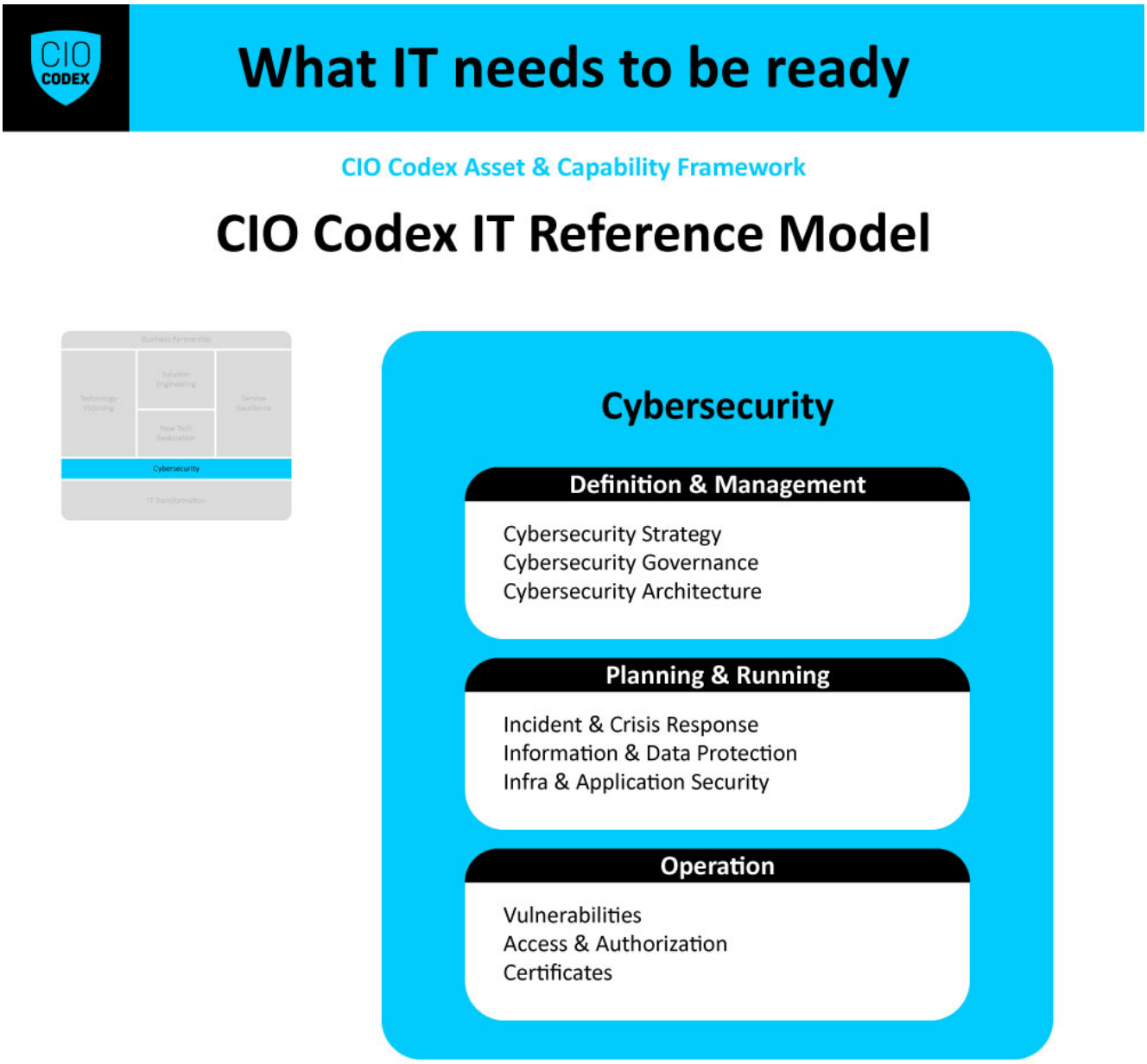

Dentro do CIO Codex Capability Framework, a camada Cybersecurity é imperativa para a proteção integral da organização.

Ela preconiza uma atuação da Tecnologia como parceira do CoE de Cybersecurity da organização.

Esta camada abrange a estratégia de segurança, a arquitetura e a operação eficaz, focando na proteção de dados, informações, aplicações e infraestruturas.

Há um monitoramento constante e uma gestão proativa dos elementos mais sensíveis de segurança, incluindo a identificação de vulnerabilidades e a gestão de acessos e autorizações.

Esta camada também estabelece e mantém rigorosos protocolos de resposta a incidentes de segurança cibernética, assegurando uma execução diligente e uma resposta abrangente.

A gestão de riscos, compliance, auditoria e segurança são tratadas com diligência e proatividade para manter a organização segura contra ameaças internas e externas, assegurando a resiliência operacional e a confiança dos stakeholders.

Essa camada apresenta como conteúdo complementar o detalhamento de cada uma de suas macro capabilities e capabilities conforme abaixo, cada qual explorada em um item específico do CIO Codex Framework IT Reference Model:

Definition & Management: Envolvendo a definição de uma estratégia de segurança cibernética abrangente, a governança de políticas e procedimentos, além da arquitetura de segurança para proteger contra ameaças digitais:

- **Cybersecurity Strategy**: Esta capability envolve o desenvolvimento e a implementação de uma estratégia de segurança cibernética abrangente. Foca em alinhar as iniciativas para negócio da organização, definindo prioridades, estabelecendo diretrizes de segurança e garantindo a alocação adequada de recursos para proteger contra ameaças cibernéticas.
- **Cybersecurity Governance**: Dedicada à governança da segurança cibernética. Esta capability assegura que as políticas, procedimentos e controles estejam conforme as regulamentações e padrões da indústria. Inclui o monitoramento do cumprimento das políticas de segurança e a avaliação contínua dos riscos para garantir uma postura eficaz e atualizada.
- **Cybersecurity Architecture**: Foca na criação e manutenção de uma arquitetura de segurança robusta. Esta capability envolve o design e a implementação de soluções que protejam as redes, sistemas e dados da organização. Inclui a integração de tecnologias, a definição de modelos de controle de acesso e a garantia de que a segurança é uma consideração central em todas as iniciativas de TI.

Planning & Running: Abrangendo a implementação prática da estratégia de segurança definida, envolvendo o planejamento, execução e gerenciamento contínuo de atividades de segurança para proteger a infraestrutura de TI, os dados e as

operações da organização contra ameaças cibernéticas:

- **Incident & Crisis Response**: Esta capability é vital para o gerenciamento e resposta a incidentes e crises de segurança cibernética. Envolve a identificação rápida de incidentes de segurança, a implementação de medidas para mitigar o impacto e a coordenação de esforços para resolver o incidente. Inclui também a comunicação eficaz com as partes interessadas durante e após o incidente, bem como a análise pós-incidente para prevenir futuras ocorrências.
- **Information & Data Protection**: Esta capability é essencial para garantir a segurança e privacidade dos dados críticos da organização. Ela envolve desenvolver e implementar estratégias abrangentes para proteger informações sensíveis contra acessos não autorizados, vazamentos e outras formas de comprometimento. Isso inclui a aplicação de controles rigorosos de acesso, criptografia, backup e medidas para a prevenção de perda de dados, garantindo a integridade e a confidencialidade das informações.
- **Infrastructure & Application Security**: Foca na proteção de infraestruturas de TI e aplicações. Esta capability envolve a implementação de medidas de segurança robustas para prevenir ataques cibernéticos e garantir a integridade dos sistemas. Inclui a aplicação de firewalls, sistemas de detecção e prevenção de intrusões, criptografia e práticas de segurança no desenvolvimento de aplicações. O objetivo é salvaguardar a infraestrutura tecnológica essencial e as aplicações críticas contra vulnerabilidades e ameaças externas e internas.

Operation: Abordando as atividades operacionais relacionadas à segurança cibernética, garantindo que as políticas e procedimentos estabelecidos sejam efetivamente aplicados e que os sistemas e dados da organização estejam protegidos contra ameaças contínuas:

- **Vulnerabilities Management**: Esta capability é fundamental para a identificação, avaliação e remediação de vulnerabilidades nos sistemas de TI. Envolve a constante varredura e análise dos sistemas para descobrir falhas de segurança, classificá-las com base no risco que representam e implementar as correções necessárias. É essencial para prevenir ataques

cibernéticos e garantir a integridade dos sistemas.

- **Access & Authorization Management**: Foca no controle rigoroso do acesso a sistemas e dados. Dependendo da organização, também atua sobre os recursos e instalações físicas. Esta capability inclui a gestão de identidades, autenticação e autorizações, assegurando que apenas usuários autorizados tenham acesso aos recursos adequados. É vital para prevenir o acesso não autorizado e proteger contra ameaças internas e externas.
- **Certificates Management**: Dedicada à gestão de certificados digitais. Esta capability assegura a autenticidade e a segurança das comunicações e transações eletrônicas. Inclui a emissão, renovação e revogação de certificados, bem como a monitorização da sua validade e conformidade. É crucial para garantir a confiança e a integridade nas interações digitais.