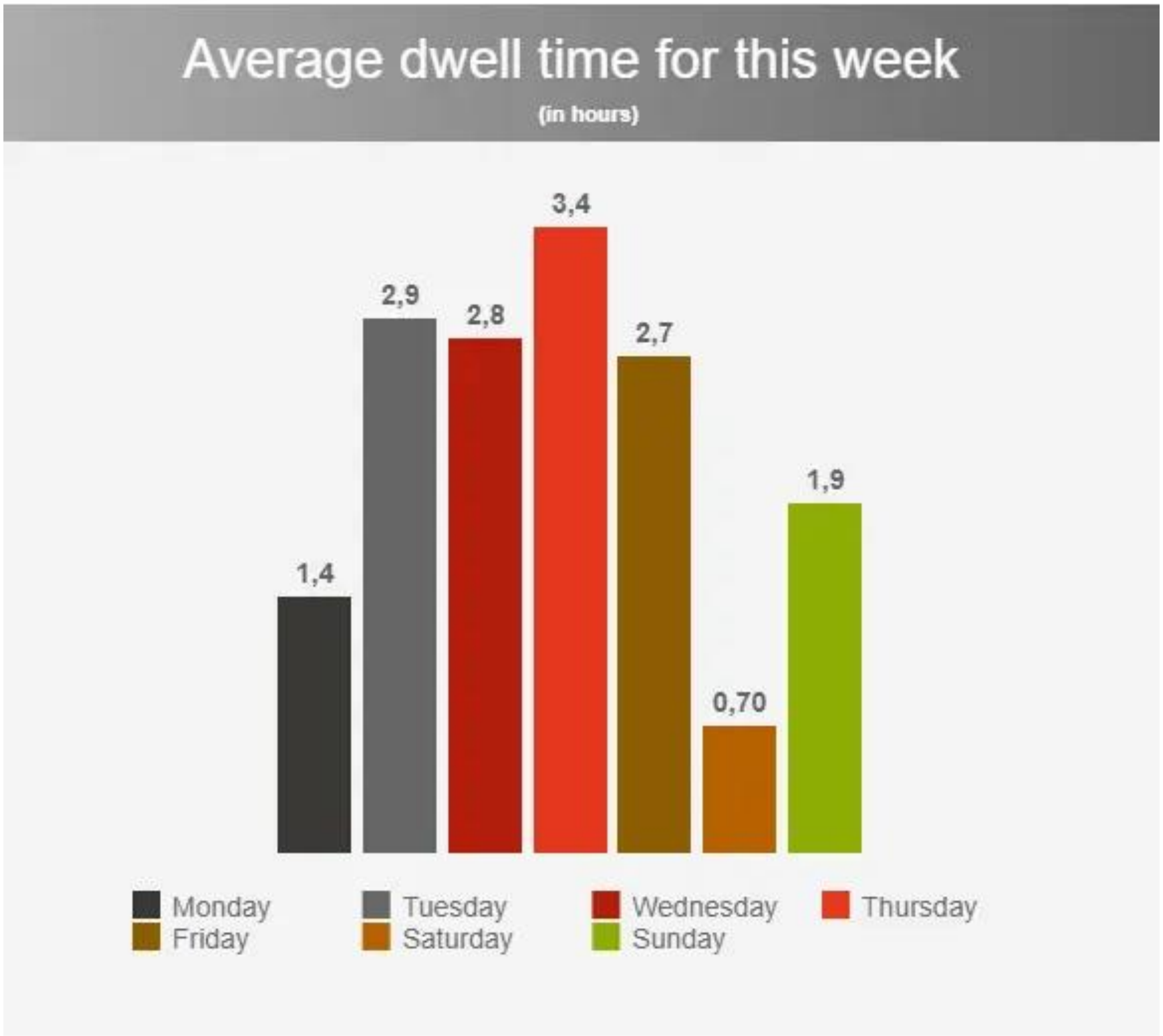
KPI: order cycle time



Construction KPI Tracking the Order Cycle Time

The order cycle time is an important KPI as it can shine a light on other issues in your supply chain. It is used to evaluate the efficiency of fulfillment processes and can significantly influence customer satisfaction. Unlike other KPIs mentioned above, the order cycle time needs to be tracked in shorter periods, such as weekly or daily, as it can be affected by multiple unexpected factors, like an influencer sharing your product and generating an unexpected increase in demand. That said, without considering unexpected events, this KPI can still be optimized by measuring different metrics. Below, we will discuss an example of one.

- **Metric: dwell time**



Average Dwell Time By Week Day

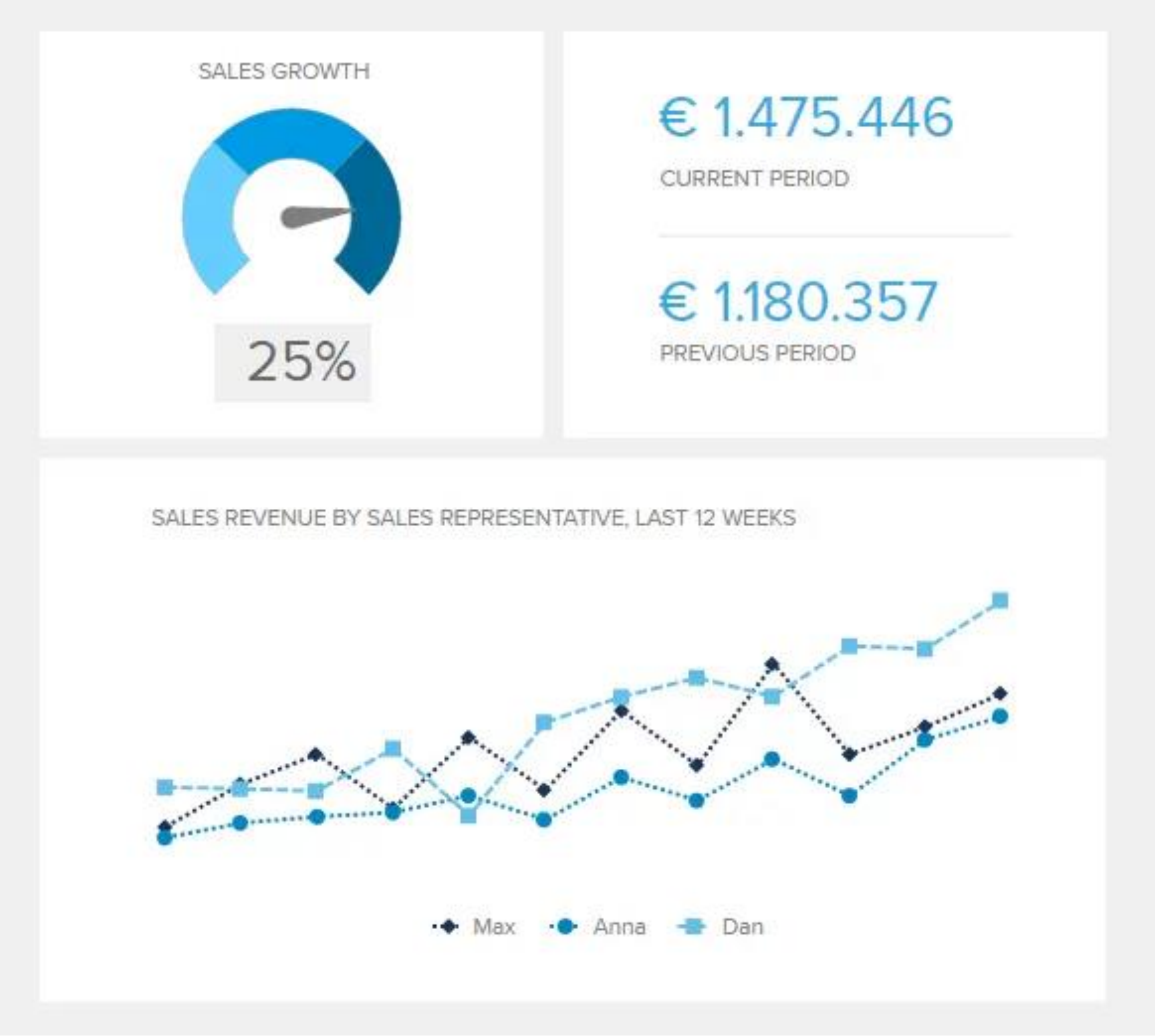
As mentioned above, many processes and people are involved in achieving a successful order cycle time. Therefore, there are several metrics, including picking accuracy, shipping time, equipment utilization, inventory accuracy, and many more, that you can measure to evaluate and optimize your order cycle time in a professional online dashboard. Today, we will focus on dwell time. This metric measures the average number of hours drivers spend in the warehouse waiting for orders to be loaded or unloaded from the trailer. Some of the most common reasons for an increase in dwell time include vehicle delays, loading complex or heavy orders, tedious check-in processes, and order volume, among others.

It is important to mention that having some dwell time is unavoidable and should be considered in your order cycle calculations. However, some of the reasons we just mentioned are easily preventable. Therefore, you should closely monitor the metric to ensure you can spot solvable inefficiencies as soon as possible.

3) Sales growth metric and KPI

Let's explore our example of increasing sales by 20% by the end of the year in more detail. A big goal like sales growth is relevant to various departments across a business, such as management, sales, marketing, and production. Each department tracks its own metrics to understand how its activities contribute to the general goal. Here, we will focus on a sales metric vs. KPI example.

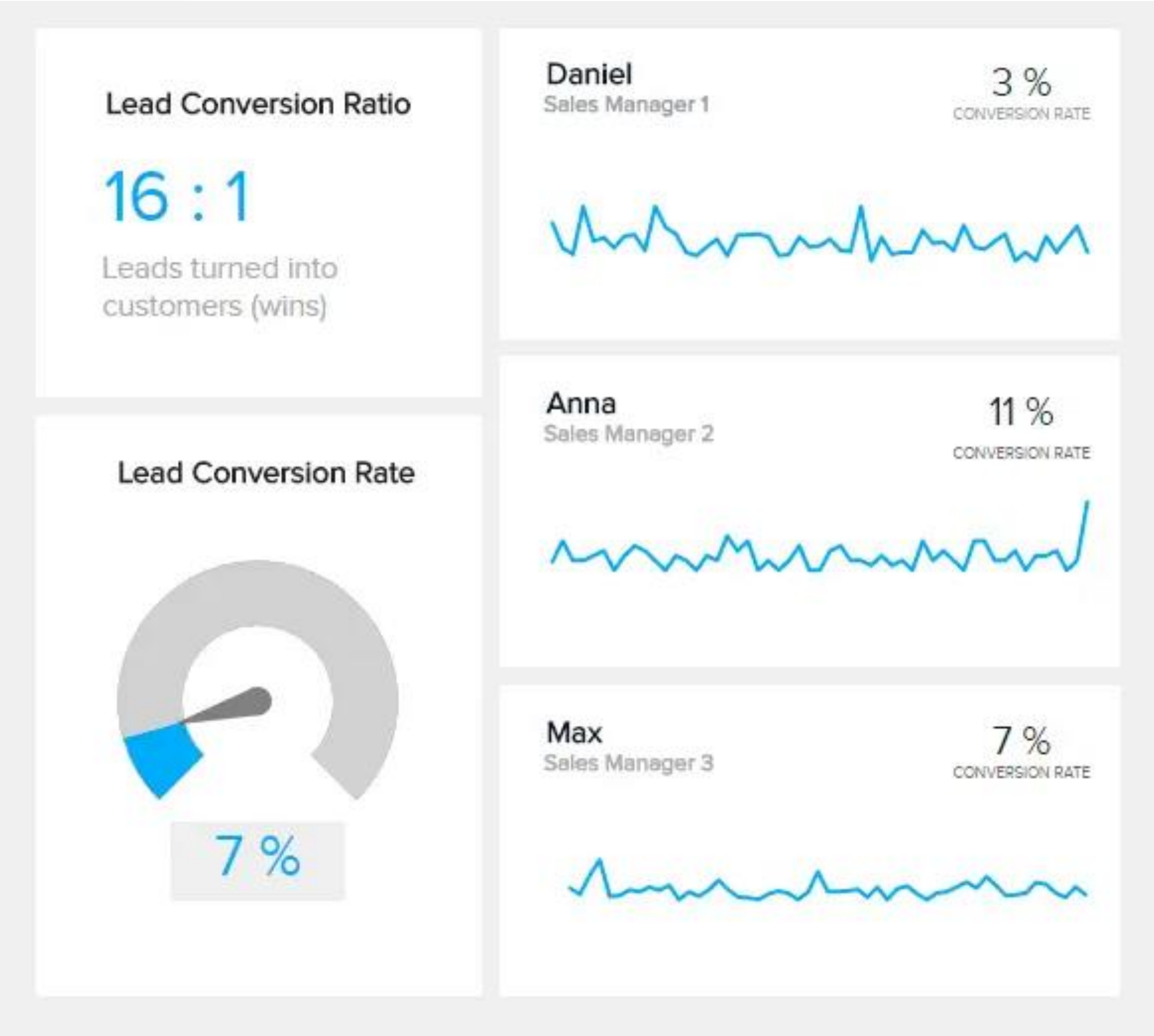
- **KPI: Sales Growth**



Sales Growth Tracked For The Last 12 Weeks

The image above visually represents our main KPI: sales growth. With information such as the current period vs. the previous one, the percentage of sales based on a target, and sales revenue by a sales representative, we can see at a glance if targets are being met or not. But to finetune the strategies, we also need to know how the different activities are performing, which can be done with the help of various sales metrics.

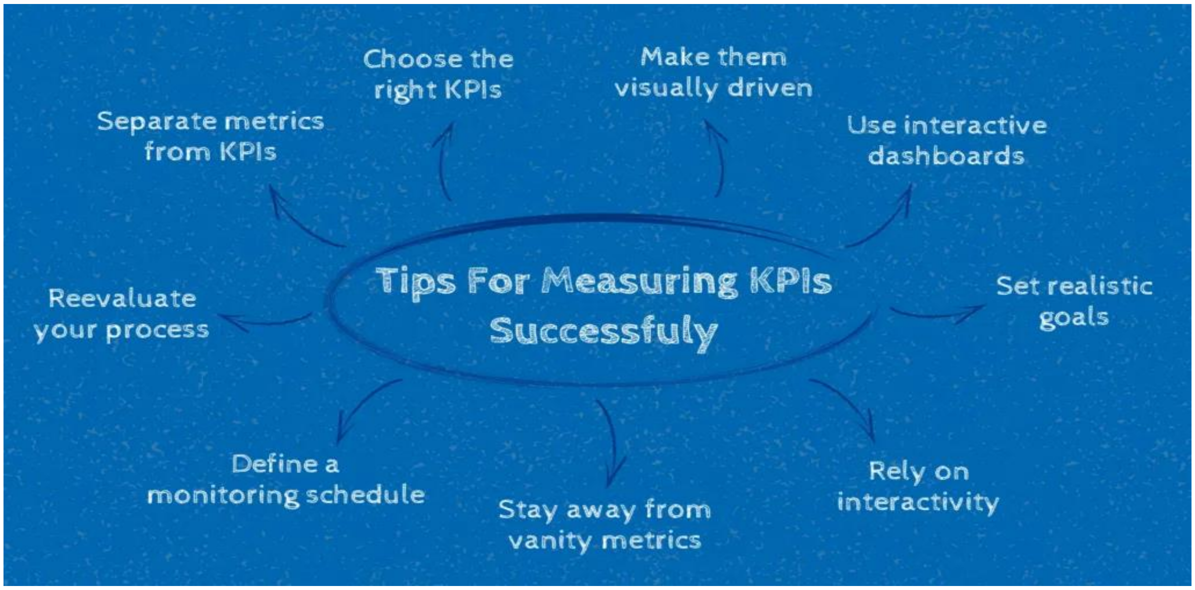
Metric: Lead to conversion ratio



Lead To Conversion Ratio Tracked For Different Sales Managers

The lead-to-conversion ratio is a great sales metric to measure for this specific goal. It measures the number of interested people who actually end up turning into paying customers. Which eventually translates into an increase in sales. This metric, generated with professional sales reporting software, is helpful as it provides deeper insights to make strategic decisions. If your lead conversion rate is low, you must consider alternatives to motivate potential customers to become actual customers. Other metrics to measure for this goal include the lead-to-opportunity ratio and net profit margin, among others.

Tips & Best Practices For Measuring KPIs And Metrics In The Right Way


Choose the right KPIs
Make them visually driven
Separate metrics from KPIs
Use interactive dashboards
Tips For Measuring KPIs Successfuly
Reevaluate your process
Set realistic goals
Define a monitoring schedule
Stay away from vanity metrics
Rely on interactivity

Tips To Measure KPIs Successfully

We've covered the definition of key performance indicators and metrics and discussed the differences between business metrics vs KPIs. In this section of the post, we will discuss five tips for efficiently measuring your goals and performance.

1. Separate metrics from KPIs

Measuring everything really means measuring nothing. When separating KPIs from metrics, you must consider what is most important for your business. Any indicator can be a metric, but if it does not provide valuable information to improve, you should discard it.

Tracking the wrong metrics can lead to a waste of time and resources that could be easily avoided. Measuring too much can get confusing and misleading. To prevent this, pick only the KPIs that add value to your goals and leave any unuseful information behind. More on this in the next point.

2. Choose the right KPIs

Choosing the right KPIs to measure is the most important step in tracking your strategies efficiently. To help with this purpose, there are some KPI tracking techniques that you can use. Here, we will explain two of them: the SMARTER and the Six A's methods.

- SMARTER: This KPI tracking practice stands for Specific, Measurable, Attainable, Relevant, Time-bound, Evaluate, and Reevaluate. It works as a list of requirements your KPIs must meet for validity. As mentioned throughout this post, they should be specific to your goals, realistic to your business reality, and flexible to change with the evolution of strategies.
- Six A's: This method stands for Aligned, Attainable, Acute, Accurate, Actionable, and Alive. Like the SMARTER criteria, this practice also aims to evaluate the relevance of a KPI, and it

is useful for businesses that have too many indicators and need to narrow them down to a few.

By applying these methods, you should be able to narrow it down to 2-5 critical KPIs per business goal. This helps you keep your analysis process specific and avoid misleading information that can affect how you interpret your data.

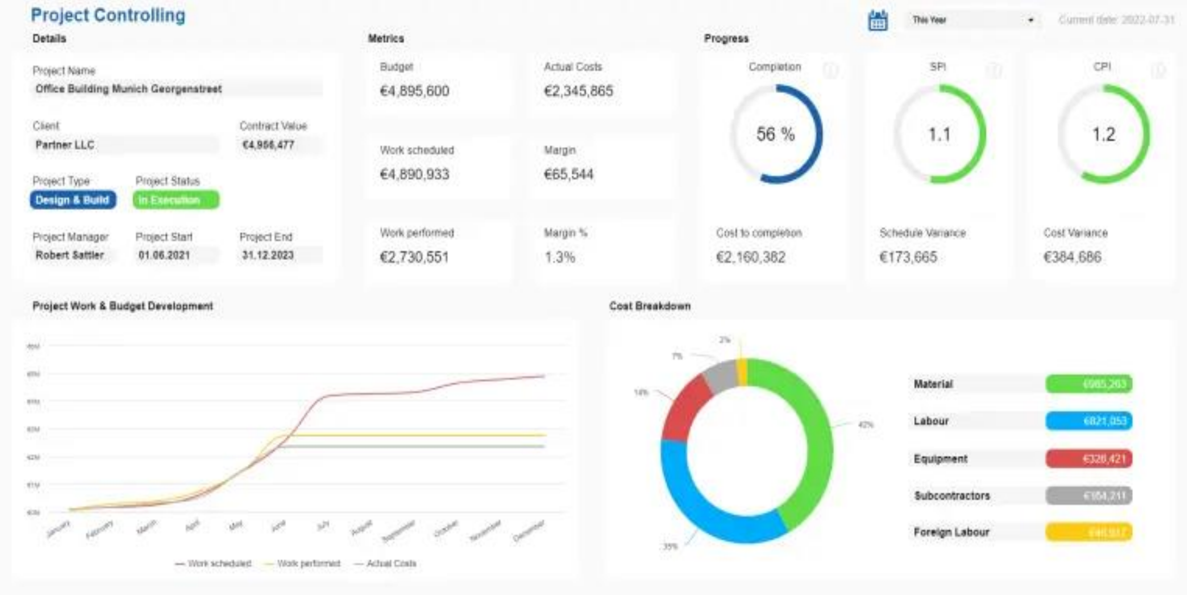
An important thing to remember here is that you should always revisit your KPIs. If you find a better approach to achieving your goals, you should ensure you are tracking the right data. You can do this by monitoring your KPIs regularly with weekly or monthly reports. Once your KPIs have been defined, you have all the information you need to start making strategic decisions and thinking about long-term actions.

3. Make your KPIs and metrics visually driven

Once you've selected your KPIs and metrics, it is time to transform them from plain values and numbers into actionable insights. This is done through various data visualizations that will help you tell a story with your indicators and collaborate through them. Plus, it is a well-known fact that the human brain processes visual information way faster than numbers, making it more accessible and easier to understand for a wider audience. Therefore, picking your graphs and charts carefully can make a difference in your analysis process. That said, it is more challenging than picking a KPI and representing it with a pie chart. Each type of graph and chart has its own purpose and use cases, and you should be careful when picking them. We recommend carefully considering your goals and what you are trying to communicate and choosing the visual that best suits your needs. This is an important point, as picking the wrong visual can mislead your analysis and damage your strategies.

4. Get a centralized view with an interactive dashboard

KPIs and metrics are valuable tools for businesses. While key performance indicators tend to be more important, metrics are also helpful to get a bigger picture of the performance of a department or specific area. Today, several data visualization tools offer a range of dashboard options to visualize your KPIs and metrics in a centralized way. Let's look at it with an example from the construction industry.



Project Controlling

This Year
Current date: 2022-07-31

Details

Project Name: Office Building Munich Georgenstreet
Client: Partner LLC
Contract Value: €4,956,477
Project Type: Design & Build
Project Status: In Execution
Project Manager: Robert Sattler
Project Start: 01.06.2021
Project End: 31.12.2023

Metrics

Budget: €4,895,600
Actual Costs: €2,345,865
Work scheduled: €4,890,933
Margin: €65,544
Work performed: €2,730,551
Margin %: 1.3%

Progress

Completion: 56 %
SPI: 1.1
CPI: 1.2
Cost to completion: €2,160,382
Schedule Variance: €173,665
Cost Variance: €384,686

Project Work & Budget Development

Cost Breakdown

Project Controlling Dashboard Template

The example above, generated with professional construction analytics software, offers the perfect overview of KPIs and metrics to track project performance. The indicators presented in this dashboard are updated in real-time, making it possible to spot any issues early and tackle them to prevent damage. In this case, we can see that the project is 56% complete, with a positive SPI and CPI of over 1. Which means the project is going according to the planned budget and schedule. This could easily change, so it is important to monitor progress closely.

5. Rely on interactivity

Interactive data analysis has become one of the most significant competitive advantages in the analytical world today. Think about your analytical process as a movie. Your KPIs are the main characters that help you achieve your goals, and your metrics are the side characters that will help you measure the performance of your strategies towards achieving those goals. Your dashboards are the scenery where everything comes together, and you can tell your data story. And interactivity will help you bring everything to life in a compelling way.

Modern KPI reporting tools provide multiple interactivity features to help you navigate and explore your data more thoroughly. For example, a drill down feature enables you to go into lower levels of hierarchical data all in one chart. Let’s say your goal is to increase sales in the US. For that, you are visualizing a chart with sales by country. A drill down would enable you to click on the USA value and adapt the entire chart to see sales by state. Likewise, an even deeper drill down would help you see sales by city or state. Other interactivity options allow you to change the period, translate the text in your charts, and much more.

By making your KPIs and metrics interactive, you’ll ensure that you can extract their maximum potential. A static view of data no longer cuts in today’s fast-paced world, where decisions must be made in an accurate and agile environment.

6. Stay away from vanity metrics

Vanity metrics refer to the indicators that may look good on paper but do not help inform future business strategies. In some cases, vanity metrics are used to show improvement, but they are actually indicators that are not actionable or related to anything you can consider really significant. A great example of a vanity metric would be with social media followers. Imagine you implemented a campaign that attracted 10.000 new followers to your Instagram. Now, that might seem like a success at first hand, but if from those 10,000 followers, only 50 bought your products or service, then the metric becomes useless.

To avoid facing the issue of vanity metrics, you need to keep your analysis as objective as possible. When choosing the KPIs and metrics you will monitor, always ensure they reflect the truth. While metrics such as the number of followers or likes might seem exciting, they can also point you in the wrong direction. BI tools offer various KPI and dashboard templates that can point you in the right direction to avoid making this mistake.

7. Set realistic targets

The next tip for measuring metrics and key performance indicators correctly is setting achievable targets. For your KPIs and metrics to be efficiently measured, you need to know where you are headed and what targets make this possible. Here, you need to be careful not to set unrealistic targets, such as a 50% increase in sales in a year when your average increase in the past years has been 5%. When building targets, consider attainable values based on your business context as well as some industry benchmarks. This way, you will ensure you are working towards achievable goals and avoid getting stacked or disappointed by setting unrealistic values.

8. Define a monitoring schedule

Another great practice that will help you measure your metrics and KPIs successfully is to define a monitoring schedule. This will help you stay on top of any insights while still having time to plan and carry out your strategies. Since metrics often track more operational activities, they can be monitored on a short-term basis and even in real-time. On the other hand, KPIs often track strategic goals that are more meaningful when tracked for a more extended period, such as a month, a quarter, or even a year.

Specialized BI tools like professional construction business intelligence software provide intelligent data alerts that will notify you as soon as your KPIs and metrics need your attention. All you have to do is predefine a goal or a threshold value, and the tool will notify you as soon as it is achieved, leaving you more time to focus on other important tasks rather than constantly monitoring your data.

9. Reevaluate your process

As you've learned by now, choosing KPIs and metrics is not a task that can be taken lightly. You need to line up a well-thought-out plan to ensure you are tracking the data that will help you measure the success of your strategies and goals and find improvement opportunities to grow constantly. And, just like many other business-related processes, it requires reassessments to be successful. Our advice is always to take the time to rethink your strategy. Are these metrics still valuable for measuring our efforts? Should we add a couple more? Are they still aligned with our goals?

Doing so will ensure that your resources are used well and that your efforts pay off with successful strategies and continuous organizational growth.

Key Takeaways from KPIs vs. Metrics

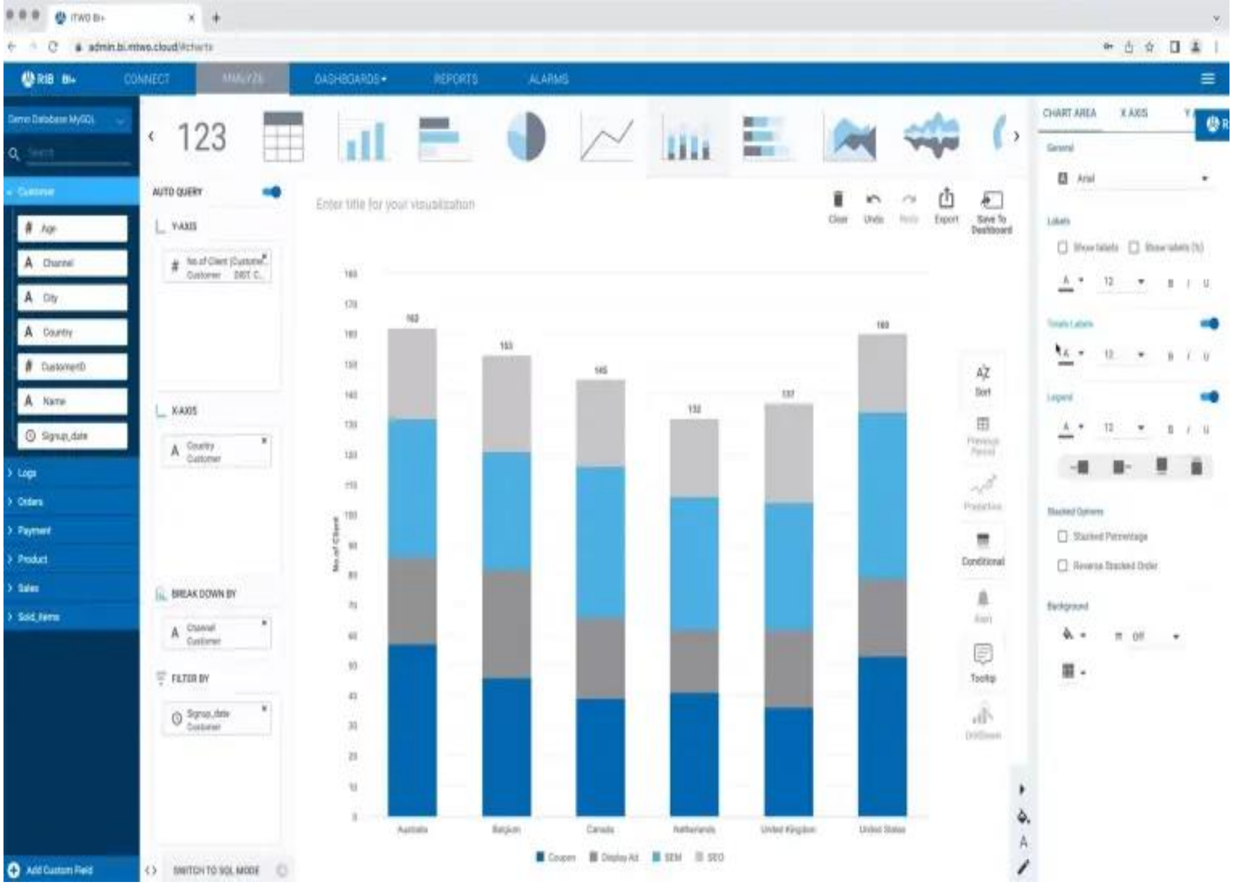
As we reach the end of this post about key performance indicators vs. metrics, we hope you have a deeper understanding of how these two differentiate themselves. The important takeaway from this post is to remember that there would be no KPIs without metrics; both are critical to ensuring a healthy return on investment from your different business activities.

KPIs and metrics are invaluable tools for performance tracking. Every day, more businesses turn to specialized software to get a centralized view of their most important indicators interactively and intuitively. Access to modern dashboard technology allows teams to stay connected and work together towards common business goals.

To keep your mind fresh, here is a small summary of the main differences between metrics and KPIs:

- KPIs measure performance based on key business goals, while metrics measure performance or progress for specific business activities.
- KPIs are strategic, while metrics are often operational or tactical.
- Metrics are lower-level indicators specific to a department, while KPIs can be tracked by various departments working towards the same goal.
- Metrics provide context for your business activities, and KPIs allow for strategic decision-making.

If you are ready to start boosting your construction project's performance with the help of informed decision-making, then try the RIB Software toolkit today. Our construction analytics solution, RIB BI+, offers companies in the building environment professional features to manage their data in real-time and use it to collaborate and boost efficiency. Book a demo today to benefit from the power of professional data analysis!



RIB BI+ ▷ The Best Construction Analytics & Dashboards

Unit Four : Developing and building action plan

At the end of the unit, the trainee will be able to:

- To explain the importance of developing a business plan

- To mention an example of a development plan

- To identify the steps of developing a business plan

- To explain the importance of improving processes and businesses

- To mention the types of process improvements

- To mention examples of continuous improvement

- To explain how to create an environment for continuous improvement

- To show the benefits of continuous improvement

Lesson1 : Developing and building action plan

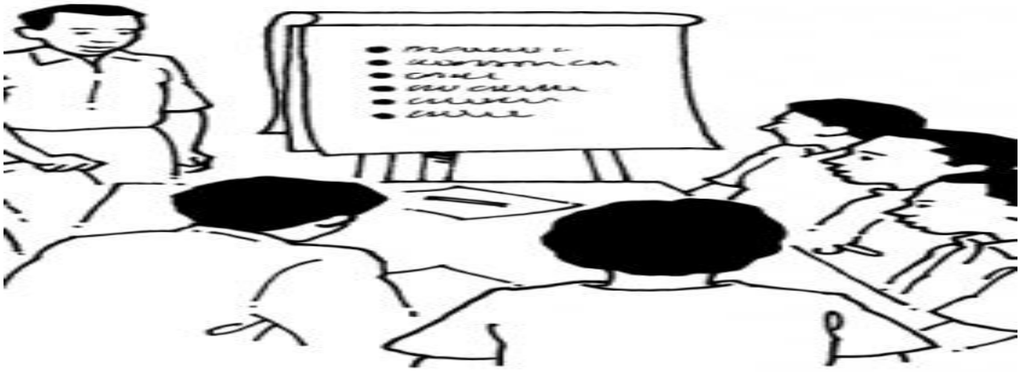
Developing an action plan

The Development Action Plan (DAP) is a systematic plan for focusing employee growth during the next year. It focuses on areas that you want to develop in order to grow in your job or to advance your career.

Developing an action plan means turning ideas raised during strategic planning or evaluation into reality. It means identifying the steps that need to be taken to achieve the resource centre's aims. The resource centre officer and their manager or supervisor should develop the action plan, in consultation with members of the resource centre advisory committee and/or other users.

What is an example of development plan?

Examples include building leadership skills, nurturing self-management abilities, and improving critical thinking approaches. Common employee development plan examples include general soft skills training, exposure to leadership roles, and succession planning.



It is useful to have action plans for each area of the resource centre's work, such as:

- fundraising
- selecting and ordering materials
- organizing materials
- computerization
- providing information services
- promoting the resource centre
- networking and cooperation.

How to develop an action plan

An action plan consists of seven steps: setting objectives, assessing the objectives, identifying action required to meet the objectives, working out how to evaluate the activity, agreeing a time-frame for action, identifying resources (human, financial and technical), finalizing the plan, and evaluating the results.

1. Set objectives

You need to identify clear objectives that will guide your work to achieve the resource centre's aims. Objectives need to be achievable - do not be over-ambitious. They need to be measurable (for example, a certain number of activities carried out within a certain period), so that you can know whether you have achieved them.

Ask yourself:

- What do we want to achieve?
- Example of an aim: To disseminate information that will improve local health workers' knowledge of local health problems.
- Example of an objective: To produce and distribute an information pack on malaria diagnosis and management to all health clinics in the district within the next three months.

2. Assess the objectives

Assessment helps to determine whether or not the objective is appropriate. It may result in confirming the objective, abandoning it or revising it. Ask yourself:

- Is the objective compatible with the resource centre's aims and objectives?
- Are the necessary resources (funds, equipment, staff) available to reach this objective? If not, are they obtainable?
- What problems might arise in working to achieve this objective?
- Example of resources needed to carry out the objective: staff time, relevant materials in the resource centre or obtainable from elsewhere, stationery, photocopier, postage.

- Example of revised objective: To produce and distribute an information pack on malaria diagnosis and management to 20 health clinics and training institutions within the next six months.

3. Identify action required to achieve the objective

A series of tasks needs to be identified for the objectives to be achieved. List these as steps.
Ask yourself:

- What tasks are necessary, in what order, to meet the objective
- Example:

1. Plan the content of the information pack and decide how to distribute the packs, in consultation with other staff and users.
2. Calculate costs and staff time, and make sure that funds and time are available.
3. Allocate responsibilities.
4. Gather information for the pack (search resource centre, contact other organizations).
5. Request permission from publishers to photocopy material.
6. Photocopy material and prepare packs.
7. Distribute packs.

4. Work out how to evaluate the activity

Plans for finding out how far the activity has achieved its objectives need to be built into the action plan. Ask yourself:

- How will we know whether we have achieved our objectives
- Example:
    - Contact five clinics to see whether they have received the packs.
    - Include an evaluation form in the pack, asking health workers whether the information has improved their knowledge, how they have used the information, and how future packs could be improved. Assess the feedback from the forms.

Then incorporate plans for evaluation into your action plan.

- **Example(showing plans for evaluation in bold italics):**

1. Plan the content of the information pack, including evaluation forms, and decide how to distribute the packs, in consultation with other staff and users.
2. Calculate costs and staff time, and make sure that funds and time are available.
3. Allocate responsibilities.
4. Gather information for the pack (search resource centre, contact other organizations).

5. Request permission from publishers to photocopy material.
6. Prepare evaluation forms.
7. Photocopy material, prepare packs.
8. Distribute packs.
9. Contact clinics to see if they have received packs.
10. Revise plans for distributing packs if they have not reached some clinics.
11. Assess the feedback from the evaluation forms and use it to plan future work.

5. Agree a time frame

As you identify each task, work out how long it will take and when it needs to be done. This will help you to see whether your action plan is on schedule or whether you need to modify the schedule.
Ask yourself:

- What is the actual time required for each individual task? (Be careful not to under-estimate)
- When will each step be completed?
  Example: Total of 18 days over a three-month period

6. Assess the action plan

Ask yourself:

- How will you know whether the individual tasks have been achieved?
- Have you allowed for possible interruptions?
- Have you tried to do too much or too little?

An action plan must be realistic if it is to work. It is easy to over-estimate what you can do, leading to disappointment and failure. For example:

1. Leaflets that you had planned to include in the pack may have run out and need to be reprinted. Can you substitute something else, or will you need to arrange for them to be reprinted before you can finish preparing the packs?
2. The member of staff preparing the pack will take annual leave for six weeks during the period in which the pack was planned to be prepared. Can you re-schedule the work, or can someone else do it?

7. Finalise the action plan

Revise the action plan. Obtain feedback and comments from colleagues, and revise it again if necessary

Tool 1: Action Plan Form

Action Plan for [Community or Initiative Name]

Community Focus Area: __________________

Community Change to be Sought:
____

Collaborating Organization(s)/Group(s):________________ Community Sector: _________________

Action Steps

Action Steps	By Whom	By When	Resources and Support Available / Needed	Potential Barriers or Resistance		Communication Plan for Implementation
What needs to be done?	Who will take actions?	By what date will the action be done?	Resources Available	Resources Needed (financial, human, political, and other)	What individuals and organizations might resist? How?	What individuals and organizations should be informed about / involved with these actions?
Step 1: By_____						
Step 2: By ______						
Step 3: By ______						
Step 4: By ______						

Tool 2: Tips for Action Planning

What is an action plan?

An action plan is an opportunity to turn your dreams for your community or initiative into a reality. It is also an opportunity to make your organization's vision concrete. An action plan outlines the strategies and action steps your organization will use to meet its goals and objectives.

Why develop an action plan?

Developing an action plan is a critical first step toward ensuring project success. An action plan may lend credibility to your organization and its initiative, increase efficiency, and provide accountability. In addition, the action plan provides a tool for mobilizing the community or group and encouraging members to share responsibility for solving the problems and improving the situation you have decided to change.

Who develops the action plan?

You can invite these people to help prepare an action plan:

- Influential people from all groups affected
- People directly involved in the problem or issue
- Members of grassroots organizations
- Members of ethnic and cultural groups of the community
- Different sectors of the community: media/business community/religious groups/schools/youth organizations/social service organizations/health organizations

How do I develop an action plan?

First, clarify your charge. Is it to work to reduce adolescent pregnancy in your community? Or are you working to increase the rate of home ownership? Your goal will provide the backbone of your action plan.

Your action plan should include the strategies you plan to use and the action steps you will take to achieve your goals and objectives. It should also identify a role for each sector of the community or group involved in your effort.

For each action step or change to be accomplished, list the following, with a due date for each:

- What actions or changes will occur-by when?
- Who will carry it out-by when (or for how long)?
- What resources are needed-by when?
- Communication (who should know what)-and when?

Tool 3: A Successful Planning Process

Adapted from an Action Planning Guide for Community-Based Initiatives, the University of Kansas Center for Community Health and Development

Be inclusive

Good planning is active and inclusive. Seek out key players with diverse viewpoints on the problem or issue. Once a diverse group of important players is at the table, it is important to get them to communicate with each other. Effective leaders often call on silent members during pauses in the discussion. They convey the value of each person's voice on the issues. Occasionally, it may be necessary to discourage an overly enthusiastic member from talking too much or dominating meetings. Leaders may do so by thanking them for their comments and indicating the importance of hearing from other members of the group.

Manage conflict

If the group is effective in attracting diverse views, conflict among members may result. Group facilitators can recognize differences, perhaps noting the diverse experiences that give rise to divergent views. To resolve conflicts, leaders may attempt to elevate the discussion to a higher level on which there may be a basis for agreement. By reminding the group that we all share the vision of a healthy community, leaders can help members find common ground.

Use brainstorming rules

Group facilitators must avoid making judgments about ideas and suggestions. Brainstorming rules apply. All ideas must be heard and noted without criticism.

Be efficient

Planning meetings must be efficient, starting and ending on time. It is helpful to have an agenda or to build a consensus at the beginning of the meeting about what will be accomplished and in what time frame.

Communicate products of planning

Planning will result in a useful product. Try to structure every planning session so that it results in a product, such as a list of issues or ideas. Show off the product at the end of planning meetings, distributing copies of the products of planning to all members.

Provide support and encouragement

Finally, it is important to provide support and encouragement throughout the process of planning. Good planning takes time; it usually requires months to produce a detailed plan of action. Acknowledge the contributions of all participants, especially key leaders. Let the group know when it is doing a good job. Positive feedback feels good, particularly to those who are used to being criticized for their work.

Tool 4: Action Planning Guides from the KU Center for Community Health and Development

Community and Public Health Action Planning Guides

- Reducing Risk for Chronic Disease
- Promoting Health for All: Improving Access and Eliminating Disparities in Community Health
- Promoting Healthy Living and Preventing Chronic Disease

Child and Youth Health and Development Action Planning Guides

- Preventing Adolescent Substance Abuse
- Preventing Adolescent Pregnancy
- Preventing Youth Violence
- Preventing Child Abuse and Neglect

- Youth Development
- Promoting Child Well-Being

Community Development and Capacity Building Action Planning Guides

- Promoting Urban Neighborhood Development: Improving Housing, Jobs, Education, Safety and Health, and Human Development
- Work Group Evaluation Handbook
- Concerns Report Handbook: Planning for Community Health

Tool 5: Action Planning Guide

Download Your Action Planning Guide for Promoting Full Community Participation Among People with Disabilities (pdf), a resource for independent living centers and other community-based initiatives, developed by the Research and Training Center for Independent Living and the Center for Community Health and Development at the University of Kansas.

Lesson2 : Developing continuous review and improvement processes

Continuous Improvement Examples You Need to Know

Process Improvement

There isn’t a business leader out there that would say no to being able to improve their business. In whatever capacity it may be, business improvements should be constant within an organization. A process called continuous improvement provides precisely this value. With a continuous improvement example, as well as techniques, this article will showcase how you can help your business operate better.

Business improvements not only benefit the bottom line, but they also improve quality, safety and both employee and customer satisfaction. 54% of continuous improvement enhancements increase customer satisfaction.

Whether you know what you need to improve or not, this article will provide you with everything you need to know about continuous improvement, as well as implementation examples that could greatly benefit your organization.

Table of Contents

1- What is Continuous Improvement?

First things first, let’s define what continuous improvement means. With its roots in manufacturing, continuous improvement is a method that strives to locate opportunities for ensuring efficiency, continuously. This involves the assessment of current processes, products and services to ensure that output is maximized and waste is minimized.

Continuous improvement benefits internal and external stakeholders, from employees to customers and investors alike. But, continuous improvement isn’t a one-and-done deal that a company performs and then forgets. If the name doesn’t give it away, let’s drive this fact home - the method is continuous, as in, it does not have an end. It’s a method that becomes a part of a business’ ongoing operations. You can consider it to be like a way of life, rather than something new you might try once. But, even though it becomes a part of your business, it still requires strategy and methodology to impact change.

Since continuous improvement becomes a way of operating, this means that everyone must be on board. So, creating a culture of improvement is a priority to make it work. This can be done by empowering everyone within an organization to understand that they can point out places for development to spark positive change.

2- Types of Process Improvement

There are various methods for process improvement. We’ll briefly define three kinds and then move into examples of continuous improvement.

- **LEAN Technology:** Created by Toyota to optimize its production cycle, LEAN improvement is customer-focused. It defines what customers value from the process most to determine what can be eliminated from the production of a product to decrease waste and cut costs.

- **Six Sigma:** Six Sigma is a method that focuses on improving the quality of business processes. It’s aimed at limiting the variation in processes to ensure consistency and increase performance. It uses statistics to measure deviations from a defined centre line on a control chart.

- **Total Quality Management:** With some similarity to Six Sigma, Total Quality Management (TCM) holds all involved parties responsible for producing quality outputs. It looks to standardize processes to reduce errors.

3- Continuous Improvement Examples

Now that you understand what continuous process improvement is, it'll be helpful to see the theory applied in a business setting.

Here's a look at eleven examples of continuous process improvement and where you can use it during your day-to-day practices:

1. Ideation and Think Tanks:

Initiating regular think tanks and ideation sessions can benefit your organization. You can choose to run think tanks with an agenda in mind or at the very least, elicit the attendance of key personnel so that valuable ideas are discussed. During these sessions, you can explain how processes are currently being run to see if there are places that need to be improved and changes to be made. Often, since technology is so intertwined with most business processes, a starting point is to discuss updates and new technology solutions geared towards optimization. For example, automation solutions are becoming increasingly necessary for businesses to remain competitive.

2. Surveys and Polls:

The people who work within your organization are the most well-versed to know where improvements can be made. It's not only important to gain feedback from customers and vendors, but important and often overlooked is employee feedback. By polling your team, you can find out their pain points and find places for improvement. As a business leader, you spend most of your time on the big picture, so the smaller details that significantly affect your business' outputs can go unnoticed without such insight.

3. Monthly Training:

In big businesses, especially, it is common that each employee works within a silo or “swim lane.” But, both cross-training and automation software can contribute to process improvement. For example, if you can train employees to know how to do multiple jobs, then if someone is absent because of sickness or vacation, a process remains unharmed. Another idea is to implement an automation tool within your organization to reduce dependency on key personnel. For example, automation tools like SolveXia’s system are designed such that processes are stored within the system and can be run by virtually anyone with access. Not only is the process stored and will automatically run, but as the process runs, the system documents the steps it is taking to produce its output.

4. Time Audits:

One of the most significant resources wasted within a business is time. Being able to accurately measure and gauge how much time a process takes on behalf of your employees can offer insight into where you can optimize a process. It’s as simple as using software to time a process. Then, you can analyze how long processes take and find ways to eliminate wasted time. This could be in the form of automating approvals and reducing touch-points, thereby preventing potential bottlenecks and delays from occurring.

5. Catchball:

Within organizations, processes are rarely started and completed by a single person. As such, every process needs to have someone who can be held responsible for its execution, but still requires the input and assistance of multiple people. Catchball is a method of continuous improvement that requires the person who initiated a process to state its purpose and concerns to the others involved clearly. In this way, they can then “throw” it out to the group for feedback and ideas for improvement, yet the single person remains responsible for its completion.

The above are just some ideas to get continuous improvement going within your organization.

Here’s a look at some areas that breed waste within the business that often have room for improvement:

- **Timeliness:** System downtimes, approvals and bottlenecks of information
- **Errors:** Manual data entry errors, invoice errors
- **People:** Underutilized workforce, excessive management and micromanagement
- **Production:** Overproduction of printed documents before necessary

All of the above are just baseline examples of what many businesses face. In every case, an automation tool like SolveXia can assist in eliminating waste and helping with continuous improvement. The automation tool is designed to be accessible to all relevant parties, and by automating data and processes, errors are inherently reduced.

6. Improving Environments:

While you may be focused on operations and productivity levels, it’s easy to overlook the environment in which your team works. However, if you’re able to implement changes to better the environment, it can improve productivity, too. For example, you can touch up interior design, add green landscaping, and adjust lighting.

7. Information Technology:

Another example of continuous improvement is adding new software and technological tools that can aid workflows. For example, if you were to implement SolveXia in your workplace, you could witness 98% gains in productivity with automation solutions.

8. Staff Training:

No matter how experienced your staff is, one of the most valuable continuous improvement activities is to grant a refresh on staff training. Things change, so it's a great way to keep everyone up-to-date with skills and knowledge.

9. Edit Work:

Of the many process improvement examples out there, you likely take part of want to implement editing your team's work. From editing to QAing, this straightforward addition to your daily activities is bound to make a world of positive difference.

10. Stand-Ups:

Stand-ups are a wonderful way to ensure everyone is involved and heard. They are open forums for discussion for everyone in your organization to air their pain points, discuss their projects, and ask for needed support.

11. Optimizing a Process:

Businesses are filled with processes, and there is usually a way to reduce waste and enhance efficiency within a process. For example, if you're surveying customers for product development but find that their answers are vague, you may update your surveying process to checkbox answers rather than open-ended responses.

4- How to Create an Environment of Continuous Improvement?

With the examples in mind, you're on you way to implementing continuous improvement. But, before you get going, be sure to set your workplace environment up for success. In order to do so, it's recommended to:

1. Involve Everyone

Every person that is part of your organization is of great value to how your operations run. As such, they should all be included in the continuous improvement process. It's a combined effort and only works well as one that is inclusive.

2. Positively Encourage

Fear-mongering isn't the way to go when you're trying to drive positive change. Instead, encouragement goes a long way. Offer support to anyone who needs it and be sure to praise changes, no matter how big or small.

3. Openly Communicate

When you’re including everyone, a major key is to clearly communicate. This aids in developing a transparent culture in which all people are on board for the ride.

5- Incremental vs Breakthrough Continuous Improvement

Continuous improvement can be made as you go or a full-fledged approach to tackle significant issues at once:

Incremental Continuous Improvement:

This type of process improvement is done as you recognize problems during a process. The upside of this type of improvement is that it is relatively cheaper and faster than breakthrough continuous improvement. Say you are running a process and notice a mistake. This could be a typo in a brochure or an error in data. You can fix the error as you go; however, to ensure that the actual process moves forward in its next iteration without the same error requires that you communicate the change. So, incremental continuous improvement is beneficial so long as the person who fixes the mistake brings it up to the rest of the organization.

Breakthrough Continuous Improvement:

Breakthrough continuous improvement happens the other way around. Rather than making a change during the process itself, it involves targeting the process for improvement and then strategically approaching the change as a united front. These are typically more substantial items for correction that require an entire team to implement.

6- Benefits of Continuous Improvement

Continuous improvement offers a wide range of advantages that positively impact various aspects of an organization. Here are the key benefits:

1. Streamline workflow:

Most processes require multiple touchpoints or parties involved. These always have room for improvement. Whether it's from the basis of the data needed or the communication between the people who play a role in its completion.

2. Reduce costs/waste:

Project managers and executives have models and data to review the cost of every project. With continuous process improvement, they can assess where the fees are too high and then work towards reducing costs and waste to make a process more efficient.

3. Risk Proofing:

Continuous improvement helps to spot issues before they grow larger. Spotting opportunities for improvement early on can help to reduce risks in the future.

4. Improved Morale:

By practicing process improvement, employees are engaged and empowered to make a positive difference in the company. This makes them feel more valued, happy, and motivated overall.

5. Quality:

The ultimate goal of any business is to deliver value to customers. By improving processes, you are also improving the outcome of said processes. As a result, there's a strong likelihood that you'll enhance the quality of goods or services, which tends to drive customer loyalty.

7- How to Identify Areas for Continuous Improvement?

When approaching continuous improvement, a comment question is where to begin and how to know what is ripe for improvement. There are a few ways to identify areas, including:

1. Feedback

Leverage the feedback of your employees through surveys, chats, meetings, or suggestion boxes. By doing so, you get those who are on the ground and in the weeds to share their experiences and shine a spotlight on processes that could use attention.

2. Process Mapping

Another useful way to identify processes that need some love is to visually map out workflows using process mapping. By seeing the steps and pieces that make a process flow, it's easier to notice where delays or redundant steps may be occurring.

3. Analytics

Leveraging automation software with access to analytics means that you have KPIs and metrics displayed in a visual dashboard to track trends and patterns. If you notice outliers, it may be a sign that it's time to review those processes.

8- When to Look for a Continuous Process Improvement Tool?

It's safe to say that it's always a good time to search for continuous process improvement tools. However, there are tell tale signs that elicit the true need for process improvement, such as:

1. Quality Challenges

If you notice that there are constant customer complaints about a specific product's quality or service, it's likely that it's in need of adjustments.

2. Bottlenecks

Noticing that workflows get stuck somewhere in the middle? Inefficiencies and delays are undesirable outcomes, so if they are creeping in your business, it's time to take notice.

3. Growth

Perhaps things are going very well, and you're not experiencing either of the above. Instead, you're scaling and growing your business because of positive outcomes.

Well, this is another good time to consider using a continuous process improvement tool because as you expand, you want to ensure the quality is unaffected and that your business can keep up with increased demand.

9- What are Continuous Improvement Process Methodologies?

There are plenty of process improvement methodologies to apply in your business. Here is a look at some of the most popular practices to use for your own continuous improvement examples:

1. PDCA

PDCA is an acronym for: Plan, Do, Check, Act. Also known as the Deming Cycle, PDCA attempts to collect knowledge about a process in order to make it better.

- **Plan**: Create a hypothesis for why the problem exists and potential solutions.
- **Do**: Implement the solutions.
- **Check**: Examine how your new solution has impacted the outcome.
- **Act**: If the results are better, then scale the solution. If there's still room for improvement, then return back to step one to try again.

2. 5 Why's

This one may remind you of that stage when a toddler can only ask, "Why?" but there's an actual reason to do so. The 5 Why's is an attempt at root cause analysis, or to uncover the reason why a process may be inefficient.

It's as simple as it sounds – you ask "Why?" five times to keep diving deeper into the heart of a problem. By leveraging perspective, you can uncover a lot.

3. Kanban Boards

For visual learners, Kanban Boards offer a way to see how processes flow visually. By doing so, it may be easier to pinpoint inefficiencies and make edits to the troublesome aspect of a process.

10- What are Continuous Improvement Metrics?

How do you know that your continuous process improvement efforts aren't being done in vain? Through the use of metrics, of course!

When it comes to continuous process improvement, the following metrics are worth keeping track of:

1. Cost

Cost is an indicator of your business' overall health and strategy. You can see how much you're spending on labor, inventory, materials, and your team's time. Hopefully, when you properly improve upon a process, you can cut costs as a result.

2. Customer Satisfaction

Another way to gauge the outcome of your actions is to measure customer satisfaction before and after the changes have been made. Consistent customer surveys and requests for feedback/reviews can show you how your business is performing.

3. Safety

Another prime concern for any business is the safety of its people. Tracking safety, such as the number of incidents in a certain time period, can provide insight into operations. The more a company prioritizes safety, the more employees feel that they can trust their employer, as well.

11- How to Implement Continuous Process Improvement?

As mentioned above, continuous process improvement doesn't always have a clear beginning and end. Instead, it works best when it is part of the company culture and involves everyone within an organization.

Here are some considerations for how to make continuous process improvement the norm within your business:

1. Have a Vision

Start by defining objectives and goals clearly. By communicating these goals within your organization, you can ensure that everyone is aligned and on the same page to promote better end results.

2. Define Measurable Goals

SMART goals are always recommended so that you can assess outcomes. SMART stands for: specific, measurable, achievable, relevant, and time-bound.

3. Leverage Data

Say goodbye to guesswork by utilizing data and analytics for quantifiable information. By analyzing data, you can also spot trends and patterns that can signal where your next process improvement efforts must reside.

4. Train Employees

Change isn't always easy. It's vital to train and support employees as you make any adjustments to existing processes. This is especially true when you implement new technologies and want your employees to make use of such tools. They should feel comfortable using new technologies as part of their processes and routines.

5. Manageable improvements

Set reasonable goals. When setting out for improvement, you want to break down larger projects into smaller, measurable pieces. This will help to reduce overwhelm, as well as keep everyone involved on the right track to succeed.

6. Elicit Feedback

You should continuously seek feedback from customers, stakeholders and employees throughout your operations. This feedback will not only help locate opportunities for improvement, but it can also offer new perspectives and breed new ideas.

7. Motivate employees

Not only should you breed a culture where each employee feels empowered to notice inefficiencies and offer solutions, but you should also develop a rewarding culture to be motivational. For example, you can create rewards or develop an accessible system for employees to share feedback continuously.

12- How to Address Continuous Improvement Challenges with No-Code Tools?

As mentioned above, there may be resistance to using no-code tools or new technologies within your business, especially when it comes to its application for continuous improvement examples.

To overcome these challenges, it can be beneficial to:

1. Communicate Openly

The most important thing you can do when introducing anything new into your business is to communicate with your employees as to the reason why. By clearly communicating the need for process improvement and process improvement tools, you can help to reduce fear and actually spark interest/ support.

2. Proof-of-Concept (POCs)

Rather than starting with widespread alterations, you can begin with a proof-of-concept project. For example, if there are multiple processes you wish to amend, start with one.

Then, you can use it as an example as to how the no-code tool has not only improved the organization, but also the lives of employees, too. When employees experience the benefits first-hand, they will be more willing to take part in widespread changes.

3. Training

We've touched on it briefly already, but adequate training and support is another critical way to overcome challenges associated with implementing new technologies. When people feel comfortable using a technology, then they are naturally more likely to use it!

No code tools, like SolveXia, can be used to automate many of your primary finance functions. Once set up, SolveXia requires no extra support from IT teams and is easy to use with drag-and-drop functionality.

Companies can leverage SolveXia to automate processes, including: expense management, reconciliation, rebate management, commissions calculations, regulatory reporting, and more.

13- How to Build a Continuous Improvement Culture with No-Code Tools?

Continuous improvement is an ongoing effort, hence the word "continuous." And, when you're using no code tools to assist, it's critical to foster a culture that is in support.

Here's how you can better support your team to support continuous improvement:

- **Recognition**: Openly recognize those who are helping to support continuous process improvement efforts.
- **Gamification:** Create leaderboards and make it like a game to reward those individuals and teams that contribute the most.
- **Collaboration**: Enable employees to share best practices and recommendations with one another.

14- The Bottom Line

Continuous process improvement offers a method for your business to get better at any point in time. Whether you choose to implement incremental or breakthrough changes or a mixture of both, you can help to reduce waste and optimize outcomes. The above continuous improvement examples and strategies can help you achieve your business goals.

Like any type of process improvement, you want to remember to track and monitor any changes to ensure you are following towards improvement, rather than hurting any other part of the process. Automation software like SolveXia can help to analyze current processes, as well as implement solutions that optimize operations.