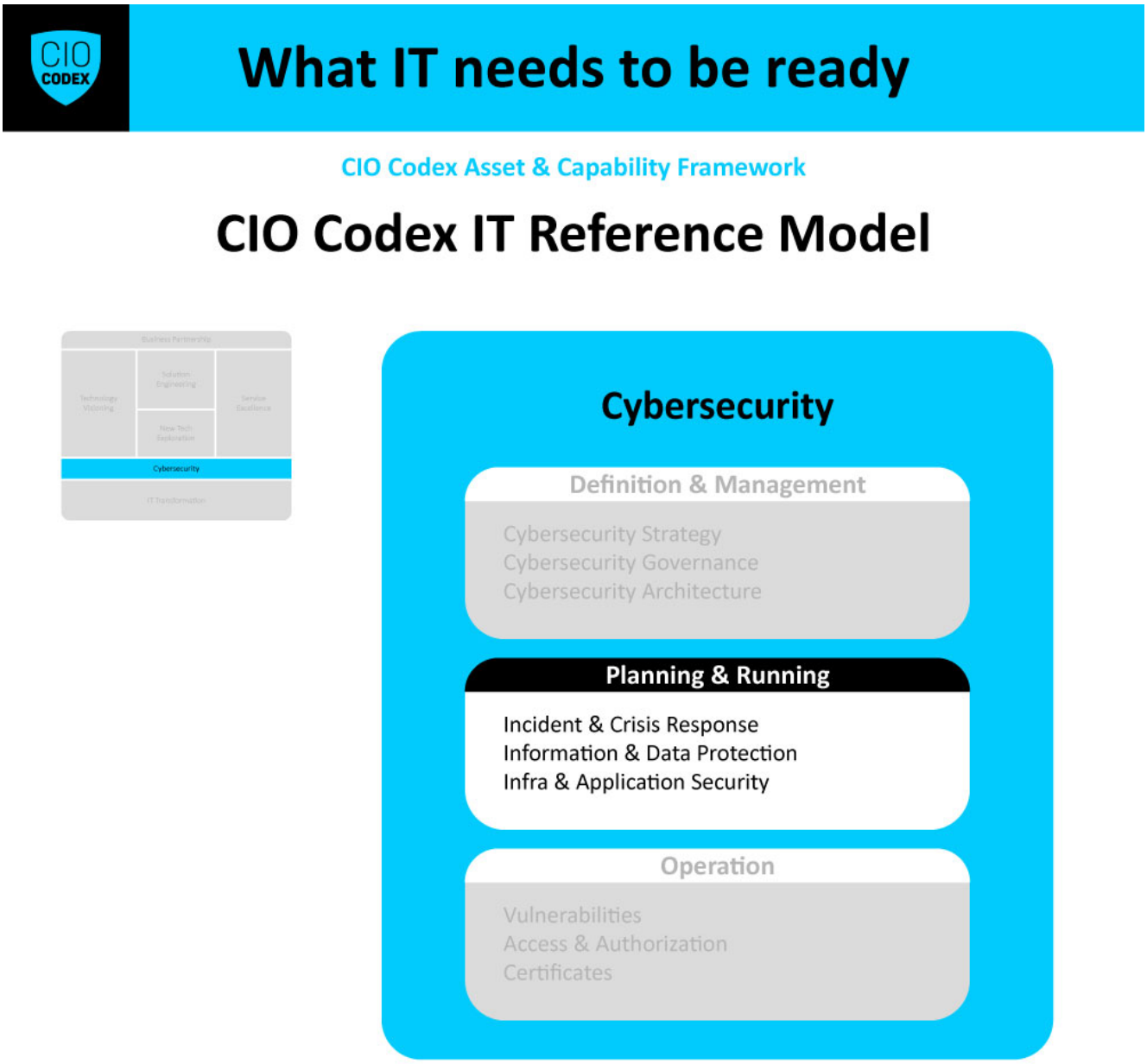

A macro capability Planning & Running, situada na camada Cybersecurity, desempenha um papel crucial na preparação e operacionalização das estratégias de segurança cibernética de uma organização.

Esta macro capability abrange 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.

O aspecto de planejamento envolve o desenvolvimento de planos detalhados de segurança cibernética, que incluem a identificação de recursos necessários, a definição de cronogramas e a preparação para cenários de ameaças potenciais.

Essa fase é crítica para estabelecer uma fundação sólida que permita uma resposta rápida e eficaz a incidentes de segurança.

A parte de execução da macro capability foca na implementação ativa das medidas de segurança.

Isso inclui a instalação e configuração de ferramentas de segurança, a realização de testes de penetração e avaliações de vulnerabilidade, e a implementação de controles de segurança em toda a organização.

Também abrange a formação e conscientização dos funcionários sobre práticas de segurança, um componente essencial para reforçar a linha de defesa contra ameaças cibernéticas.

Por fim, a operacionalização contínua das estratégias de segurança é um componente chave da Planning & Running, o que inclui aspectos de proteção de dados e informações.

Isso implica no monitoramento constante da eficácia das medidas de segurança, na adaptação às novas ameaças emergentes e na atualização contínua das práticas de segurança para garantir que a organização mantenha uma postura de segurança robusta e resiliente.

Em resumo, a macro capability Planning & Running é vital para garantir que as estratégias de segurança cibernética de uma organização sejam não apenas teoricamente sólidas, mas também efetivamente implementadas e mantidas ao longo do tempo.

Ela desempenha um papel fundamental na proteção contínua dos ativos digitais da organização e na prevenção de interrupções operacionais causadas por incidentes de segurança.

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:

- **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.