Deloitte 360°Cyber Programme

Connect, support & lead by example

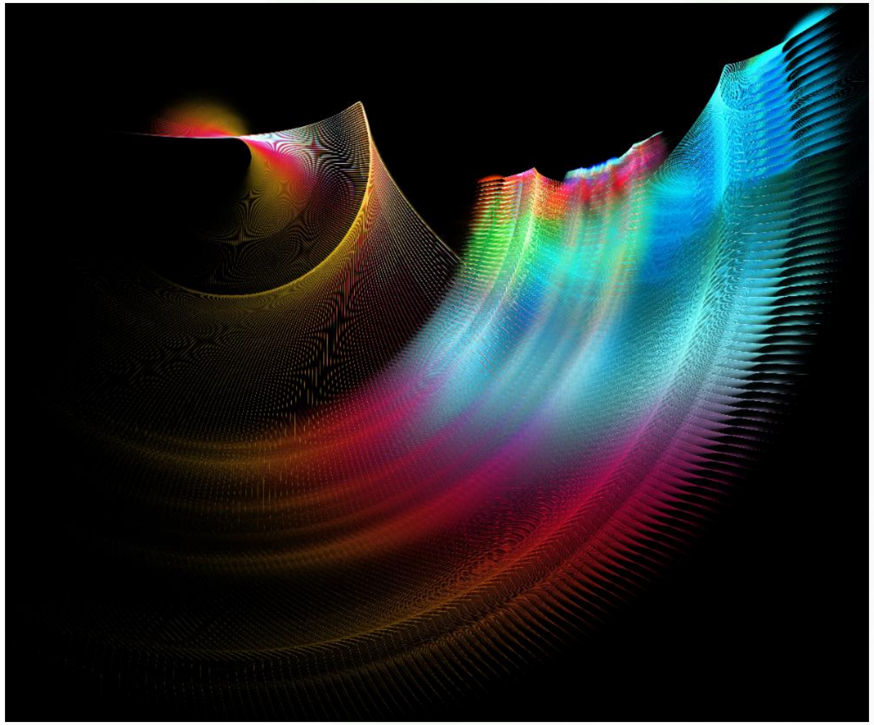
2023

Empowering your cyber-powered future

Deloitte 360°Cyber Programme Overview

Deloitte 360°Cyber Programme Overview

The role of the Chief Information Security Officer (CISO) is more critical and demanding than ever, and effective leaders are in high demand.



The Deloitte 360°Cyber Programme focuses on developing Cyber Security and Cyber Risk professionals as Cyber Security leaders.

The exclusive Programme places emphasis on the broad set of skills required to make an impact that matters and to lead by example rather than just build technical knowledge.

The Programme provides a confidential, safe space with opportunities for teams to benefit from tailored activities, which are often overlooked.

This is an opportunity for Cyber Security and Cyber Risk leaders to focus on their specific roles within an organisation, whilst building a Cyber network.

By participating in this Programme Cyber Security and Cyber Risk leaders have access to several initiatives which can support and equip leaders and their teams.

Throughout the calendar year, participating organisations will have access to a diverse range of thematic and industry-focused events, that bring expertise, discussion and insights.

The events will be centered around the five building blocks of the Deloitte 360°Cyber Programme: *build, influence, growth, balance and lead.*

This Programme provides a unique opportunity for organisations to establish new connections and relationships with Deloitte Subject Matter Experts (SMEs), whilst Cyber Security leaders focus on their development and building a Cyber network with Cyber Security leaders in similar and varied industries across a variety of experience levels and countries.

We want to hear from you

A major part of the community is co-creation, collaboration and feedback on all Programme activities. This is a chance to feed into upcoming insight papers and topics, and speaker opportunities on webinars and at events. This is *your Programme*, and we want you to shape it.

Programme Components Overview

The CISO Value Cycle

The Deloitte 360°Cyber Programme complements the CISO lifecycle with tools, experiences, networks and learning opportunities to deal with the everyday pressures posed by the role.

The Programme consists of five key actions that are enablers for success.

Lead

Your role as the CISO relies on leadership and guidance in Cyber Security – a topic of high importance to both business and stakeholders. This level of leadership goes beyond simply managing others. You need to set the example.

Do you feel like you possess those qualities within yourself? Through the Deloitte 360°Cyber Programme you have an opportunity to focus on your personal development and the attributes of a Cyber Security leader.

Build

As a CISO, you are expected to face the pressure of cyber attacks and an ever evolving threat landscape, whilst still maintaining day-to-day technical credibility.

Through various activities, this component builds on your technical skills including running successful programmes and keeping a close eye on changing regulatory requirements and cyber risks.

Influence

An integral part of your day-to-day life involves making an impact on your Board and Executive leadership to gain their trust in the selected security function.

The uncertainty of cyber risk often leads to uncertainty in trust. With expert knowledge at the forefront, influence is often the decider. Can you successfully influence decision making? Communication, demonstrating positive behaviours and setting high standards for performance are all key.

Growth

Growth is about developing your skills and capabilities alongside the evolving requirements of the CISO role. Some of this is tactical; from running large projects to sharpening your edge on non-technical skills. But there are also strategic components; with succession planning, prioritisation, decision-making, and career choices made with a view to your legacy.

Our Deloitte 360°Cyber Programme challenges your perspective on growth within the world of Cyber.

Balance

Stress and strain within the world of a CISO is common and balancing the shifting demands of Cyber Security can be challenging. You need a high level of resilience to manage the pressures of expectation, stress, and risk that come with execution decisions.

Within the Programme you will focus on personal learning as well as work life balance, especially in the more remote world.

Deloitte.

Deloitte 360°Cyber Programme

Connect, support & lead by example

March 2023

Empowering your cyber-powered future

Deloitte 360°Cyber Service Components

Component 1: Events and Workshop Sessions

Tailored events and workshop sessions to assist CISOs with expert Cyber Security advice and guidance

Events and Workshop Sessions

Facilitated labs and workshop sessions with key role players within an organisation, which are specifically tailored for new, existing or future Cyber Security and Cyber Risk leaders:

- Strategic thinking workshops
- Future focused labs
- Problem solving greenhouses (half a day or full day sessions)
- Transition labs

The transition labs are most suitable for Cyber Security and Cyber Risk leaders who require assistance with transitioning into a new role, for example a new Chief Information Security Officer (CISO).

These facilitated labs and workshop sessions are specifically tailored for CISOs, however, various other Cyber Security and Cyber Risk leaders will also benefit:

- Chief Executive Officers (CEOs)
- Chief Information Officers (CIOs)
- Chief Technology Officers (CTOs)
- Chief Security Officers (CSOs)
- Chief Financial Officers (CFOs)
- Chief Risk Officers (CROs)
- Chief Operating Officers (COOs)

A Transition Lab Overview

A transition lab is an immersive one-day workshop session that allows a newly appointed or incumbent CISO to step away from their day-to-day deliverables to take a fresh look at the following:

- Their function
- The CISO office’s strategy, team structure and goals
- To define their professional aspirations
- To consider where their time is spent and where their time needs to be spent
- To assess the CISO’s team and talent needs
- To examine key relationships and influence
- To outline a personal 180-day plan
- To develop a talent strategy for the team

The one-day workshop session is focused on the Information Security role of one of the following executive roles:

- Chief Information Security Officer (CISO)
- Chief Executive Officers (CEOs)
- Chief Information Security Officers (CIOs)
- Chief Technology Officers (CTOs)
- Chief Security Officers (CSOs)
- Chief Financial Officers (CFOs)
- Chief Risk Officers (CROs)
- Chief Operating Officers (COOs)

"EVERY SUCCESS STORY IS A TALE OF CONSTANT ADAPTION, REVISION AND CHANGE"
Transition

Component 2: Next Generation CISO Programme

Prepare aspiring CISOs on their journey to success

Next Generation CISO Programme

The Next Generation CISO Programme develops aspiring CISOs into Cyber Security leaders and provides delegates with access to insights from Deloitte professionals globally, including CISO leaders from various industries.

Existing CISOs selects one of their high-performing team members who is a potential successor to attend the Deloitte 360°Cyber Programme. The benefits of the Programme include:

- Aspiring CISOs are set up for success
- An opportunity for professional development with aspiring CISOs from the same and different industries
- The Programme is designed to prepare aspiring forward-looking CISOs for their journey to succeed
- The ability to build cross-functional relationships to support innovation and transformation
- The ability to be a strategic thinker and agent of positive change to the benefit of an organisation

Future support offered by Deloitte: As the Deloitte 360°Cyber Programme develops, there will be opportunities for teams to benefit through leadership labs and coaching.

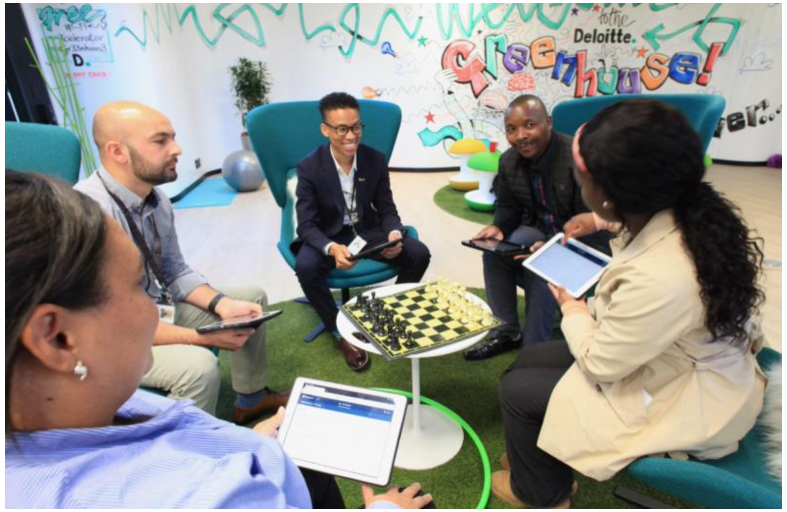
Next Generation Programme Overview

The development of an aspiring CISO as a Cyber Security leader, with an emphasis on the broad set of security skills required to make an impact that matters and to lead by example.

The Next Generation Programme includes:

- Tailored activities for CISOs and or their teams
- An opportunity for aspiring CISOs to be mentored by a Deloitte Cyber Security Subject Matter Expert (SME)
- An opportunity for aspiring CISOs to sign up to be a mentor within an industry
- An opportunity for an aspiring CISO to broaden their Cyber Security network through:
  - The annual Deloitte CISO Forum (DCF)
  - Deloitte 360°Cyber Programme Greenhouse events
  - Access to an international peer-to-peer network
  - Access to Deloitte Cyber Security expertise globally

The Next Generation Programme is focused on ***aspiring CISOs***, nominated by existing CISOs.



Component 3: Onsite CISO/Virtual CISO

Operational enablement of ISMS leadership governance, strategy, thought leadership and regulatory compliance

The Role of a CISO

The role of a CISO is a multidimensional, immersive one that faces accountability from several pillars within an organisation. A CISO is required to not only possess technical expertise, but also have a strategic outlook to drive security-oriented business direction.

A CISO must adapt to the Cyber Security culture of an organisation, and have the experience to guide an organisation through a breach with resilience. Typically a CISO is accountable for and expected to drive:

- Security-business enablement
- Security budget
- Identity governance and management
- Governance risk and compliance
- Threat prevention
- Threat detection
- Compliance and audits
- Security architecture
- Cyber Security Board/Executive reporting

Deloitte Cyber offers clients Cyber Security SMEs to assist organisations with the delivery of a CISO's responsibilities through an onsite CISO or virtual CISO service offering.

Onsite CISO

The Deloitte 360°Cyber Programme onsite CISO service component is suitable for organisations seeking an onsite global CISO, new CISO, or assistance for an existing CISO, through the use of a dedicated secondment or adhoc use of a senior-level Cyber Security Subject Matter Expert (SME).

Modes of engagement:

- Full Time – Dedicated, focussed CISO
- Part Time – Transitional CISO
- Once Off – Board/Executive guidance, advice, security simulations, Information Security training and awareness

The benefits of an onsite CISO include:

- Access to Deloitte Cyber Security SMEs globally
- An operationally focussed CISO office
- Transparent Cyber Security Board/Executive reporting
- Security dashboards
- Knowledge sharing and continuous upskilling of organisation's existing CISO office team members

Virtual CISO

The Deloitte 360°Cyber Programme virtual CISO service component is suitable for organisations seeking a virtual/remote CISO and or Cyber Security consultants. Deloitte virtual CISOs and or Cyber Security consultants, provide strategic deliverables and solutions virtually both nationally and internationally. Proactive Board members or CEOs of organisations assign a virtual CISO with the task of:

- Understanding an organisation's Cyber Security threat and risk landscape
- Establishing the Cyber Security risk posture of an organisation
- Creating a security structure and assist with the deployment of a known baseline framework

Modes of engagement:

- Virtual – Virtual dedicated – Strategic Cyber Security deliverables

The benefits of a virtual CISO include:

- Access to global Deloitte specialists and expertise
- A robust methodology for effectively running a security programme
- Not being limited by employee considerations such as skill sourcing, training or benefit packages
- The ability to seamlessly scale security efforts up or down based on required needs

Component 4: Environmental, Social and Governance Initiatives

Security initiatives for Environmental, Social and Governance (ESG) included in the Deloitte 360°Cyber Programme

Environmental, Social and Governance

Cyber Security is one of the governance concerns within ESG considerations due to an increase in the frequency and severity of Cyber Security threats and attacks.

The Deloitte 360°Cyber Programme incorporates the following ESG initiatives to assist our clients to benefit of the broader community with improving their ESG contribution from a security perspective. As an outcome of these improvements, our client's mature the skillset and overall governance of their respective organisations:

- Cyber Security training, awareness and collaboration in universities
- Green IT
- Women in Cyber
- Women in Artificial Intelligence (AI)
- Women in Data
- The Deloitte South Africa Cyber Graduate Programme
- Technology Resilience
- Data Privacy Governance

The ESG service component is a unique opportunity for organisations to have access to Cyber Security initiatives which can equip and support diverse Cyber Security leaders.

ESG Initiatives Overview

Through the Deloitte 360°Cyber Programme, the team wants to provoke curiosity and reveal the opportunities that exist within the Cyber workplace.

The Deloitte South Africa Cyber Graduate Programme onboards new graduates annually to become part of the Deloitte South Africa Cyber team. Graduates are given the opportunity to develop and improve their Cyber Security skills, whilst being part in the delivery of exceptional value to clients.

The Women in Cyber, AI and Data Programmes focus on the underrepresentation of women in the Cyber workforce. Deloitte Cyber is committed to addressing the gender imbalance and promotes gender diversity in the Cyber Security industry to close this gap.

Component 5: Threat Intelligence

Threat landscape insight for your organisation and industry

Threat Intelligence

Better visibility and threat response readiness at a CEO and Board level requires CISOs to become more strategic in their Board communications and interactions about the security threats in relation to the attack surface and risk landscape.

CISOs are also required to control regulatory requirements compliance in order to succeed in attaining a desirable security compliance posture. The Deloitte 360°Cyber Programme provides Cyber Security and Cyber Risk leaders with the following insights – amongst others:

- Africa specific threat intelligence
- Global threat intelligence
- Client specific threat intelligence
- Industry benchmarking
- A Digital Footprint Assessment (DFA) which is non-intrusive
- Dashboards for continuous monitoring
- Malware analysis and reporting
- Vulnerability Assessment monitoring
- External threat monitoring (brand abuse, confidential data leakage, threat monitoring and hacktivism)

The threat intelligence service component provides organisations with an overview of their evolving threat landscape, with a practical mitigation and prevention approach.

Threat Intelligence Key Sources

The Programme's threat intelligence key sources include the following:

- Dark web insights – Global and Africa
- Deloitte threat intelligence developer
- Manual evaluation
- Threat group insights
- A forward looking threat landscape view
- Threat reports
- Threat studies
- Industry threat reports

|

Component 6: The Annual Deloitte CISO Forum

The Annual Deloitte CISO Forum

Annual Deloitte CISO Forum (DCF)

The Deloitte CISO Forum is a by-invitation-only annual event which takes place during the Cyber Security awareness month (October).

By attending the Forum, Cyber Security and Cyber Risk professionals will have access to the following:

- An interactive 3 hour session with 1 – 2 Key note speakers and an accelerated Greenhouse breakaway
- Information Security newsletters/research papers
- Lessons learnt from Transition Labs which ran throughout the year
- Threat Intelligence reports per industry
- CISO member portal access
- A chance to become the Deloitte Africa CISO Programme CISO of the year
- A change to become the Deloitte Africa aspiring CISO of the year – Aspiring CISOs which are part of the Deloitte Next Generation CISO Programme
- 5% discount on events relating to the Programme
- 5% discount on engagements over R2 million

DCF Additional Add-On Services

Organisations have an opportunity to purchase one-on-one sessions with Deloitte industry Subject Matter Experts (SMEs).

In the event that the insight or advice provided to an organisation during a session did not shift their approach or thinking, there is no obligation for organisations to pay Deloitte for that particular session.

The Deloitte 360°Cyber Programme Professional Think Tank component provides Cyber Security and Cyber Risk leaders with access to ask questions in real time, answered by:

- A security management mentor/coach
- A security Subject Matter Expert (SME)

Component 7: CISO Governance-as-a-Service

Governance of best practice roles, responsibilities and practices to enable strategy execution

CISO Governance-as-a-Service

The role of the CISO is a multidimensional, immersive one with accountability for security pillars within an organisation. A CISO is required to not only possess technical expertise, but also have the strategic outlook to drive security-oriented business decisions.

CISOs have to understand and adapt to the Cyber Security culture of an organisation, and have the experience to guide organisations through a breach with resilience.

The CISO Governance-as-a-Service service component has been established to assist CISOs/Cyber Security leaders with their roles and responsibilities from a governance perspective – giving a CISO/Cyber Security leaders more time to focus on day-to-day operational deliverables.

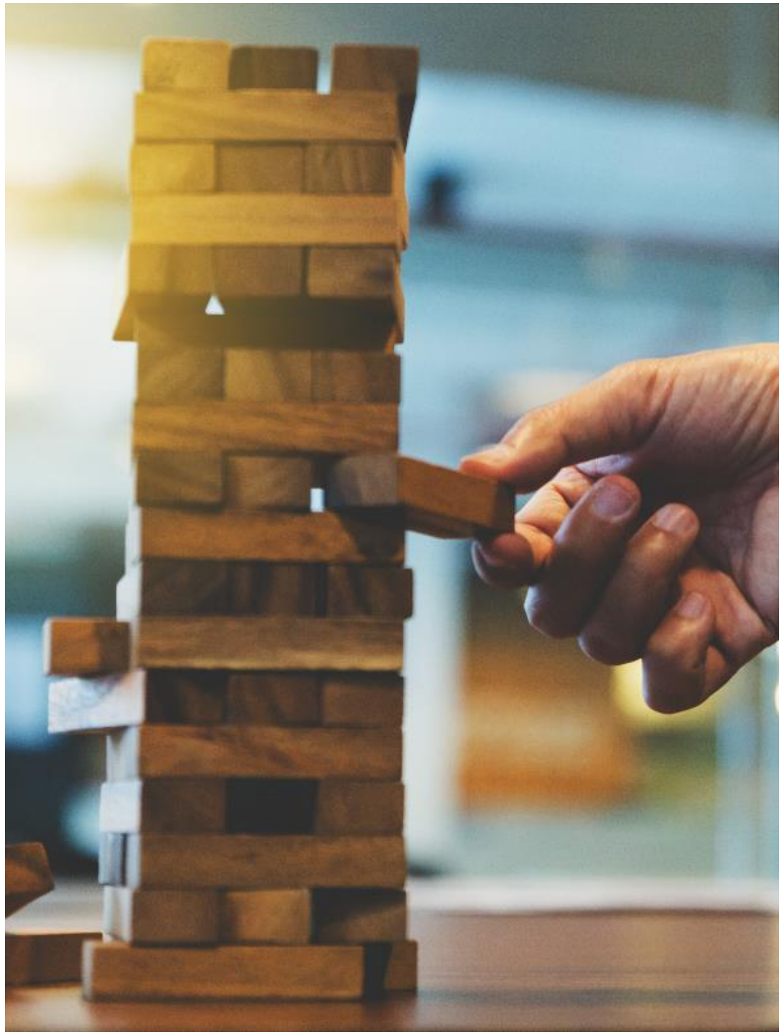
Modes of engagement:

- Full Time – Dedicated Cyber Security leader secondment
- Part Time – Over a one year period
- Part Time – Over a two year period
- Part Time – Over a three year period
- Once Off – CISO and or Cyber Security leader guidance and advice

Governance-as-a-Service Examples

- Assist with the development, review and or update of the following:

  - Cyber Security Strategy
  - Cyber Security Framework
  - Cyber Security Policies and Standards
  - Documenting processes and procedures
  - Cyber Security Office roles and responsibilities
  - Review and update of existing Cyber Security reporting templates and dashboards, etc.



Component 8: Board and EXCO Training & Awareness

Educate Board and Executives on their industry specific Information Security awareness responsibilities

Board and EXCO Training & Awareness

The primary objective of the Board and Executive Committee training and awareness component of the Deloitte 360°Cyber Programme is to educate members on their responsibility to help protect the confidentiality, availability and integrity of their organisation's information and Information Technology (IT) assets.

The programme provides organisation's with:

- An established, practical Information Security training and awareness programme for an organisation's specific needs and requirements
- Information Security crisis simulations
- Information Security awareness training and awareness content with helpful tips and actionable tasks
- Board and Executive members with an increased awareness of Information Security threats and a better understanding of their Information Security responsibilities

Modes of engagement:

- Full Time – An annual content subscription
- Part Time – A quarterly content subscription
- Part Time – A monthly content subscription
- Once Off – A once off content subscription

EXCO Training & Awareness Overview

An organisation's Information Security training and awareness programme should continuously evolve in response to the evolving nature of Cyber Security attacks, the increased targeting of confidential information and the potential costs associated with Cyber Security breaches.

The Deloitte 360°Cyber Programme Board and Executive Committee Information Security training and awareness component, provides clients with a practical programme based on industry specific Cyber Security threats and incidents.

This component offers clients with a unique opportunity to:

- Develop an Information Security awareness strategy and programme that is fit for purpose
- Participate in face-to-face training and awareness workshop sessions with Deloitte Subject Matter Experts (SMEs)
- Implement an Information Security Learning and Development platform with automated dashboard reporting and automated Information Security awareness campaigns
- Participate in industry focussed crisis simulation exercises

Component 9: Third Party Cyber Risk Management-as-a-Service

Third Party Cyber Risk Management-as-a-Service (TPCRMaaS)

TPCRMaaS

As third-party ecosystems continue to expand, important questions are being asked by Boards of Directors and other key stakeholders regarding the risk to the extended enterprise, such as:

- Is there a process for continually assessing and monitoring risks related to third parties?
- Do we understand our most critical assets, their locations and the third party implications?
- Is there a mechanism to monitor who has access to the identified critical data?
- Do our contractual arrangements sufficiently protect us and do they adequately address Cyber Security?

The Deloitte 360°Cyber Programme TPCRMaaS component assists clients with:

- Cyber Security Third Party Risk Assessments
- Third party ecosystems automated risk monitoring and threat intelligence
- Assistance with the set up of a Third Party Cyber Risk Management operations centre for the management and oversight of third party Cyber risk.
- Third Party Cyber Risk Management managed services (e.g. maturity assessments, gap assessments etc.)

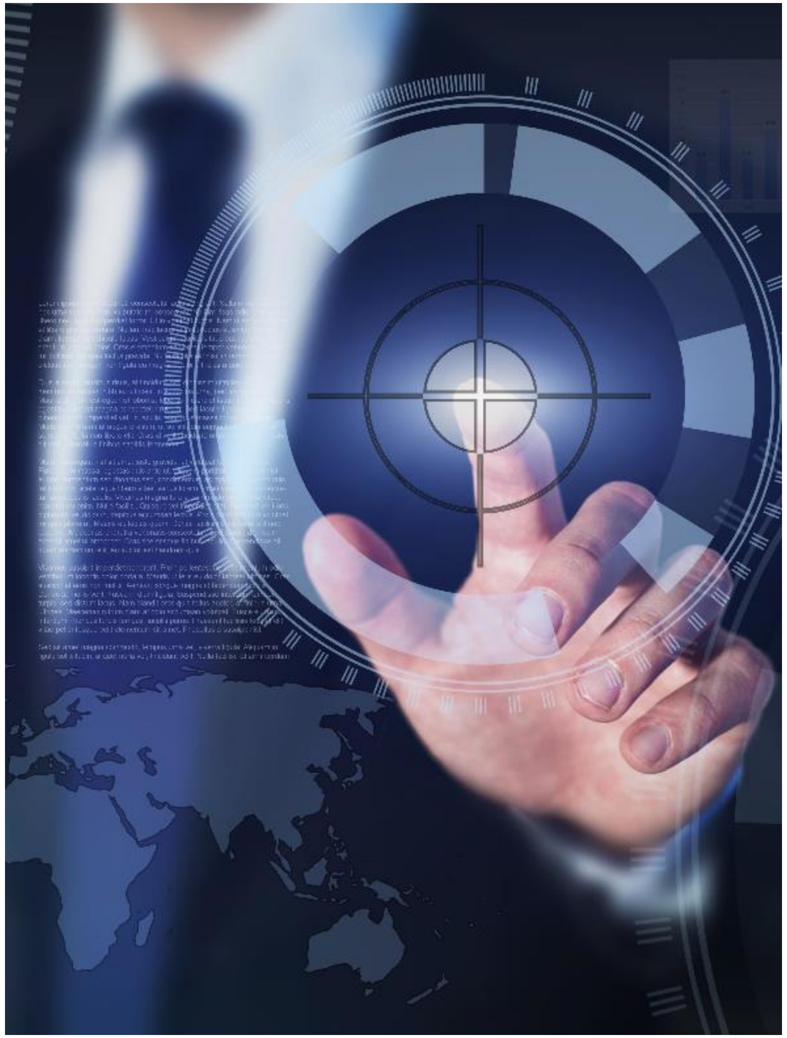
TPCRMaaS Overview

Organisations that rely on third parties to fulfil their market and customer obligations need to have sight of and manage the Cyber Security related risks posed to them by these third parties.

As organisations and their associated third party ecosystems continue to expand it is recommended that the current capabilities be matured to ensure robust mechanisms are in place to detect, prevent and respond to Cyber and data privacy risks.

An effective Third Party Cyber Risk Management Programme requires an integrated approach with an understanding of current capabilities, integration across the supply chain processes and interdependencies across an organisation.

The Deloitte Third Party Cyber Risk Management Subject Matter Experts (SMEs) assist organisations with practical insights and guidance on how to mature their Third Party Cyber Risk Management maturity, to ensure efficiencies and the effective management of Cyber Security risks across all third party types.



Component 10: Deloitte Cyber Professional Think Tank

Sounding board for Cyber Security leaders with real time advice and guidance

Professional Think Tank

- Professional Think Tank – ask questions in real time:
  - A security management mentor/coach
  - A security Subject Matter Expert (SME)
- CISO/Cyber Security professional portal

Deloitte 360°Cyber

Meet our team

Samresh Ramjith

Samresh is the Cyber Risk leader for Deloitte Africa, his Cyber Security experience spans more than 20 years across the continent.

Nombulelo Kambule

Nombulelo is a Partner in Cyber Risk. With extensive experience in Cyber Security Third Party Risk Management and Supply Chain Risk across various industries.

Tiaan van Schalkwyk

Tiaan is a Senior Associate Director in Cyber Risk. With extensive experience in Information Security, Cyber Security and Privacy, he advises the security of Industrial Control Systems (ICS), Operational Technology (OT), Enterprise Security Architecture, IT Governance and BCM/DR.

Mary-Ann Labuschagne

Mary-Ann is a Senior Manager in Cyber Risk. With extensive experience in Information Technology and Cyber Security Risk and Governance, in the Financial Services and the Telecommunications industry.

Flip Erasmus

Flip is a Senior Manager in Cyber Risk. He helps clients in preventing cyber-attacks and protecting valuable assets.

Deloitte.

Thank you.

This publication contains general information only, and none of the member firms of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collective, the "Deloitte Network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte Consulting LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte USA LLP, Deloitte LLP and their respective subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.