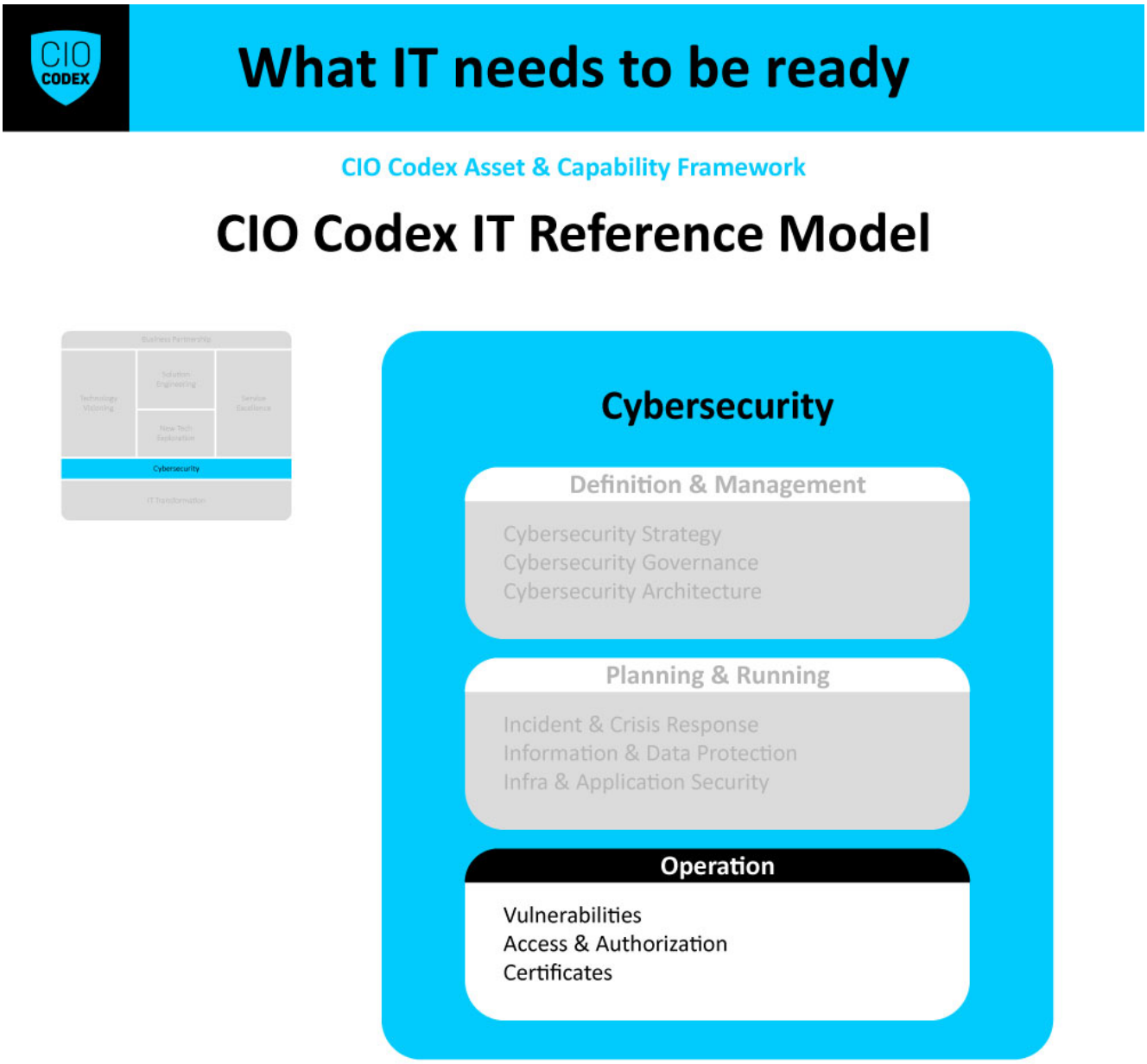

A macro capability Operation, localizada na camada Cybersecurity, é fundamental para a execução e manutenção diária das iniciativas de segurança cibernética em uma organização.

Esta macro capability aborda 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.

Um aspecto crucial da Operation é o monitoramento contínuo e a gestão de ameaças de segurança.

Isso envolve a vigilância constante dos sistemas de TI para detectar atividades suspeitas, identificar ameaças emergentes e responder rapidamente a incidentes de segurança.

Uma gestão eficaz de vulnerabilidades também faz parte dessa macro capability, incluindo a identificação, avaliação e correção de vulnerabilidades nos sistemas para prevenir ataques cibernéticos.

Além disso, a Operation inclui a gestão de acesso e autorizações, assegurando que apenas os usuários autorizados tenham acesso aos recursos críticos e que esse acesso seja monitorado e gerenciado de forma segura.

Isso é essencial para prevenir acessos não autorizados e proteger a integridade dos sistemas e dados.

A gestão de certificados digitais é outro componente importante, garantindo a autenticidade e segurança das comunicações e transações eletrônicas.

Isso é crucial para manter a confiança e a integridade nas interações digitais da organização.

Em resumo, a macro capability Operation é vital para assegurar a implementação efetiva das estratégias de segurança cibernética e para manter uma defesa contínua contra ameaças.

Ela representa uma combinação de vigilância, prevenção e resposta, essencial para proteger os ativos digitais da organização e garantir a continuidade das operações de negócios em um ambiente digital cada vez mais desafiador.

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

- **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.