bsi.

...making excellence a habit.™

Effective vulnerability and remediation management

Implementing a robust system

A Whitepaper

Executive summary

This insight paper discusses the benefits of adopting a vulnerability and remediation management system within an organization.

Through the adoption and implementation of a robust vulnerability and remediation management system, an organization can make continual improvements to the security posture of its systems, ensuring the on-going security of its critical business processes.

An effective system involves the implementation of vulnerability management software coupled with the development and deployment of well-designed supporting policies and procedures built in line with industry standards such as ISO PCI DSS and NIST

An effective vulnerability and remediation management system should have the goal of:

- Providing a repeatable and reliable platform to support the timely identification of internal and external vulnerabilities;
- Gaining an on-going, and in many cases a "real time" view of an organizations security posture;
- Reduce the likelihood of an external and internal threat taking advantage of unknown vulnerabilities;
- Increasing and streamlining remediation response times; and
- Reducing the overall threat profile to the organization to an acceptable level

This paper will discuss the following challenges of vulnerability and remediation management:

- Understanding the risk;
- Asset identification;
- Asset ownership and responsibilities;
- Asset criticality;
- Misunderstanding; and
- Remediation requirements and business objectives.

We will also provide insight on how the above challenges can be overcome, through the proposition of our preferred framework.

Introduction

As the internet and connectivity between systems has evolved, the threat of a cyber-attack against organizations has followed suit. Companies are now faced with two challenges to overcome; threats to their external networks and threats to their internal networks.

Prior to the implementation of a Vulnerability and Remediation Management System, the following list of questions should be considered:

- Is there a pre-existing vulnerability management system in place?
- Is there a formal patching policy & procedure in place?
- Do any vulnerability management processes, policies or procedure exist?
- Who has responsibility for vulnerability management currently within the organization?

- Does the organization have any external internet facing assets?
- What types of internal system components are in use in the internal IT environment?
- What data types are currently stored by the organization?
- Is the organization subject to PCI DSS, or any other relevant regulation / legislation?
- Have data and systems been formally classified based on their business value?
- What existing controls are in place to support the confidentiality of systems and data?
- What existing controls are in place to support the integrity of systems and data?
- What existing controls are in place to support the availability of systems and data?
- Is there an established SDLC (Software Development Lifecycle) in place which supports the privacy and security by design principal through each stage of the project lifecycle?
- Does the organization have any Intellectual Property which requires additional layers of protection?

The output from the above list of questions will, at a minimum help identify which assets are most critical and as such, require the most attention and focus.

Remediation of identified vulnerabilities should always follow a risk based approach, placing focus on:

- Criticality of assets (asset value)
- Susceptibility to attack (likelihood of occurrence); and
- Criticality of issues (Impact)

We have found that many organizations do not have an effective vulnerability management program in place, often leaving themselves exposed to existing and emerging risks and threats. It is not uncommon for an organization to develop their networks without taking into account the vast array of external and internal threats that exist today. Another layer of complexity that some organizations are faced with is the pre-existence of legacy applications and systems, which were not originally designed with security in mind. Additionally, the issue of scale can also cause problems for some organizations. Where organizations are large in size or located over multiple geographical locations, the question of "*Where do I start?*" comes into play. Regardless, a structured planned and methodical approach should be taken to ensure a consistent and repeatable process is implemented.

Based on these factors it is imperative that organizations apply a commensurate level of security controls / protection to data and systems, based on their classification level and importance to the overall business model. Vulnerability and remediation management forms one layer of the multi-layer approach required to operate securely in today's environment.

The purpose of the framework outlined in this paper is to provide a strategy to enable an organization to gain an understanding of their threat profile, and subsequently implement a functional effective Vulnerability and Remediation Management System that offers:

- Internal and external coverage
- Prioritization of assets
- Classification of vulnerabilities against prioritized assets
- Triage
- Vulnerability remediation

Challenges

There are many challenges that must be overcome by organizations that are considering the implementation of a Vulnerability and Remediation Management programme.

Challenge no. 1 - Understanding the risk

To achieve and maintain "Executive and Senior Management buy in", organizations must be prepared to invest time into understanding the risks and threats to the organization which can result from the non-identification and/or delayed response to technical vulnerabilities. Some risks that may result from technical vulnerabilities include:

- The potential loss of data as a result of a breach or control failure
- Reputational damage and subsequent profitability losses resulting from publically disclosed breaches or incidents
- Inability to trade for extended periods of time, due to denial of service attacks or system compromise
- Inability to recover in a timely manner from a combination of any number of the above risks

Ultimately, the vulnerability profile of critical IT systems can have knock on effects, and/or negative impacts on business processes, business objectives and the overall strategic goal of the organization. As such, security and effective vulnerability management is crucial to the continued protection of these critical assets and the key business processes they support.

Identification, qualification, quantification and proactive management of the risks associated with technical vulnerabilities are the key elements which are required in order to provide senior management with timely, accurate and reliable data. This will enable management to make informed business decisions relating to budget spend, and allocation of resourcing to support the vulnerability management programme.

Challenge no. 2 - Asset identification

An effective Vulnerability and Remediation Management System relies upon having a complete, accurate and up to date inventory of all assets. Without clear visibility of an organization's true asset inventory, it's possible to "miss" assets and asset groups throughout the vulnerability management lifecycle.

In cases like this, where there are instances of shadow IT, management will not have an accurate viewpoint of the overall threat profile of the organization. These vulnerable unknown assets may offer an attacker a way into your internal network or access to sensitive data.

We advise that a good starting point for building an accurate asset inventory, is to perform a discovery scan against all owned network ranges, with the aim of identifying all live systems on those networks. Once all known network ranges and systems have been mapped, assets can be on boarded into an asset register, which will ultimately provide management with clear visibility of their assets.

Additionally, it would be advisable to run multiple scans to validate your asset discovery baseline, to allow for the identification of systems which may have been temporarily switched off for system maintenance or other legitimate business reasons.

Challenge no. 3 - Asset ownership and responsibility

A challenge that many organizations face, relates to the lack of pre-defined business and IT asset ownership. Without allocated ownership, it can be quite a difficult task to progress timely remediation of identified vulnerabilities. Additionally, this challenge can be increased when coupled with a decentralized remediation management framework.

In many large organizations, it is not uncommon for vulnerabilities and or/security risks to be identified and escalated for remediation from various different channels / teams (e.g. internal audits, security reviews, vulnerability scans, penetration tests, project reviews etc). Regardless of where a vulnerability is identified, we recommend that a clear and transparent remediation approach is followed, so that management, on request, can firstly obtain up to date detail on the remediation status of specific open items, and

also can be presented with a view of all open vulnerabilities within the organization.

To support this, it is critical that management understand, agree and formally allocate ownership of systems, services and the supporting IT assets to ensure that responsibility for vulnerability remediation for a particular asset is clearly defined. Once allocated, owners are then accountable for remediation activities and the on-going vulnerability profile of the asset.

Challenge no. 4 - Asset criticality

A key challenge that organizations face is the priority and order in which remediation activities should take place. It is a common mistake to complete remediation activities based solely on the criticality score of the vulnerability alone. The review of vulnerability scoring coupled with asset criticality will enable the business to accurately prioritize remedial activities, and ultimately reduce the likelihood of a significant risk materialising.

For this process to be successful, management need to ensure that criticality scores have been defined for all IT assets. As a critical asset to one team's operation may not be critical to the organization's overall operation, the valuation of an asset should be agreed at a strategic level.

Additionally, management need to define remediation response times, which both meet industry leading practice guidelines and are commensurate with the risk appetite of the organization. In general, critical issues identified against critical assets should be resolved as soon as possible, where safe to do so; however timelines can and do differ between organizations. As an example, the Payment Card Industry Data Security Standard recommends that critical vulnerabilities are remediated within a 30 day window or sooner where required.

Challenge no. 5 - Misunderstanding

A challenge exists where organizations have a misunderstanding of what an effective vulnerability management programme entails. It is not uncommon for management to assume that they have a comprehensive programme in place following a deployment of a well-regarded automated vulnerability management solution. While automated vulnerability management solutions provide valuable insight into an organization's technical security posture, they are of limited value, if they are not supported by well-designed processes and procedures.

Processes and procedures are required to be in place to ensure that staff are aware of their responsibilities, and the steps that must be followed to ensure a structured and repeatable approach is taken to vulnerability and remediation management. Having these in place ensures that vulnerability resolution can be handled in a consistent and effective manner that has been approved by senior management.

Developing and implementing processes and procedures to support existing vulnerability management software enables companies to effectively manage tasks such as; issue prioritization, timely vulnerability remediation, false positive identification, update of asset inventory, and assignment of ownership and responsibility.

Challenge no. 6 - Remediation requirements and business objectives

A further pitfall relating to vulnerability management can be where a team or business unit refuses to prioritize the remediation of identified issues within an acceptable timeframe. For example, if the business process maximum tolerable downtime does not allow for the service to be offline, to allow for a patch to be applied. In these instances, it is essential to have a formally defined escalation process, so as to provide the vulnerability manager an avenue to raise concerns with senior management. The goal of the escalation process is not to act as a finger pointing exercise, but more to provide senior management with an overview of associated risks and consequences of not completing the remediation in a timely manner. This process will then enable senior management to make an informed decision with regard to the assessment of the cost / benefit of implementing the fix.

Vulnerability and remediation management framework overview

Our approach when assisting clients with the development and implementation of a robust Vulnerability and Remediation Management System is based around the use of Qualys' industry leading vulnerability management software, combined with the development of supporting processes and procedures. These supporting documents are tailored to suit each organization's unique requirement.

For the purposes of this white paper, we have outlined the various steps involved in a vulnerability and remediation management framework that can be applied to any organization.

Please Note: It is assumed that all required policies and procedures have been designed, approved and implemented prior to the use of the below framework.

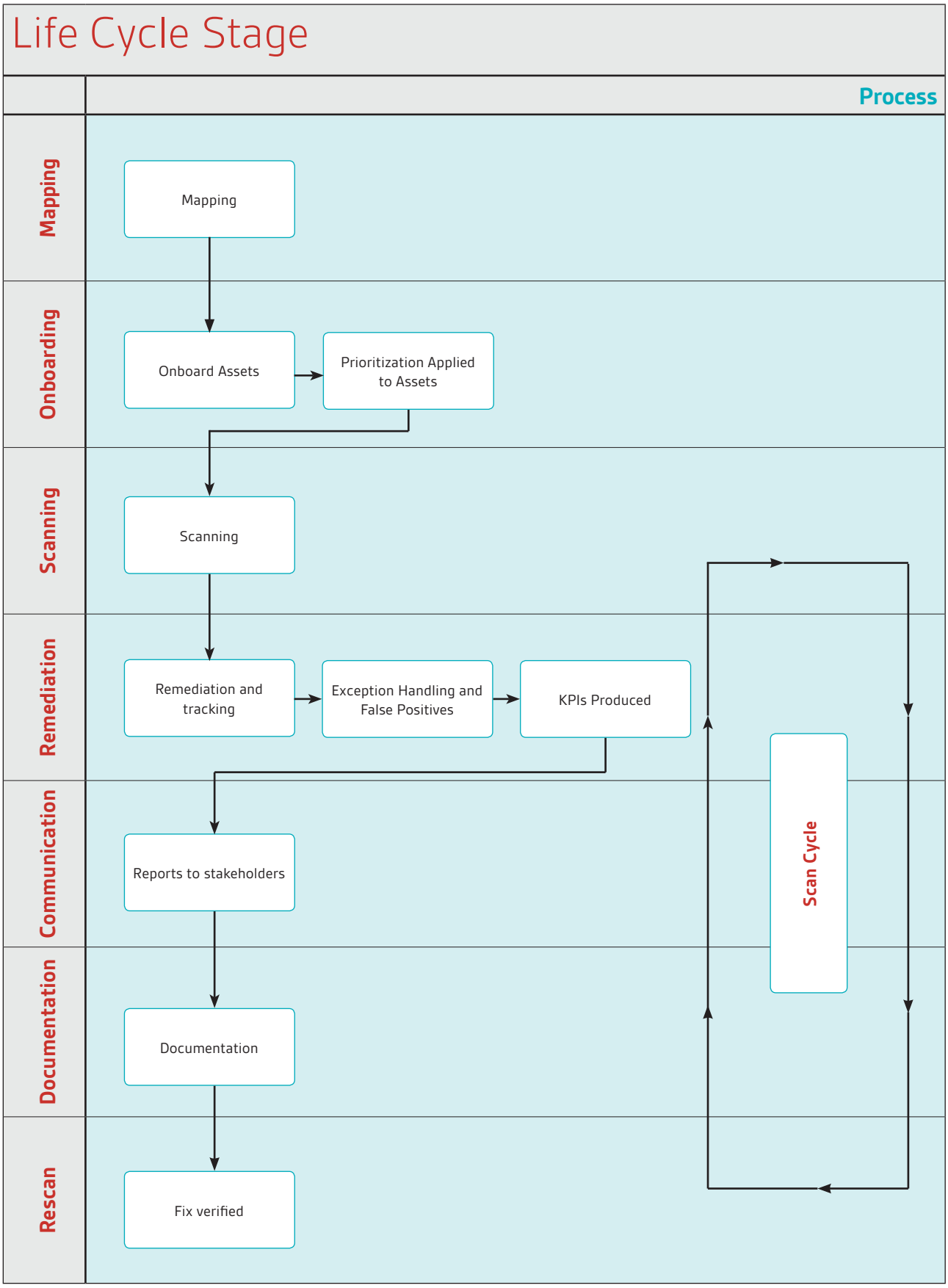
The framework is made up of the following phases:

- Phase 1: Mapping
- Phase 2: On-boarding;
- Phase 3: Scanning
- Phase 4: Remediation
- Phase 5: Communication
- Phase 6: Documentation
- Phase 7: Rescanning

A detailed overview of our framework can be seen on the next page.

Phases

The following is a sample lifecycle for the framework



Phase 1: Mapping stage

The first action to undertake as part of the framework is to map the entire network range owned by the organization. Typically, this is done by performing map scans of known internal and external address ranges.

Mapping should be performed in accordance with an organization's IT department and any third parties who may host an organization's external assets. This is an on-going process, as networks can and do change overtime, as new systems are added, and older machines are decommissioned.

The mapping stage provides an organization with the visibility of "live" assets across their network and is the initial piece required to perform the on-boarding stage.

A key consideration prior to performing mapping is to assess whether the discovery scan can have any negative impact on the network or associated systems. Prior to performing scans, a risk assessment should be performed, with outputs shared with management, so as to get final approval prior to commencement.

Phase 2: Asset On-boarding stage

Once assets have been discovered, they must be on-boarded into an asset register. The asset register will document the criticality of each asset based on pre-defined criteria, which can include, but is not limited to the following:

- The key business processes that the asset supports
- Whether the asset is internal or externally facing
- The classification of data that is stored, processed or transmitted by the asset
- Relationship of the asset to relevant compliance or legislative requirements
- Availability requirements or demands on the asset

Assessing the criticality of each asset based on business risk ensures that an appropriate level of focus is placed on the asset and identified vulnerabilities are addressed in order of priority using a risk based approach. This ensures the maximum business value and return on investment is realised for all remediation activity.

Phase 3: Scanning stage

Scanning

Armed with a complete asset register, IP addresses for the organization's assets will be on boarded onto the vulnerability management solution. Typically, an organization's assets are grouped by criticality, ensuring that critical assets are scanned first. Organizations may also group and scan assets based on any criteria, such as operating systems, location, department, etc, which is left to the discretion of management.

Vulnerability management solutions, such as Qualys allow for:

- Tailored scan policies and assessments
- Tailored scheduling of scans to ensure assets are scanned in line with business and compliance requirements

Findings review

Once scans are completed, the vulnerability management solution can issue reports on an asset by asset basis, or can be scaled to cover the entire scope of the organization's assets. Reports can also be tailored for different audiences, ranging from granular technical details to comprehensive executive summary information.

These reports should be communicated to asset owners and management for review, and the process of root cause analysis should be initiated.

Following the review of all findings, management and project stakeholders can begin the process of issue ownership and resource assignment.

Phase 4: Remediation stage

Remediation

The identified vulnerabilities and resulting remediation strategies should then be placed into a tracker, to facilitate a structured approach to remediation management. We recommend the development of tailored dashboards within the Qualys cloud suite to give a live view of the current vulnerability profile on an asset by asset, or asset group basis. This depends entirely on the preferred method of the business and can be adapted as required. Dashboards can be used to view vulnerability management trends, which can be very useful when assessing current and historic results and monitoring key performance indicators (KPI's).

Vulnerabilities should then be prioritized and resolved based on the organization's business requirements, risks and resource availability. This may vary from addressing issues on individual critical assets, to resolving vulnerabilities with similar root causes that affect multiple assets located across the organization's IT infrastructure.

Remediation activities should continue to be performed,

until all issues against all assets are remediated or accepted in line with the business risk tolerance. This is an ongoing process once the next sets of scans have been completed.

Exception handling

Exception handling is generally a necessity for a number of organizations and is entirely driven by; an organizations scale, existence of legacy IT systems, risk appetite, and platform dependence. Dependent on the asset assessed, and the resources available, it may not be possible in all cases to perform remediation activities. This can typically be seen in software platforms which do not support backwards compatibility or upgrades, or where, the cost or impact of implementing a fix, outweighs the benefits of completing remedial activities.

Exceptions and exception handling are a reality of any vulnerability management system. Where management have accepted the risk associated with an identified exception, this must be formally recorded and managed in the organization's IT risk register, or equivalent. Compensating controls and/or alternative remediation strategies should be designed and implemented to reduce the impact or likelihood of the exception being exploited.

Exceptions must be accurately recorded in the organization's vulnerability management system, to avoid the scanning software re-identifying known exceptions as vulnerabilities. This is an essential step, as the scanning software will not have detail of the newly designed compensating control. We advise that a predetermined expiry date should be set for each exception, which is based on the risk appetite of the business, after which point the value and compensating controls must be re-evaluated.

False positives

False positives are also a typical by-product of using any automated vulnerability scanning software. These automated solutions depend upon the responses from the scanned system, which can vary in detail. The solution can only perform a limited number of checks to verify the presence of vulnerabilities without potentially impacting the stability of the system, so it is imperative to review the technical details for all findings and review any issues marked as "potential". False positive results can be reduced by providing the scanning solution with credentials or additional access to in-scope systems, so that further more in-depth analysis can be performed. False positives can also be tracked and recorded in within the vulnerability and remediation management system.

KPI generation

Key Performance Indicators (KPIs) can be built out during the remediation phase, and trend analysis can be completed to present changes from month to month, showing progress to Senior Management. The ultimate goal of presenting KPI's to management is to support informed decision making relating to the allocation of budgets and resourcing.

Some typical KPIs are listed below:

- Average number of high and medium issues per host
- Number of "Clean" assets
- Number of systems with critical issues identified by vulnerability scans
- Number of critical vulnerabilities addressed within 30 days of identification
- Number of exceptions
- Number of false positives

Supporting documentation should be available to management on request, to provide more granular detail or a background on vulnerabilities and their associated remediation plan.

Phase 5: Communication stage

Transparent and timely upward communication and escalation channels to senior management are the cornerstone of every successful vulnerability management system. While the level of detail required may vary depending on the audience, it is critical that the business have a full and up to date understanding of the status of the vulnerability management programme. Typical items that are communicated to management are KPI's, programme updates or changes, detail of risks to the programme. These details are essential to help management understand and justify return on investment (ROI).

Phase 6: Documentation stage

Reporting of identified vulnerabilities is a key phase within the vulnerability management lifecycle and is likely to take place at various junctures, e.g. post completion of scan cycle, post remediation phase, and during the development of KPI's.

Reports should be issued to different stakeholders in varying degrees of depth, i.e. the board would typically have dashboard overviews, whereas the centralized point of contacts or system owners may want more tailored granular reports.

It is essential that reports are reliable, timely and easy to read so that management and other key stakeholders can obtain quick and accurate information relating to the security posture of the assets under their responsibility.

Additionally it is advisable that historic reports are retained, so that they can be used as reference points for future analysis, or to facilitate trending of vulnerabilities. Historic reports can also be used to support root cause analysis during the remediation phase, whereby previously applied fixes or investigations can be re-used in instances where identified vulnerabilities reoccur. With a tool such as Qualys, all reports can be templated and automatically distributed as required.

Phase 7: Rescan stage

A common mistake when undertaking a vulnerability and remediation management system is to treat security as a project with a start and end date. If vulnerability management is not continuously performed, an organization's security posture can decline over time. Threats and new vulnerabilities can surface at any time, either through new exploits or security misconfigurations.

This framework advocates a consistent and continuous scanning and remediation cycle, in line with risk appetite and industry standards such as PCI DSS, NIST and ISO27001.

Restarting the cycle validates the success of remediation work, as well as detecting and highlighting new vulnerabilities. For larger global organizations, assets can be offset into groups, meaning that assets can be in different phases of the cycle at different times or geographic areas. Mapping can be incorporated into the rescan cycle, to identify new assets as they are introduced to the network.

Additionally, following the remediation of more critical vulnerabilities, it is advisable to perform a rescan on the specific asset(s) as soon as possible, to validate the success of the remedial activities.

Conclusion

To combat today's evolving threat landscape and to support a continual improvement ethic, which will ultimately lead to increased benefits to an organisation's security posture, we recommend the implementation of a vulnerability and remediation management system.

To ensure the successful design and implementation of this, an organization must first:

1. Establish a clear understanding of business objectives and requirements
2. Understand risks relating to technical vulnerabilities and how they can impact the organisation and its business objectives
3. Understand which assets support business critical processes and classify
4. Have visibility and allocated ownership of all assets within the organisation
5. Design and deploy supporting processes and procedures to support the various elements involved in the vulnerability management process

Implementing a vulnerability and remediation management system is an ongoing and evolving process and using vulnerability management software such as Qualys, coupled with the appropriate supporting controls, processes and procedures, will improve vulnerability strategy, timely remediation and overall security posture of the organisation.

We advocate the use of a risk based approach to vulnerability management, which will inevitably identify and prioritize the protection of business critical assets and processes. Additionally this will ensure that continuous assessments and remediation strategies are aligned with business risk, impact and criticality.

Our vulnerability and remediation management system provides organizations with a proven methodology which draws from industry standards such as ISO 27001, PCI DSS and NIST. Organizations who are undertaking the framework are placed in a fundamentally stronger security position, ensuring the on-going protection of their critical business processes.

Cybersecurity and Information Resilience services

Our Cybersecurity and Information Resilience services enable organizations to secure information from cyber-threats, strengthening their information governance and in turn assuring resilience, mitigating risk whilst safeguarding them against vulnerabilities in their critical infrastructure.

We can help organizations solve their information challenges through a combination of:

Consulting

Cybersecurity and information resilience strategy, security testing, and specialist support

Training

Specialist training to support personal development

Research

Commercial research and horizon scanning projects

Technical solutions

Managed cloud solutions to support your organization

Our expertise is supported by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™

CYBER ESSENTIALS

CSA cloud security alliance℠

bsi.

Find out more
Call UK: +44 (0)345 222 1711
Call IE: +353 (0) 1 210 1711
Visit: bsigroup.com