Confidentiality, integrity and availability – finding a balanced IT framework

Michael Aminzade

Michael Aminzade, Trustwave

With the high level of cyber-risk facing organisations today, taking a thorough look at their risk management processes can be one of the most important activities of the year. Conducting a regular IT risk assessment is an essential task to ensure that the business's compliance standards are met. However, going above and beyond regulatory mandates, it is also vital for an organisation to be aware of what risks it is facing and what should be done to mitigate the threat and the impact.

When embarking on an IT risk assessment, it is advisable to evaluate the existing security that is already in place. Firms should take the time to identify which types of data will require the highest levels of security, as it is not practical or necessary to have all data protected at the same level. It is also essential to ensure that the risk mitigation and data protection strategy addresses the whole organisation, including mobile workers, third party vendors and supply chain partners. Failing to provide secure access to these groups can leave an organisation exposed to high-profile data compromises, data loss or misuse or the inability to access critical information.

Business-saving decisions

One of the main objectives of conducting an IT risk assessment is to use the information acquired to make business-saving decisions, identify key security deficiencies and to develop a plan for acknowledging and mitigating those risks.

The classic CIA triad is often used as a basis for carrying out IT risk assessments. The balance between the three points – confidentiality, integrity and availability – is one that is difficult to achieve. Too much of a focus on availability will likely compromise integrity and confidentiality, while a focus on confidentiality and integrity will inevitably impact availability. One point to consider if choosing to adopt this method is that cyber-criminals are also aware of these principles and can often exploit that knowledge to gain access to the IT infrastructure.

> ***"Cyber-criminals are also aware of these principles and can often exploit that knowledge to gain access to the IT infrastructure"***

When a business is embarking on an IT risk assessment, it must have clear business goals, knowledge and information on potential threats and have considered the likelihood of a compromise and the impact of the loss associated. One step that can be undertaken to achieve this is a comprehensive interview process involving all areas of the organisation, such as senior management and key stakeholders. This process will help to determine the current threat landscape and what level of risk the business is prepared to accept, and help to determine where the gaps in security lie. Once this has been done, the next step is to determine which security controls are necessary and how long it is going to take to implement them.

Which framework is best?

There are many different options for security risk assessment frameworks available for consideration. Two of the most widely recognised are frameworks from the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC), jointly the ISO/IEC, as well as the US National Institute of Standards and Technology (NIST).

The ISO 27000x Series provides a guide to best practice for the overall information security management system.[1] The framework encourages organisations to assess their IT risks, then put appropriate controls in place according to their specific needs. It incorporates continuous feedback and improvement activities to address the current threat landscape or take into account security incidents. The standard is not based on a particular risk management method but a continual process of structured sequences of activities.

The ISO 27000x series is designed to be used by organisations of all shapes and sizes: however, in some cases the level of detail involved in applying the framework will not be applicable. In these cases, using the broader, simpler OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) framework alongside ISO27000x will help to eliminate excessive 'not applicable' responses.

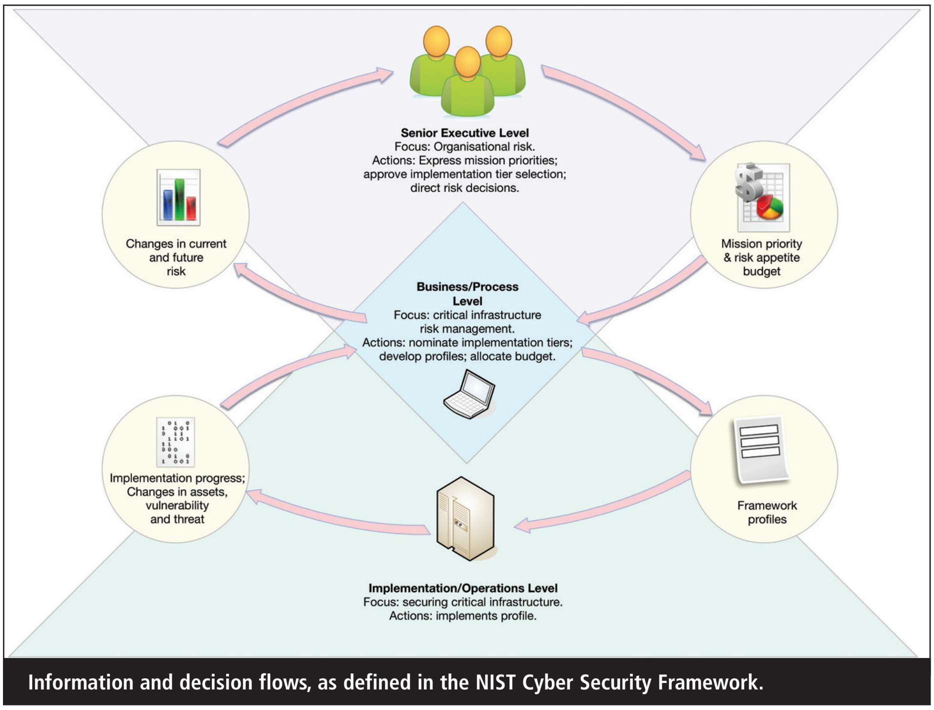
The OCTAVE framework is used to determine risk levels and for planning against cyber-attacks. Its structure is designed to minimise organisations' exposure to threats and to predict the probable outcomes of attacks and address the ones that succeed. The framework is split into three definitive phases – building asset-based threat profiles; identifying infrastructure vulnerabilities; and developing security strategy and plans. There are two versions of OCTAVE, with OCTAVE-S, providing a simplified version aimed at smaller organisations with flat hierarchical structures. OCTAVE Allegro, meanwhile, is a more comprehensive version aimed at large companies with multi-layered structures.[2]

For organisations particularly concerned with operational up-time, another strong option is COBIT (Control Objectives for Information and Related Technologies).[3] Developed by the Information Systems Audit and Control Association (ISACA), the most current version of COBIT, version 5, is a business framework intended for the governance and management of enterprise information technology end-to-end across the entire business. The framework is made up of five subsets each covering a domain – audit and assurance, risk management, information security, regulatory compliance and governance, and enterprise IT. The focus on up-time makes it a good choice for the likes of manufacturing organisations as it allows them to select appropriate governance domains depending on their risk categories and priorities.

Exploring NIST

Some of the best-known frameworks were created by NIST, itself a unit of the US Commerce Department. The guidelines published by NIST are available free of charge and have been seen to be useful to businesses, educational institutions and government agencies. The most commonly used NIST frameworks are 800-53 and the Cyber Security Framework (CSF).[4,5] Even though the CSF was initially launched by a US government agency, it is becoming more widely used across the globe. The framework recognises standards globally for cyber-security and NIST promotes it as a "model for international co-operation on strengthening critical infrastructure cyber-security".

NIST Special publication 800-53 was originally designed to help companies comply with the US Federal Information Processing Standards (FIPS). Included within this framework are strategies to harmonise the Federal Information Security Management Act of 2002 (FISMA) with the international security standard ISO/IEC 27001. The adoption of the newer CSF is picking up momentum as an alternate framework which is applicable to the requirements of risk assessments beyond government entities and the US.


Senior Executive Level
Focus: Organisational risk.
Actions: Express mission priorities; approve implementation tier selection; direct risk decisions.
Changes in current and future risk
Mission priority & risk appetite budget
Business/Process Level
Focus: critical infrastructure risk management.
Actions: nominate implementation tiers; develop profiles; allocate budget.
Implementation progress; Changes in assets, vulnerability and threat
Framework profiles
Implementation/Operations Level
Focus: securing critical infrastructure.
Actions: implements profile.

Information and decision flows, as defined in the NIST Cyber Security Framework.

> ***"In today's threat environment it is likely that most organisations have already been breached. It is important to be realistic with security expectations and be aware that 100% security does not exist"***

The first version of the NIST Cyber Security Framework (CSF) was released in 2014 as a result of the US Cyber Security Enhancement Act and was designed for improving critical infrastructure cyber-security. The framework is offered as a living document and incorporates information gained from new threats and risks and offers solutions by way of regular updates.

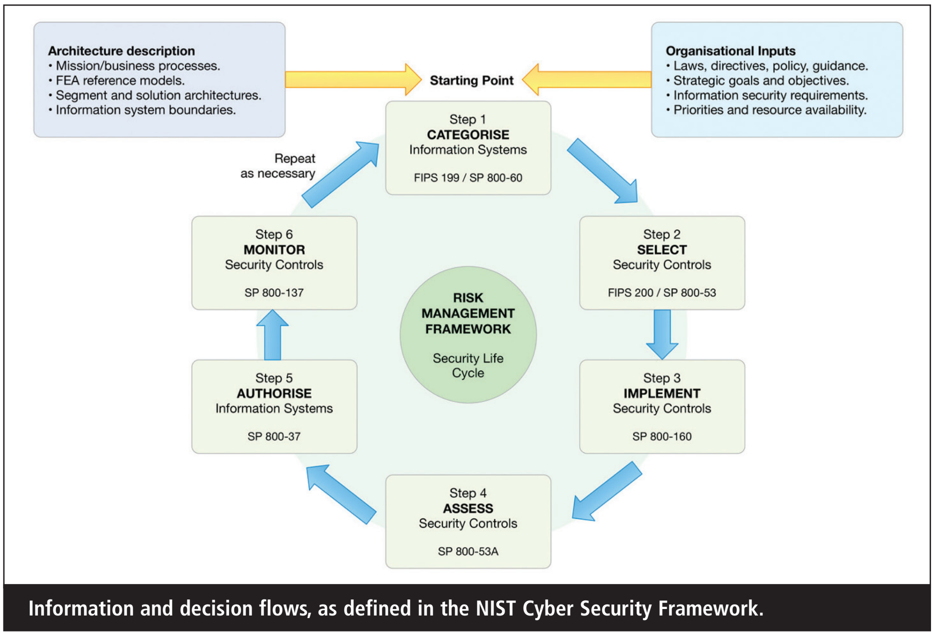
The framework is composed of three key components – framework profile, framework core and framework implementation tiers. It is intended to help organisations of any size and level of cyber-security sophistication to apply risk management best practice. The framework includes globally recognised standards that enables it to be relevant across the globe. The core enables communication of risk across the organisation by providing a set of activities which will achieve specific cyber-security outcomes. The implementation tiers categorise how an organisation manages cyber-security risks and the overall cyber-security risk management practices.

Best practice

With the increasing commercialisation of cybercrime, many businesses are moving from a compliance approach to a broader risk mitigation and data protection strategy. Prioritising a business's critical assets is an essential element in devising an effective security risk management programme.

Historically, risk assessments have been inclusive of the entire supply chain, not just internal systems. Recently though, we have seen an increased focus on the assessment of third-party vendor access to internal systems. Similarly, the BYOD trend has increased the need for stronger endpoint security.

Unfortunately, in today's threat environment it is likely that most organisations have already been breached. It is


Architecture description
• Mission/business processes.
• FEA reference models.
• Segment and solution architectures.
• Information system boundaries.
Starting Point
Organisational Inputs
• Laws, directives, policy, guidance.
• Strategic goals and objectives.
• Information security requirements.
• Priorities and resource availability.
Repeat as necessary
Step 1 CATEGORISE Information Systems FIPS 199 / SP 800-60
Step 2 SELECT Security Controls FIPS 200 / SP 800-53
Step 3 IMPLEMENT Security Controls SP 800-160
Step 4 ASSESS Security Controls SP 800-53A
Step 5 AUTHORISE Information Systems SP 800-37
Step 6 MONITOR Security Controls SP 800-137
RISK MANAGEMENT FRAMEWORK
Security Life Cycle

Information and decision flows, as defined in the NIST Cyber Security Framework.

important to be realistic with security expectations and be aware that 100% security does not exist. However, if a business implements state-of- the-art protection, there will naturally be an increased focus on detection, response and recovery and on the speed with which it is deployed after a breach.

Establishing a maturity model for a business is an essential part of current best practice. The Capability Maturity Model (CMM) was developed by the Software Engineering Institute, a research and development centre sponsored by the US Department of Defense.[6] Initially the model was designed to refine software development processes, but is now more broadly used in business processes. The model is made up of five levels: level one demonstrates disorganised or even chaotic processes. At the top end, level five demonstrates the optimal level of process, with constant improvement and the introduction of new and innovative processes.

Organisations that integrate their risk frameworks with maturity modelling are able to demonstrate to the executive what good looks like. This will be achieved with a three-to-five-year roadmap aligning the business goals and risk appetite, as well as the return on investment to achieve the previous two. The progress of moving the needle is trackable and quantifiable at regular checkpoints for the executive with programs that are set up in this manner. It also enables finance departments as well as operational departments to speak the same language and focus on helping the business and the executive team achieve the business goals.

Key considerations

Whether you are just beginning a business's security risk assessment for the first time or re-evaluating an existing one, it is essential to have executive support. Ultimately, senior management must understand and accept the inherent risks within their organisation. The CISO office may lead the risk assessment but they need to be either part of the executive team or have a direct channel of communication to it.

To keep an organisation secure it is necessary for every employee to understand their part in the process. Security needs to be emphasised from the top levels down through the entire organisation. It is also important to acknowledge to everyone that perfect security is not achievable and that the goal is to have the optimum level of security specific to the organisation, particularly in regard to fast breach detection, response and recovery.

With so many different security frameworks available, all organisations should be able to find a hybrid approach that will work best for them. The overall result must address the objectives of a seamless, comprehensive, appropriate and actionable assessment and take all internal and external risk factors into consideration. The assessment of an organisation's IT risks is not something to be taken lightly. As we have already seen this year, the likelihood of a ransomware attack or similar is higher than ever. The only way to successfully secure a company's security network is to regularly assess its structure.

About the author

Michael Aminzade is VP of global compliance and risk services at Trustwave. Possessing more than 20 years' experience in information security and compliance, he holds an extensive range of security risk qualifications, including CISSP, CISM, C|CISO, CRISC, QSA and PCIP. In his role at Trustwave, Aminzade is responsible for leading a team of security professionals that seek to advise businesses on how to develop and meet the objectives of their compliance, risk and security maturity programmes.

References

1. 'ISO/IEC 27000-series'. Wikipedia. Accessed May 2018. https://en.wikipedia.org/wiki/ISO/IEC_27000-series.
2. 'Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process'. Carnegie Mellon University, 2007. Accessed May 2018. https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8419.
3. 'What is COBIT 5?'. ISACA. Accessed May 2018. www.isaca.org/cobit/pages/default.aspx.
4. 'Security and Privacy Controls for Federal Information Systems and Organizations'. NIST Special Publication 800-53. National Institute of Standards and Technology. Accessed May 2018. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
5. 'Cyber Security Framework'. NIST. Accessed May 2018. www.nist.gov/cyberframework.
6. 'Capability Maturity Model for Software (Version 1.1)'. Carnegie Mellon University, Feb 1993. Accessed May 2018. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=11955.