OCR Guidance on Risk Analysis Requirements under the HIPAA Security Rule

Risk analysis requirement in § 164.308(a)(1)(ii)(A).
Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule.

The guidance is not intended to provide a one-size-fits-all blueprint for compliance with the risk analysis requirement. Rather, it clarifies the expectations of the Department for organizations working to meet these requirements.

http://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

U.S. Department of Health and Human Services (HHS) The Office of the National Coordinator for Health Information Technology (ONC) - Security Risk Assessment (SRA) Tool

The purpose of the SRA Tool is to assist healthcare practices in performing and documenting a Security Risk Assessment. The HIPAA Security Rule, effective since 2005, requires that all healthcare organizations that are covered entities or business associates under the HIPAA Privacy and Security Rules conduct a thorough and accurate Risk Assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the entity (164.308(a)(1)(ii)(A)).

This SRA Tool is designed for small to medium sized practices. … ONC has historically defined small to medium sized practices to be those with one to ten healthcare providers.

https://www.healthit.gov/providers-professionals/security-risk-assessment

National Institute of Standards and Technology - HIPAA Security Rule Toolkit

The purpose of the NIST HSR Toolkit project is to help organizations better understand the requirements of the HIPAA Security Rule, implement those requirements, and assess those implementations in their operational environments.

The HSR Toolkit is intended to be used by any organization, including covered entities and business associates that wish to augment their understanding and implementation of the HIPAA Security Rule. This spans the entire spectrum of healthcare entities from very large organizations with vast IT resources to very small businesses and provider practices that may have limited access to IT expertise.
https://scap.nist.gov/hipaa/

NIST Special Publication 800-53A - Guide for Assessing the Security Controls in Federal Information Systems and Organizations

Security control assessments are not about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits—rather, security controls assessments are the principal vehicle used to verify that the implementers and operators of information systems are meeting their stated security goals and objectives. Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, is written to facilitate security control assessments conducted within an effective risk management framework.

Special Publication 800-53A is a companion guideline to Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.

http://www.nist.gov/itl/csd/risk-092011.cfm

NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.

Security controls are the safeguards/countermeasures prescribed for information systems or organizations that are designed to: (i) protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems/organizations; and (ii) satisfy a set of defined security requirements.[4] There are several key questions that should be answered by organizations when addressing the information security considerations for information systems:

• What security controls are needed to satisfy the security requirements and to adequately mitigate risk incurred by using information and information systems in the execution of organizational missions and business functions?

• Have the security controls been implemented, or is there an implementation plan in place?

• What is the desired or required level of assurance that the selected security controls, as implemented, are effective in their application? [5]

The answers to these questions are not given in isolation but rather in the context of an effective *risk management process* for the organization that identifies, mitigates as deemed necessary, and monitors on an ongoing basis, risks[6] arising from its information and information systems. NIST

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
https://web.nvd.nist.gov/view/800-53/Rev4/home

US Department of Homeland Security Cyber Security Evaluation Tool

The Cyber Security Evaluation Tool (CSET®) is a software tool for performing cybersecurity reviews of an organization's enterprise and industrial control systems. It was designed to help asset owners identify vulnerabilities and improve the organization's overall cybersecurity posture by guiding them through a series of questions that represent network security requirements. The presented requirement questionnaires are based on selected standards, common requirements, and the network diagram (or network topology and architecture).

The tool has a component focus rather than a system focus. Therefore, network architecture analyses, including network hardware and software configuration analyses, will be limited to the extent that they are defined by programmatic and procedural requirements.
CSET is not a risk analysis tool; it will not create a detailed risk assessment.
Most importantly, CSET is only one component of a comprehensive control system security program. A security program based on a CSET assessment alone must never be considered complete or adequate.

Maps to NIST SP-800-53.

https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET