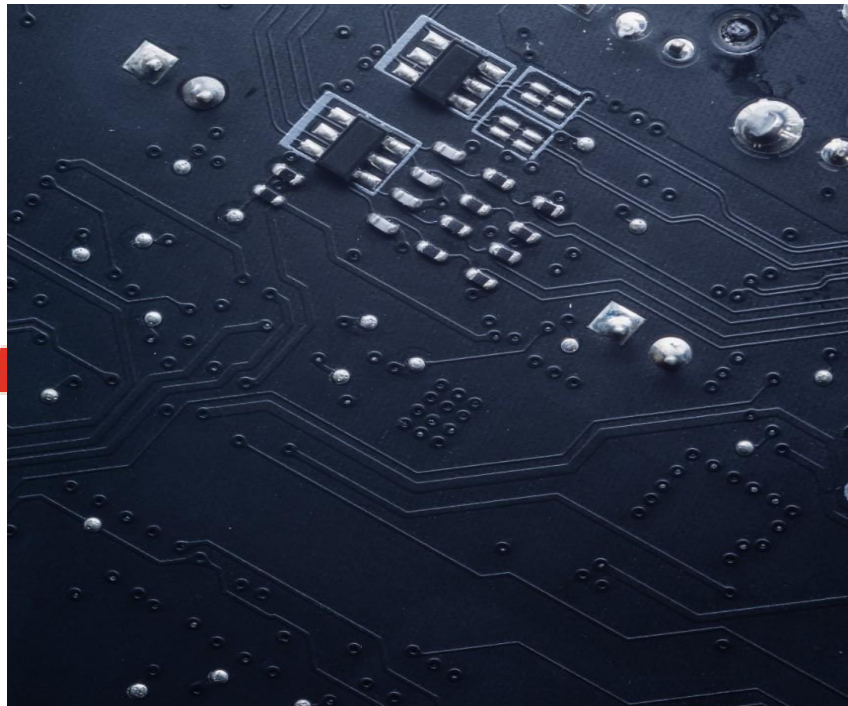
Cyber Security Services



pwc

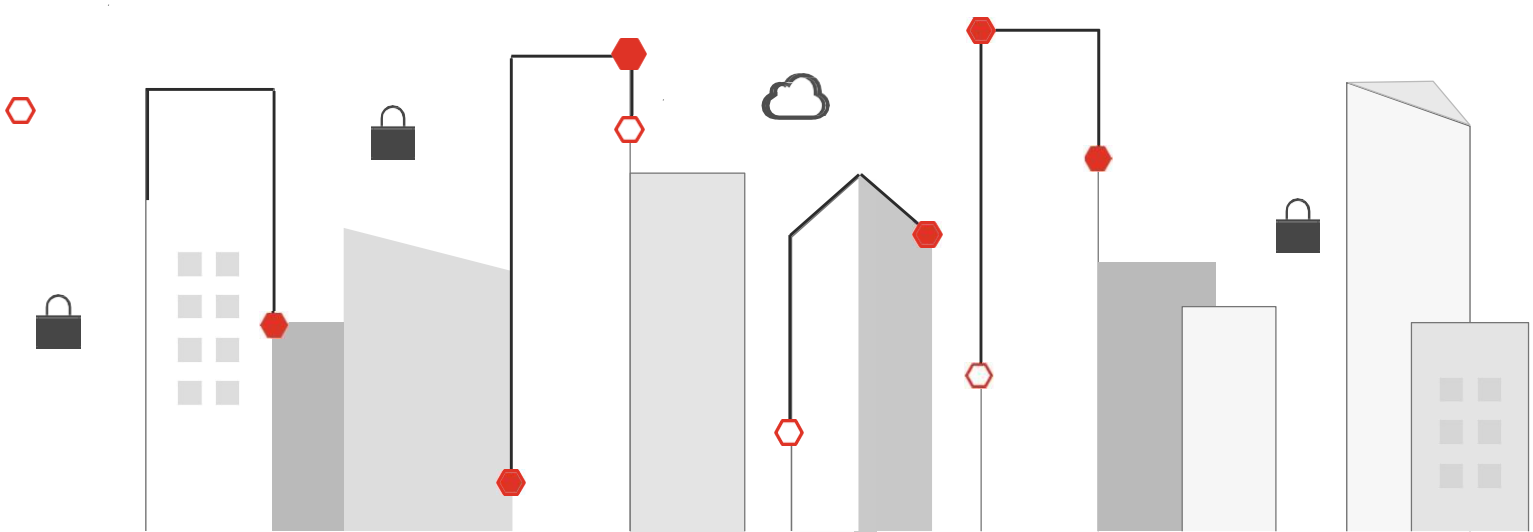
Content

How we can help you

At PwC, we can utilize our expertise to **help you build resilient operations and reduce cyber risk**. We can help you to obtain the clarity your business needs to allow you to confidently adapt to new challenges and opportunities.

Our services are designed to:

- **enhance your team members' security awareness**
- **enhance your processes**
- **reduce your technology weaknesses**
- **boost your cloud security position, and**
- **continuously improve your security**



Our services

The PwC **cyber threat intelligence team** gathers information about the tools, techniques and processes used by real world attackers. We utilize this information to assess the full suite of defense controls, including the often overlooked areas of people and processes.

Our **people awareness services** support your team members to take appropriate security related actions when needed.

Our services related to **risk management and governance** help you improve security procedures with contextual insights gained from analyzing data sources.

Our **penetration testing services** apply tailored testing methodologies to identify security vulnerabilities and issues which could be exploited by real world threat actors.

Our **advanced penetration testing services** (e.g. red teaming) help organizations understand how to defend themselves against cyber attacks such as gaining access to a critical application or stealing privileged credentials. The way which the attack is carried out could involve multiple vectors to achieve this goal.

Cloud computing is an integral part of any modern IT infrastructure. It offers numerous advantages such as high flexibility and less complexity, but comes with some challenges such as responsibility for data protection or data location or data access control.

Our **cloud security services** help you establish the measures you need for cloud security. We take into account your company risk profile as well as the level of protection which your systems and data need.

Portfolio

Information & Cyber Assurance Services

Executive Summary

Cyber Risk is a business risk. The question is **“Are you confident** in your cyber security position and ability to manage cyber risks?”

If in doubt, welcome to our world!

What are Information & Cyber Assurance Services?

Evaluation of subject matter from cyber and information security perspective against a defined criteria. The conclusion is designed to enhance the degree of confidence in the compliance with the required controls and is supported by sufficient and appropriate evidence.

Information & Cyber Assurance Services

Subject Matter:

- ✓ Cyber and Information Security Risk Management
- ✓ Application and Infrastructure security
- ✓ Security Strategy, Operating Models, Architecture, Program
- ✓ Core Cyber Functions: Identify, Protect, Detect, Respond, Recover
- ✓ SOC2: Service organization control compliance with Security, Availability, Processing Integrity, Confidentiality and Privacy principles
- ✓ SOC1: Controls at service organization relevant to the accuracy and completeness of your financial reporting process operate effectively
- ✓ Digital channels, Supply chain, Remote work, Cloud

Information & Cyber Assurance Services

Criteria:

- ISO/IEC (27000 series, 31000 family, 22301, 33001,2000, etc.);
- ITIL (v.3 and v.4);PCI DSS; PSD 2; SANS; CIS; COBIT;
- OWASP (Open Web Application Security Project);
- ISAE 3402; ISAE 3000; SOC 1; SOC 2; NIST

Benefits:

- ✓ **Reduce risks**
- ✓ **Manage and prioritise costs and investments**
- ✓ **Embrace digital with confidence**
- ✓ **Boost your regulatory trustworthiness**

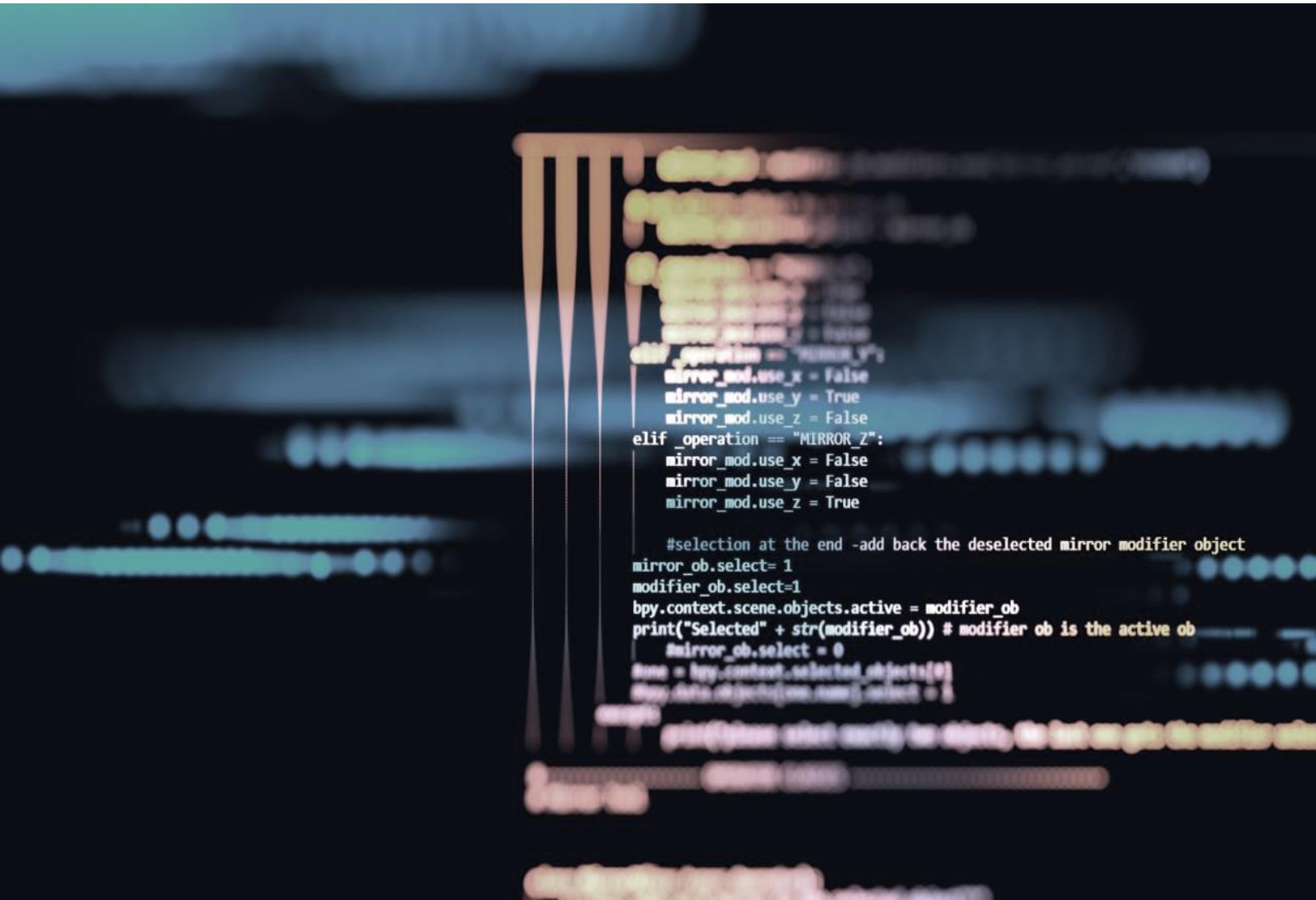
Target Audience: CTO/COO/CISO

Cyber Security Maturity Assessment

Executive Summary

Cyber security is a **principle enterprise risk** which has long been comfortably settled into executives' agendas. It is the inevitable companion of the flourishing digitalization, but it goes far beyond information technology.

Despite the advanced security technologies and the evolving cyber security practices, diverse failures are commonplace. Recent trends and cyber security statistics reveal a **significant increase in targeted, high profile and disruptive security breaches threatening financial and physical resources** across critical national and corporate infrastructures.



Cyber Security Maturity Assessment

Critical Questions

- When did you get the last report on cybersecurity threats & risks?
- Are you getting a regular, reliable report on financial risks?
- Do you know your financial position and your key figures? Do you also know your cybersecurity situation and your cybersecurity risk potential?
- You have competent accounting, finance and controlling. What about your cybersecurity team?
- Would you like to digitize your company? Are you aware of the risks?
- Can you rely on your cybersecurity?

What is Cyber Security Maturity Assessment

Cyber Security Maturity Assessment answers the questions above. It is an **objective, in-depth review of the organization's cyber security effectiveness**, along with prioritized remediation guidance. It takes a rounded view of people, process and technology and combines core components from key industry frameworks, including ISO 27001, NIST Cybersecurity Framework, CIS Critical Security Controls Top 20, PCI DSS, OWASP.

Using questionnaires, interviews, workshops and in-depth analysis of high-risk areas, we work with the key technical, commercial and executive stakeholders in the organization. Looking at current activities, future plans, the organization's technological and strategic direction, and its approach to risk helps us to **build a picture of the organization’s cyber security, identify key weakness and draw a strategic roadmap.**

Cyber Security Maturity Assessment

Benefits

- ✓ **Modular approach**: Assessments can be adapted to the needs and the level of cyber maturity of the company.
- ✓ **Reuse options**: Methodology and procedures can be used for internal purposes (internal audit) and results can be compared.
- ✓ **Awareness-raising**: In addition to the comprehensive examination, the contact persons on the part of the company are made familiar with the increasing threats from the cyber sector and are given comprehensive and cross-topic advice by the competent PwC experts.
- ✓ **Manage and priorities costs and investments**: Identified red flags represent fields of action in which there is an urgent need for action. Thus measures can be worked out in a targeted manner and planned in a risk-oriented manner.
- ✓ **Reduce risk**
- ✓ **Embrace digital with confidence**
- ✓ **Boost your regulatory trustworthiness**

Target Audience: CTO/COO/CISO

Cybersecurity Governance

What is cybersecurity governance?

The policies, procedures and practice in place aimed at strengthening the capacity of any one organisation to prevent, detect, and mitigate malicious activities and actors in cyberspace, whilst ensuring compliance with existing legislative and strategic frameworks, obligations and expectations.

Services we offer entail:

1. **Cybersecurity policy advice** - With the complexity of cybersecurity governance constantly expanding, we are seeing a growing overlap of jurisdictions, obligations and expectations at the international, regional and local level. Detailed policy analyses and tailored recommendations will support you in developing clear roadmaps for ensuring rounded-up compliance with European frameworks and best practices, at the same time tailored to local legislation and existing capacities.
2. **Cybersecurity strategy development support** - Adopting a similar approach to policy advice, strategic development support is there to help your institution and/or organisation to establish a clear and plausible vision and mission, identifying also the steps for achieving these in the short, medium and long term.
3. **Cybersecurity Awareness Raising** - Understanding that strengthening the capacity of individuals is the best strategy for ensuring greater cyber resilience, we can provide cybersecurity awareness training tailored to specific contexts (public administration, private enterprise, small and medium sized businesses, etc.) and levels of decision-making/nature of tasks.

Cybersecurity Governance

Benefits:

- ✓ **Keep track of both national and international developments in the field of cybersecurity governance** affecting your organisation both in terms of obligation and voluntary practice
- ✓ **Ensure a comprehensive approach** taking into account the effects the proposed solutions will have on a wide pool of stakeholders, from the public and the private sector
- ✓ **Develop policies and strategies** tailored to your organisation's goals, needs and capacities, thus ensuring implementability in the short-to-medium and sustainability in the long-term.
- ✓ Support your colleagues to **strengthen your organisation's resilience** by providing them with tailored know-how on cybersecurity basics
- ✓ Make use of our **cybersecurity governance team**, experienced in providing comprehensive analyses and tailored advice, with hands-on experience in cybersecurity policy and strategy development.

Target Audience: Different levels of both public and private sector in charge of cybersecurity governance and beyond

Cyber Red Flag Analysis

Red Flag analysis is a **comprehensive tailor made cyber security assessment**. It allows us to identify **opportunities for strengthening cybersecurity areas**. Configurable and customizable based on client preferences, size and industry and based on international standards like ISO, NIST, OWASP, CIS.

- Consists of **11 audit areas, 39 risk categories and more than 200 specific risks**
- **Assessment planning** -> Self-assessment –> Red flag workshop -> Deep dive audit –> Results presentation and audit report
- Establish an **overview of client's security position** with periodical reassessments to follow the maturity evolution

What is in there for the clients?

- **Risk management:** Identifying the most critical areas in the client's security position, thus enabling targeted and cost-effective risk mitigation
- **Modular approach:** Tailor-made assessment, based on client's preferences, size and industry
- **Raising awareness:** In addition to being thoroughly examined by the PwC experts, the client's security staff's knowledge on cyber threats is being increased
- **Methodology:** Client receives methodology and can reuse it for internal purposes, e.g. internal audits

Information Security
Risk Management and Compliance

Executive Summary

Organizations are becoming increasingly dependent on highly complex ecosystems to communicate and interact with customers, partners and third parties, on data-driven intelligence to boost reach and wins and improve decision-making. Technology-based innovations and initiatives open doors to **cyber risks and pose greater governance challenges.**

We can help with:

- **Defining and setting up cyber strategic direction**
- **Managing, monitoring and reporting on cyber risk**
- **Building up comprehensive catalogue of cyber controls**
- **Designing review of cyber security policies and procedures**
- **Providing customized cyber security awareness trainings**

Information Security
Risk Management and Compliance

What is Information Security, Risk Management and Compliance?

It is a set of services to enable and **enforce organization's cyber governance, management and strategic focus.**

Security Control Optimization

Designing a comprehensive and **optimized catalog of controls which enables companies build and maintain secure processes, systems and applications.** We focus on identifying redundancies in control objectives to allow for different aspects to be addressed with fewer controls covering multiple requirements based on analyzing variety of statutory, contractual, and good practice frameworks and standards.

Security Policies and Procedures Design

Consulting services designed to assist in organization's **security policies and procedures design and implementation initiatives** while meeting organizational objectives, regulatory and contractual requirements.

We provide practical guidance, hands-on assistance and insights for setting up an effective requirement scheme that is aligned with best practices and international standards *(NIST Cybersecurity Framework, CIS Critical Security Controls Top 20, PCI DSS, OWASP, ISO 27001).*

Information Security
Risk Management and Compliance

Security Strategy Design

PwC follows a **four-phased approach** for helping clients develop a security program.

1. Strategic Driver Analysis - We work collaboratively with your security team and internal stakeholders to define the expectations and drivers of the security program.
2. Target State Design - Business knowledge and understanding of industry trends coupled with our technical know-how and experience allows us to evaluate your key business, risks, and compliance. requirements in order to define your future state vision and priorities;
3. Gap Analysis - We leverage a variety of frameworks, industry standards, information gathered through interviews, technical assessments, documentation review to assess your security program against capability maturity levels in each of the security functional areas.
4. Roadmap Development - Using the gap assessment results, PwC will work with you to develop a prioritized roadmap to help realize the stated benefits of the enhanced the security program function.

Security Compliance

Our in-depth knowledge, understanding of the industry and experience with the most pervasive and influential cyber and security frameworks and standards could help you **put an end to a regulatory confusion.**

We work directly with your team to help your **company maintain the complete compliance that your business depends on.**

Frameworks and Standard: NIST Cybersecurity Framework; PCI DSS; SWIFT CSP; ISO 27000 series, CIS Controls and Benchmarks, GDPR, SOX, etc.

Penetration Testing

Web application penetration test

The main goals of this assessment are:

- **Identifying and assessing the feasibility and impact of technical attacks against the web application(s)** with the intent to gain access to resources and data. This activity will simulate attacks that could be performed from authenticated and unauthenticated adversaries who can interact with the web applications (i.e. external and/or internal adversaries), and
- **Recommending appropriate actions** to manage the identified issues/weaknesses/vulnerabilities.

Timeline:

On average **10 man-days** are required to perform a web application penetration test that will assess one application.

Penetration Testing

Internal penetration test

The main goals of this assessment are:

- **Identifying and assessing the feasibility and impact of technical attacks against the internal targets** of evaluation with the intent to gain access to resources and data. This will simulate attacks that could be performed from adversaries who have managed to gain access to your network (i.e. internal adversary), and
- **Recommending appropriate actions** to manage the identified issues/weaknesses/vulnerabilities.

Timeline:

On average **5 man-days** are required to assess 25 internal IP addresses. The client can provide the IP addresses or the penetration testers can select these from devices identified in the network range provided by the client.

Mobile application penetration test

The main goals of this assessment are:

- **Identifying and assessing the feasibility and impact of technical attacks against the targets of evaluation** with the intent to gain access to resources and data located on the mobile device and the back end systems the mobile applications interacts with. This activity will simulate attacks that could be performed from authenticated and unauthenticated adversaries who can interact with the mobile application, and
- **Recommending appropriate actions** to manage the identified issues/weaknesses/vulnerabilities.

Timeline:

On average **10 man-days** are required to perform a mobile application penetration test that will assess one application. Please note that:

- Android and Apple implementations of the same application are considered different applications for the assessment purposes as they are most likely built with different technologies, and
- The time it takes to complete this assessment varies based on the complexity and size of the application.

Penetration Testing

API penetration test

The main goals of this assessment are:

- **Identifying and assessing the feasibility and impact of technical attacks against the API(s)** with the intent to gain access to resources and data. This will simulate attacks that could be performed from authenticated and unauthenticated adversaries who can interact with the exposed API(s) (i.e. external and/or internal adversaries), and
- **Recommending appropriate actions** to manage the identified issues/weaknesses/vulnerabilities.

Timeline:

On average **2 man-days** are required to perform a test of one API.

External penetration test

The main goals of this assessment are:

- **Identifying and assessing the feasibility and impact of technical attacks** against the externally exposed targets of evaluation with the intent to gain access to resources and data. This activity will simulate attacks that could be performed from unauthenticated adversaries who can access the externally exposed targets of evaluation (i.e. external adversaries), and
- **Recommending appropriate actions** to manage the identified issues/weaknesses/vulnerabilities.

Timeline:

On average **5 man-days** are required to assess 10 static IP addresses that:

- will be owned by the client for the duration of the assessment, and
- will forward traffic to devices (physical or virtual) owned by the client.

Penetration Testing

Thick client penetration test

The main goals of this assessment are:

- **Identifying and assessing the feasibility and impact of technical attacks against the applications with the intent to gain access to resources and data** located on the device where the thick client application is executed and the back end systems the thick client applications interacts with. This will simulate attacks that could be performed from authenticated and unauthenticated adversaries who can interact with the thick client application, and
- **Recommending appropriate actions** to manage the identified issues/weaknesses/vulnerabilities.

Timeline:

On average **10 man-days** are required to assess one application. Please note that the time it takes to complete this assessment varies based on the complexity and the size of the application.

Build Review

The main goals of this assessment are:

- **Identifying security issues** related to the security configuration of the operating system running on physical or virtual device, and
- **Recommending appropriate actions** to manage the identified issues/weaknesses/vulnerabilities.

Timeline:

On average **one man-day** is required to perform a build review of one device (physical or virtual).

Penetration Testing

Vulnerability assessment of data in transit

The main goals of this assessment are:

- **Identifying whether data is transmitted over secure channels**
- **Recommending appropriate actions** to manage the identified issues/weaknesses/vulnerabilities.

Timeline:
This assessment is executed for the **duration agreed with the client**.

Perimeter vulnerability assessment

The main goals of this assessment are:

- **Identifying vulnerabilities** related to devices exposed to the Internet
- **Recommending appropriate actions** to manage the identified vulnerabilities.

Timeline:
On average **one man-day** is required to perform an assessment for up to 25 static IP addresses owned by the client for the duration of the assessment.

Please, note that:

- one month is required to complete the vulnerability assessment,
- the static IP addresses have to be owned by the client for the duration of the assessment, and
- the static IP addresses have to forward traffic to devices (physical or virtual) owned by the client for the duration of the assessment.

Phishing

Phishing simulations

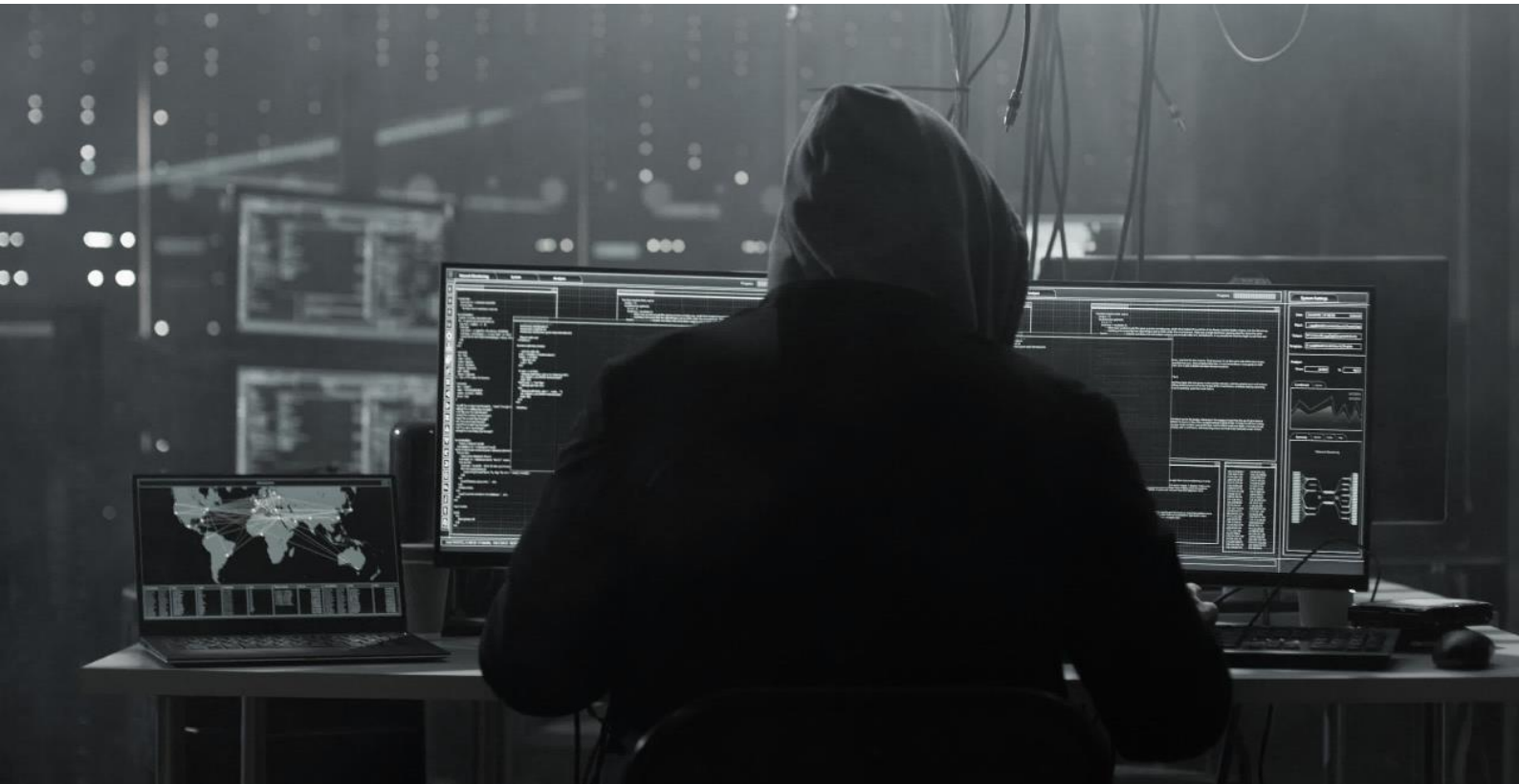
The main goals of this assessment are:

- **Identifying your employees' response** to phishing campaigns
- **Providing an awareness message** that can be modified to your policies and adapted to your organization to raise awareness among employees and inform how to react when they receive a phishing email.

Timeline:

On average **5 man-days** (spread across one or two months) are required to perform a mass phishing simulation assuming that:

- The client will provide a list (that include all people and their email addresses) that will be used to send phishing emails, and
- The mass phishing simulation aim is to test the people responses when they receive a phishing email not whether the phishing email can be successfully sent to the client team members (i.e. bypassing security solutions like MIMECAST is not an objective of this assessment).



Threat hunting

Threat hunting is a **human-led process that enriches your existing security procedures** with contextual insights gained from analyzing data sources.

✓ Enhance your threat hunting infrastructure

We can work with you to help you improve your threat hunting infrastructure to advance your logging and alerting capabilities.

✓ Improve your threat hunting evidence collection

We can work with you to help you improve your threat hunting process to advance your data analysis to gather intelligence about indicators of compromise.

✓ Hypothetical/theoretical threat hunting

We work with you to develop hypothetical threat hunting scenarios that can be used as a base for the data analysis and threat hunting.

Information Systems Internal Audit

Executive Summary

The institute of Internal Auditors (IIA) defines the mission of Internal Audit as **enhancing and protecting organizational value by providing risk-based and objective assurance, advice, and insight.**

We know that sometimes ensuring the capacity and adequate skills and proficiency in conducting IS audit and assurance assignments is hard.

We offer you **Elasticity.**

It is simply the convenience to **match the supply of resources to demand.** We know how to do it.

What are Information Systems Internal Audit Services?

Objective examination of evidence for the purpose of **providing an assessment on risk management, control or governance processes for the enterprise** (ITAF 3-rd Edition).

It could be in the form of a specific audit assignment, task or review activity, such as an audit, control self-assessment review, fraud examination or consultancy.

Information Systems Internal Audit

Models available to organizations for their internal audit function include:

1. **Outsourcing** - Execution of a full-scope, risk-focused internal audit plan outsourced to PwC. A designated in-house contact, who reports to the Audit Committee or the Board of Directors, acts as the liaison with PwC.
2. **Co-sourcing** - Adopts a similar overall approach as the full outsourcing model, but the execution of the audit plan is shared between PwC and the organization. Usually, we handle specialized areas or those that are more cost-effective to outsource. These areas include computer security auditing, special investigations, financial or operational auditing. This eliminates the need for the organization to recruit expertise that is difficult and sometimes relatively expensive to retain and maintain.
3. **Advisory Services -** Designing and building IT Audit Methodology; IT Audit Programs; Trainings.

Benefits:

- ✓ **Rich palette of professionals with diverse set of skills** and proficiency, knowledge and hands-on experience in wide-ranging technologies and processes
- ✓ **Stay agile and improve your responsiveness by** adapting quickly to challenges and opportunities brought by the emerging technologies
- ✓ **Reduce your exposure to evolving technology and cyber risks**, while delivering **cost efficiency**
- ✓ Pay-as-you-go lets you **adapt with ease to changing business needs** without overcommitting budgets or pay less by using more

Target Audience: Head/Seniors of IA Function

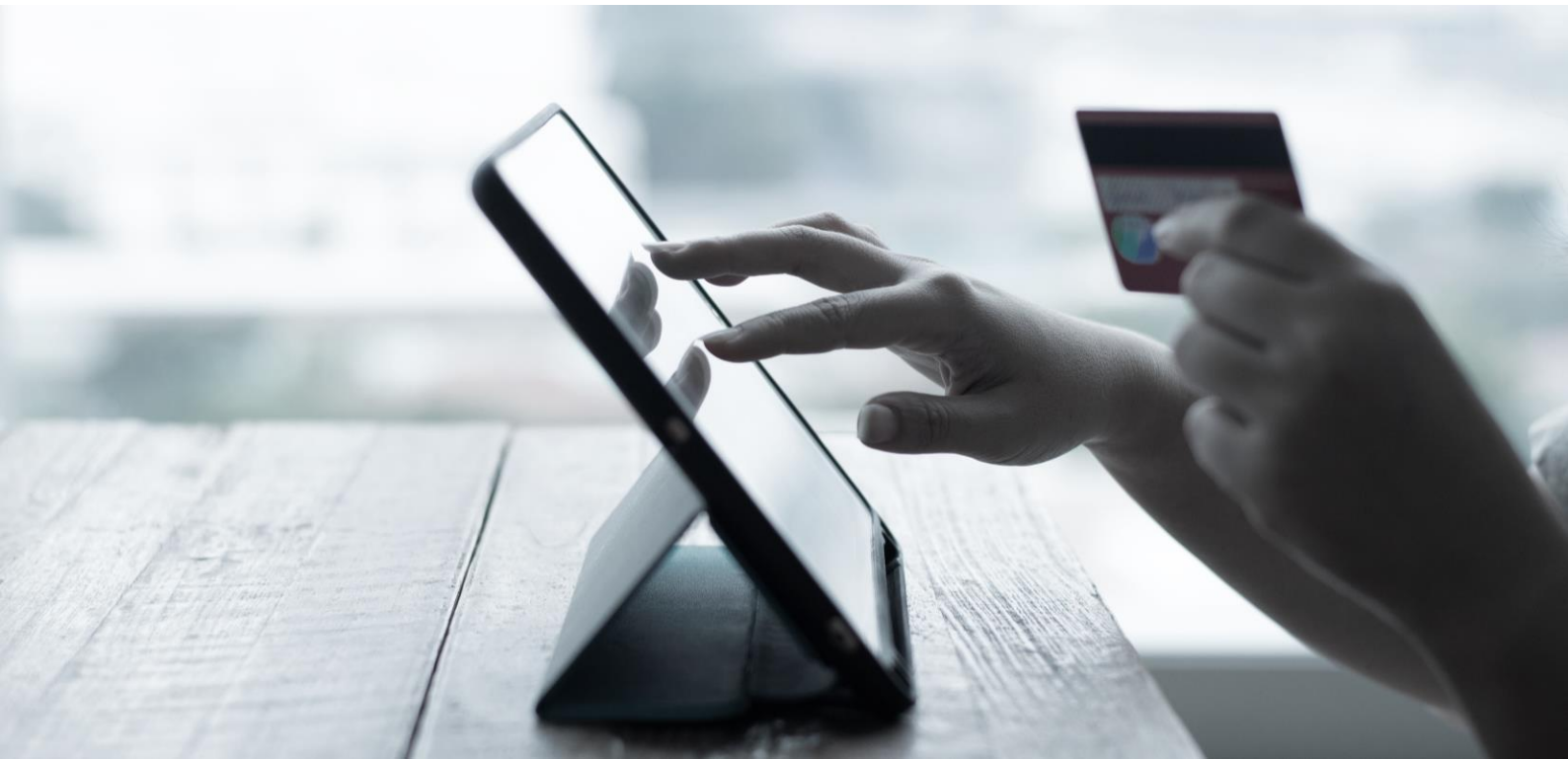
SWIFT Customer Security Program

Executive Summary

- Is SWIFT environment one of your crown jewels?
- Are you confident in your ability to keep it safe?

SWIFT payments community continues to suffer from a number of cyber-attacks and breaches, (some stemming from third parties). While all SWIFT customers remain primarily responsible for protecting their own environments, **SWIFT aims to support its community in the fight against cyber-attacks** and has identified 19 mandatory and 10 optional security controls for all its 11 000 customers worldwide.

All SWIFT users are required to undergo an "independent assessment" in support of their annual self-attestation of their compliance with the SWIFT Customer Security Control Framework.



SWIFT Customer Security Program

What are the SWIFT related services we deliver?

- **Swift Customer Security Program Audit**

At the time being SWIFT randomly selects customers who will be **required to provide additional assurance either from their internal or their external auditors.** If you are one of those selected entities, we could provide a validation of successful alignment of controls with the SWIFT Customer Security Program guidelines resulting in a control report under recognized standards (e.g. ISAE3000).

- **SWIFT Customer Security Program Assessment**

A **detailed evaluation of your local SWIFT control activities** against SWIFT Customer Security Control Framework and Guidelines supported by sufficient and appropriate evidence obtained during the assignment.

- **Technical Assessments of SWIFT environment**

A **detailed penetration testing of your local SWIFT environment**, including Operators PCs, Data Exchange Layer and SWIFT Secure Zone (software and network) components.

- **Embedded in Internal Audit**

Work alongside your internal audit function to report on SWIFT Customer Security Program controls.

SWIFT Customer Security Program

Benefits:

- ✓ You will improve your **confidence in security position of your SWIFT environment**
- ✓ Boost your **regulatory trustworthiness** and peace of mind
- ✓ You will get an **industry insight** that is relevant to your market segment, as well as a balanced view on how to prioritise any associated actions
- ✓ **Proven SWIFT Customer Security program** experience coated with technical experience and knowledge on the subject matter
- ✓ Service that **adapts to your requirements**

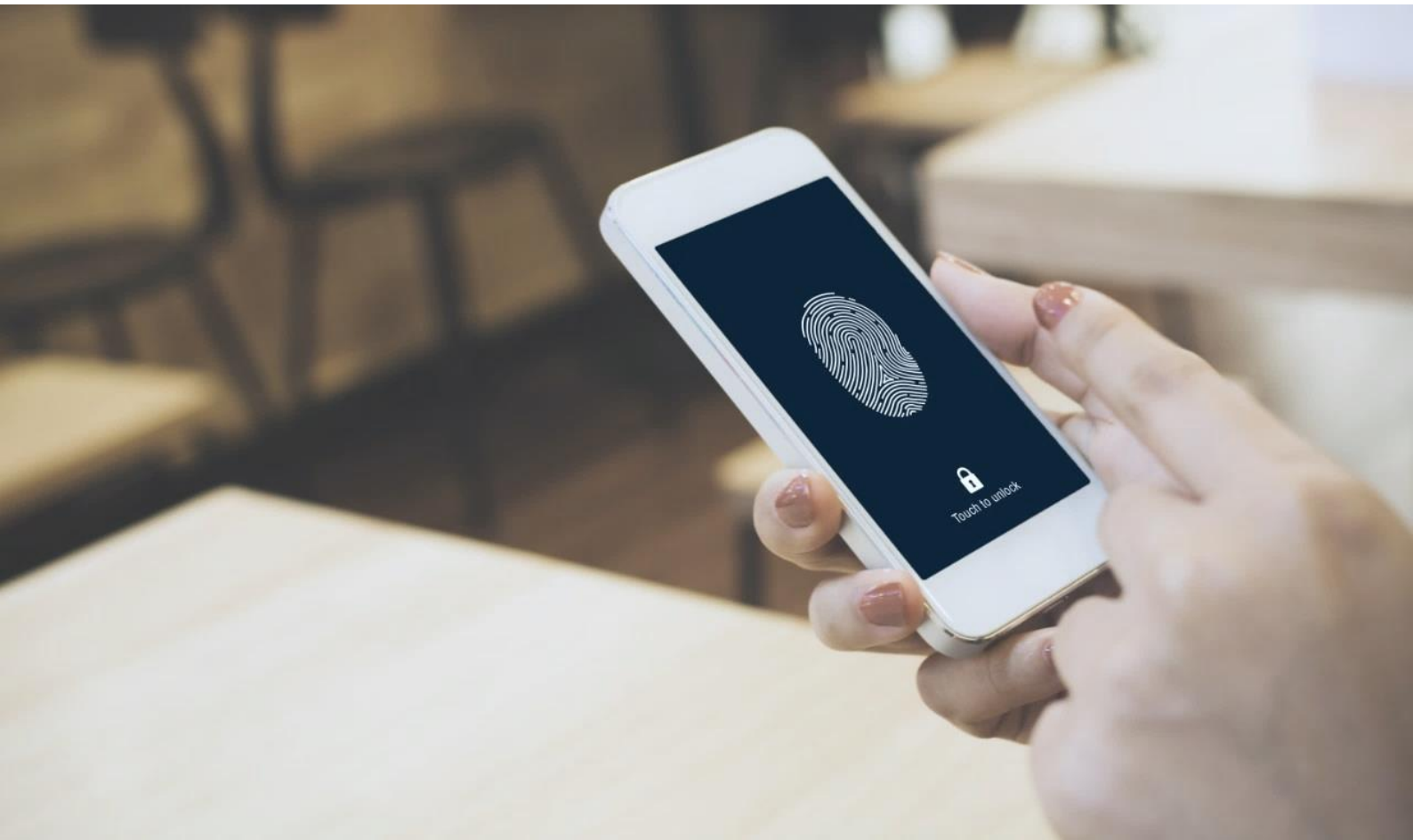
Target Audience: CTO/COO/CISO

Identity and Access Management

Identity and access management (IAM) is the (security) discipline that enables the **right individuals** access the **right resources** at the **right time**, in the **right way** for the **right reasons** and being able to report on that access. It comprises solutions involving people, process as well as technology.

The need to ensure **appropriate access** to resources across increasingly **complex technology environments** is paramount to ensuring a secure environment.

The need to **empower end-users** with control over their data in an intuitive and secure way, while **protecting their privacy** is one of the core challenges.



Identity and Access Management

Employee identity (IGA)

- Reduce time to service
- Increase cost efficiency
- Increase security
- Protect intellectual property
- Prevent fraud
- Protect brand
- Improve compliance posture

Privileged identity (PAM)

- Assure confidence in business practices
- Protect against insider threats
- Increase compliance
- Increase security
- Protect assets
- Reduce IT costs

Consumer identity (CIAM)

- Improve Omni-channel user experience
- Mass One-on-One marketing (BI)
- Real-time personalization
- Increase (GDPR) Compliance
- Digital customer services (AI)
- Increase time-to-market for digital initiatives

Identity of Things (IoT)

- Combining things with people
- Ensuring data integrity
- Enable interoperability
- Enable payment services
- Increase security

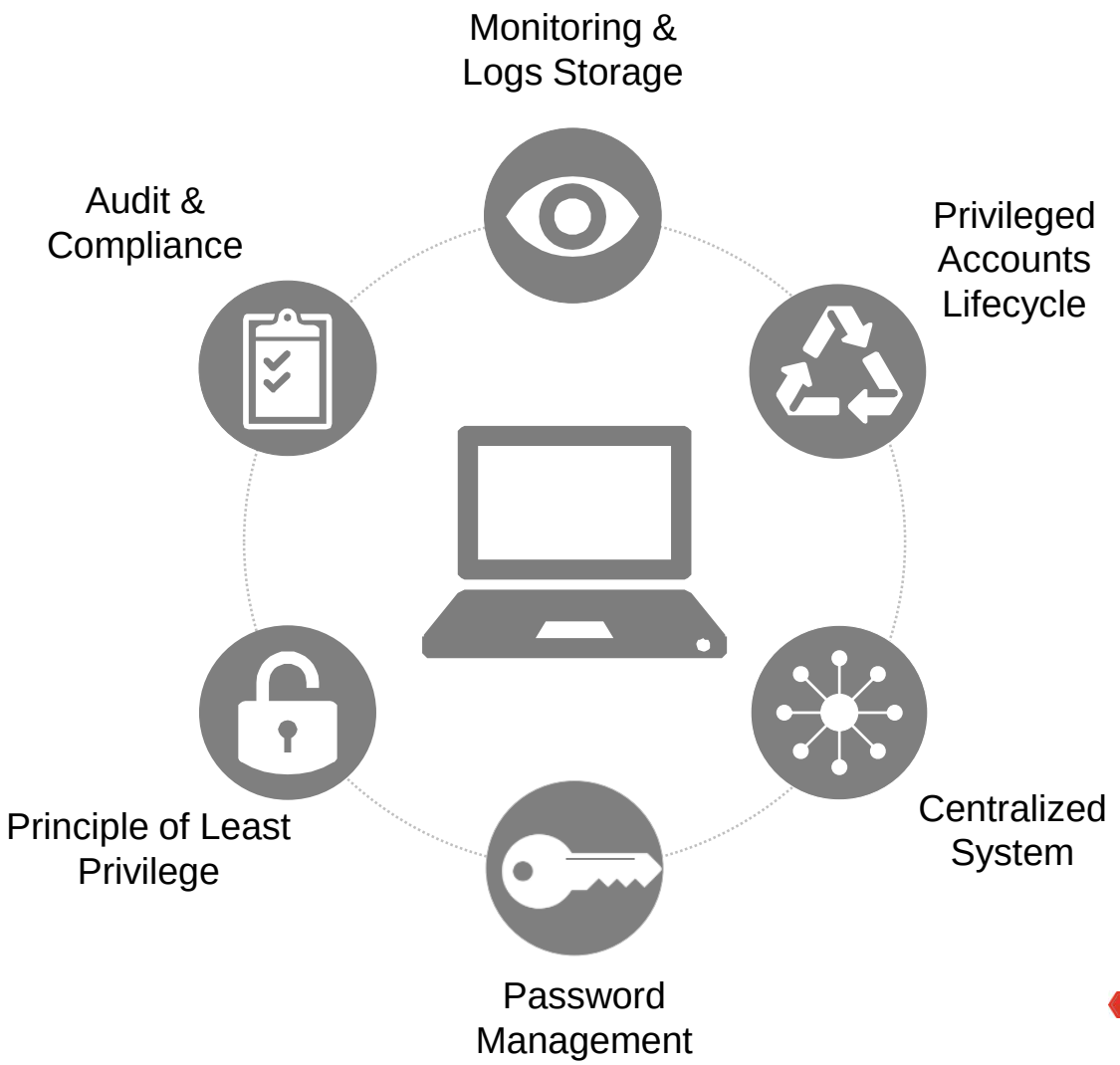
Identity and Access Management

Service type	Service areas	Key capabilities	
Strategy and planning	**Assessments**	• Capability assessment • Benchmarking	• Org structure, processes, and technology evaluation
	Strategy and roadmap	• Future state definition • Gap analysis	• Business case development • Economics and financial modeling
Governance	**PMO**	• Steering committee • Strategy and architecture • Risk and compliance management • Business change enablement	• Business case & stakeholder management • Balanced scorecard • Portfolio management • Benefits management
Design and Implementation	**Access management**	• (Biometric) Authentication • Authorization • 2FA and multi-factor • Web access management	• SSO • Policy management and enforcement • Privileged access management • Remote access
	Identity governance and administration	• Identity lifecycle management • Directory services • Entitlement administration	• Role and policy management • Access requests • Access fulfillment (provisioning) • Access certification
	Federated IAM	• Identity correlation • Identity synchronization • Identity provider (IdP)	• Identity as a Service (IDaaS) • Externalized authorization management (EAM)
	Identity analytics and intelligence	• Log aggregation • Reporting engine • Business metrics (KPIs) • Risk management	• Compliance proof • Process effectiveness • Decision support • Behavioral analytics
	Vendor identification	• Proof of concept	• Vendor analysis
	Technology management	• Design, build, test, and operate (cloud and on-premises)	• Technology enhancement
Operation	**Managed IAM**	• Level 1, 2 and / or 3 support	• Strategic operations (continuous improvement)

Privileged Access Management

What is Privileged Access Management?

Privileged Access Management (PAM) is the practice of **securely managing highly privileged account (HPA) access to sensitive information or functionality.** It deals with the management (creation, modification, and removal) of HPAs as well as enforcing, logging, monitoring, auditing, and certifying privileged access, and reporting violations.



Privileged Access Management

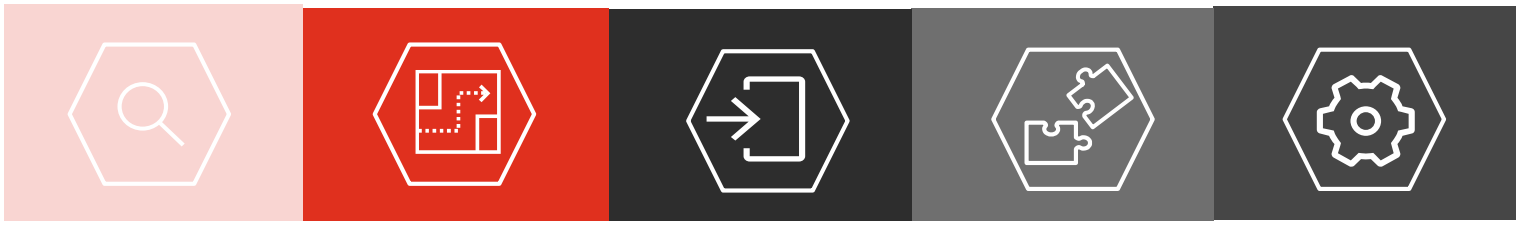
Benefits of a PAM Solution

- Mitigates risks and compliance costs – ensures passwords are regularly changed to **meet policies** and **strengthens password integrity** by providing new passwords at each access
- Can **improve IT efficiency** by ensuring appropriate users have access to the current passwords for required accounts
- Auditing can help **meet industry regulations** while **maintaining company policies** around highly privileged access accounts
- **Can integrate with additional security tools** such as SIEM, Identity & Access Management (IAM), 2FA, etc. to further enhance security of IT environments
- Preventative measure against internal / malicious internal attacks

Risks of Not Having a PAM Solution

- Passwords can be shared among multiple users via insecure methods, resulting in the possibility of **non-authorized users having access** to key privileged accounts
- Password policy **requirements are difficult to enforce** on end target systems
- **Lack of accountability** in tracking users of non-personal accounts and the privileges provided to an account
- Financial, reputational, brand value, customer confidence loss

Privileged Access Management



Current state and discovery	Strategy and roadmap	Implementation and upgrades	Expansion and integration	Security Managed Service Operations
1. Conduct an As-Is assessment 2. Assess vulnerabilities 3. Develop requirements and cases for using the PAM model 4. Develop an inventory process	1. Conduct a fit-gap analysis 2. Conduct vendor assessments 3. Define the future state 4. Conduct a target-state proof of concept or pilot	1. Support the greenfield implementation of a PAM solution or upgrade 2. Define the privileged account criteria 3. Execute testing and deployment	1. Integrate and extend infra, platform, apps, endpoints, multifactor, IAM, SIEM, ticketing and CMDB 2. Train staff 3. Implement an operating model	1. App maintenance, DR / failover services 2. Assess current process 3. Process Automation 4. Custom report generation

Deliverables

Assessment	Findings	Implementation	Integration	Managed Service
1. Requirements 2. Use cases 3. Vulnerability report 4. Capability matrix	1. Vendor scorecard and recommendations 2. Enterprise strategy 3. Implementation roadmap and improvements	1. Solution architecture 2. Test plan, scripts and results 3. Deployment plan 4. Live/deployed solution	1. Integration plan 2. Integration testing 3. Knowledge transfer 4. Implemented operating model	1. Privileges through PwC Managed Services 2. PwC runs and maintains your services, leaving you without the hassle

Proposed time frame

2 to 8 weeks	4 to 12 weeks	8 to 16 weeks (on average)	4 to 8 weeks (on average)	Flexible

Cloud Readiness Assessment

Executive Summary

With digitalization high on most organizations agendas, the number of requests for migration to cloud is growing significantly and continuously. To ensure a **smooth migration from legacy to cloud solutions, it's important to know the current level of maturity of your IT processes and applications and define your business needs and expectations** in terms of flexibility and efficiency. Relying on our cloud readiness assessment framework, our experts can help you determine the current level of maturity of your IT systems and applications and identify possible risks related to migration to cloud.

Benefits

- We will **facilitate the process of migration into the cloud by applying our standard methodology for performing cloud readiness assessment of IT systems and applications.** We will provide insights on which applications and IT services could be moved into the cloud by providing information on cloud readiness gaps in order to perform the migration. We will provide **transitional roadmap based on multi-criteria analysis and support defining an operational model** for applications by priority for transition and recommended timeframe for migration.
- We will help **you assess your security needs and determine risk acceptance level** of security in cloud and recommend solutions in line with your business goals.

Target Audience: CIO/CISO/COO/CFO/CRO

Cloud Provider Selection

Executive Summary

Today many companies would like to **use cloud-based solutions or move their existing services into cloud environment but are not sure how to select a cloud provider**. They usually want to ensure data and infrastructure security, managing access control, corresponding service level agreement, compliance with local regulations and relevant standards, and interoperability of cloud service. To fulfill all stated requirements you need to know local regulations referring to cloud services as well as international regulations and standards and best practices.

Starting the project, we will use **desk research and discussion with the client to collect and analyze the information related to the IT infrastructure** and business services that should be used in cloud. We will see into existing policies, procedures and regulations applied.

We will develop a proposal for the set of tools, such as questionnaires, that can be used during the process of selection of cloud provider. The tools / questionnaires will be aligned with your business needs and be compliant with your policies and procedures as well as local regulations.

Benefits

You will get your **own, tailor-made criterion for selection of cloud provider** that is compliant with local lows and bylaws, EU regulations, international standards and best practices.

Target Audience: CIO/CISO/CRO/CCO

Cloud Service Assessment

Executive Summary

Trust and transparency are the baseline and an important success factor for the sustainable usage of Cloud Computing – for both users and providers. It is a very rare practice for cloud users to be able to audit cloud providers. Common practice is that cloud users need to rely on a third party independent assessments that the cloud service provider meets their requirements for security, scalability, availability, and functionality. Purchasing and IT departments that want to outsource parts of their IT infrastructure and operations or business services are often not sure how to select the right cloud provider which can be trusted.

Cloud Service Assessment is a **process of determining a maturity level of the cloud service against set of rules concerning legal regulations, data protection and security, resource/application security, infrastructure and operations, and system interoperability**. Based on the results of the assessment, PwC issues a cloud service audit report that provides a better understanding of cloud provider's services and the effectiveness of the implemented security measures. These reports are an essential guarantee of reliability and trust, especially because they are issued by impartial and independent third party.

Cloud Service Assessment

Benefits

- ✓ **Referring to cloud users:** When planning to use cloud services, it is essential to focus on a selection process of cloud provider and understand the compliance-related aspects of the cloud service.
- ✓ With our extensive experience in IT-related control systems and cloud-specific risks, we **can help cloud users select the right cloud provider,** monitor cloud services they use as well as review and update existing cloud-enabled processes.
- ✓ **Referring to cloud providers**: We have extensive experience with cloud compliance projects and have a focus in the compliance criteria of CSA and BSI C5. In addition to this, we deliver projects regarding ISO 27001/ISO 27017/ISO 27018/ISO 27701 implementations for all sizes of cloud providers.
- ✓ We can help cloud providers **implement their cloud service in most secure way** to fulfil the cloud users' needs and expectations and build trusted relationships with them.

Target Audience: CIO/CISO/CPO – Chief Procurement Officer

Our Team of Experts

Mircea Bozga
Partner
Risk Assurance Services
PwC Romania
E: *mircea.bozga@pwc.com*

Mircea Bozga leads the Risk Assurance practice of PwC in South East Europe (SEE). With a background in engineering, Mircea joined PwC in 1997. He has coordinated IT Regulatory audits (Financial Services industry) as well as other engagements related to controls, third party assurance (SSAE 16 , ISAE3402), internal &external audits and other consulting engagements. Mircea is a Certified Information Security Auditor (CISA).

Ilian Stoianov
Director
Cyber Security Services
PwC Bulgaria
M: +359 895 558 319
E: *ilian.stoianov@pwc.com*

Ilian leads the cybersecurity practice in South East Europe (SEE). He is focused on Information Security audits, risk assessment and analysis of information systems, project management, cyber resilience, GDPR compliance. He has extensive international experience, working in Austria, Bulgaria, Czech Republic, Japan and UAE. Ilian holds the following certifications: CISA, CRMA, CIA, CIPM.

Uroš Žust
Director
Risk Assurance Services
PwC Slovenia
M: +386 30 661-001
E: *uros.zust@pwc.com*

Uroš is a seasoned professional with (ISC)² CISSP, CISA & CISM, PMI PMP and PRIS certifications and more than 15 years of experience leading teams, providing security, IT audit and cybersecurity governance services for organizations in various industries both in Europe and in the US.

Petko Petkov
Senior Manager
Cyber Security Services
PwC Bulgaria
M: +359 894 421 042
E: *petko.petkov@pwc.com*

Petko has more than 10 years of experience in the IT industry, in the last 5 years - in the role of architect and management for Identity, Access and Governance projects. His responsibility included leading discussions on IAM architecture, process and governance development, developing deployment and implementation methodologies, supervising and coordinating IAM deployments. Core certifications and competencies: Azure Solution Architect, MCSE – Server Infrastructure 2012, MCSE – Productivity Exchange 2016, MCTS – FIM 2010, Configuring, SailPoint IdentityIQ Engineer; CyberArk Sentry, etc.

Our Team of Experts

Adel Abusara
Manager
Cyber Security Policies
PwC Serbia
M: +381 64 857 4005
E: *adel.abusara@pwc.com*

Adel has more than 10 years of experience in Cybersecurity Governance and Security Sector Reform. He performed various roles in international organizations, NGOs, working with relevant security and cybersecurity Public Sector institutions. As a Cybersecurity Policies Manager in PwC he is handling the cybersecurity governance portfolio of PwC in South East Europe (SEE). Adel holds ISO/IEC 27001 Lead Auditor Certificate.

Iliyan Velikov
Manager
Cyber Security Services
PwC Bulgaria
M: +359 895 558 319
E: *iliyan.velikov@pwc.com*

Iliyan is recognized professional with (ISC)² CCSP, OSCP, GIAC GXPN, GIAC GMOB, GIAC GDAT and CRTP certifications who has 8+ years of experience leading teams to provide penetration testing services for organizations in various industries including financial services, telecommunications and public sector.

Ivana Tepcevic
Manager
Risk Assurance Services
PwC Serbia
M: +381 62 8833431
E: *ivana.tepcevic@pwc.com*

Ivana has 18-year experience in consulting and auditing information security management systems and cloud service providers as well as managing projects in various industries. She holds ISO/IEC 27001 Lead Auditor Certificate, ISO 27018 protection of PII in public clouds acting as PII processors Certificate, ISO 27017-2015 IS controls for cloud services certificate and ECSA-AA Accredited Auditor for Cloud services.

Petko Petkov
Manager
Cyber Security Services
PwC Bulgaria
M: +359 89 305 8584
E: *petko.x.petkov@pwc.com*

Petko has 10 years of experience across both financial services and commercial sectors. Petko holds the following certificates: CISSP, CISA, ISO/IEC 27001 Lead Auditor. He specializes in: information systems security audits and assessments; secure configuration baseline and hardening; information security governance, risk management and compliance; protection of information assets.

www.pwc.bg