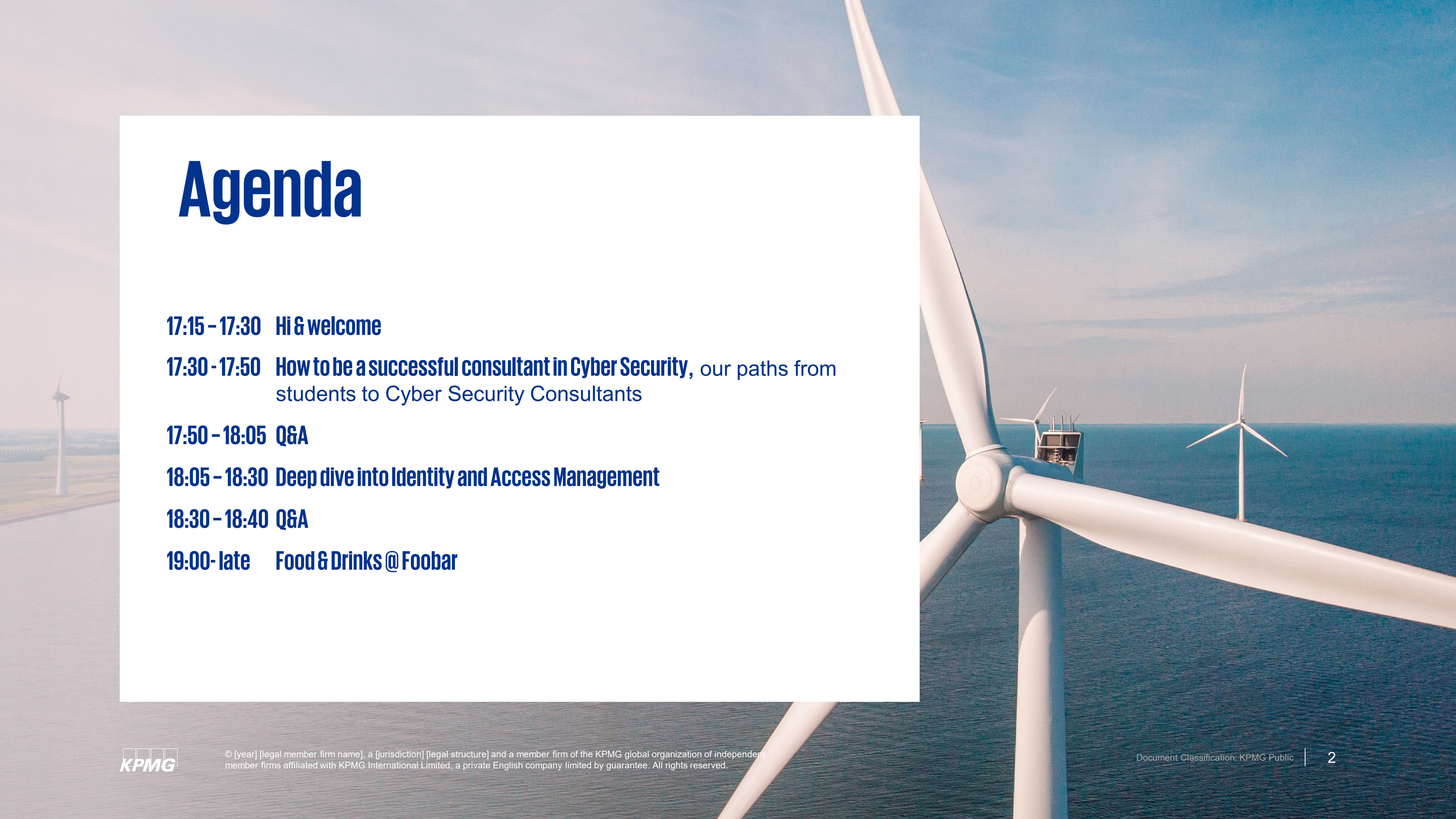
KPMG

Management Consulting Cyber Security

September 28, 2022



Agenda

17:15 – 17:30	**Hi & welcome**
17:30 - 17:50	**How to be a successful consultant in Cyber Security**, our paths from students to Cyber Security Consultants
17:50 – 18:05	**Q&A**
18:05 – 18:30	**Deep dive into Identity and Access Management**
18:30 – 18:40	**Q&A**
19:00- late	**Food & Drinks @ Foobar**

Who are we?

Carl Flodin - Associate

- Bachelor of Information Systems from Uppsala University
- Master of Information Security from Stockholm University
- Studied Computer Science at the University of Texas at Austin
- First year as Cyber Security Consultant at KPMG

Lukas Grönquist - Manager

- + 5 years within Cyber Security Consultancy
- Bachelor of Computer and System Sciences at Stockholm University
- Certified ISO 27001 Lead Implementer by PECB
- Board member for the Swedish Chapter of Cloud Security Alliance (CSA)

Sebastian Lennartsson - Associate

- Background within Software, PC hardware and Server Security @ Microsoft & HP
- BSc Business and Economics from Lund University
- First year as Cyber Security Consultant at KPMG

Cecilia Olin - Senior Associate

- Background within Information Security, Human Resources and Business Development
- Bachelor of Personnel, Work & Organization and Master of Information Security from Stockholm University
- Certified ISO 27001 Implementer by PECB
- Board member in SIG Security

01

KPMG

This is why we are here:

- Inspire
- Confidence.
- Empower Change.

This is our Purpose.

This is what we believe in

- **Integrity** | we do what is right
- **Excellence** | we never stop learning and improving
- **Courage** | we think and act boldly
- **Together** | we respect each other and draw strength from our differences
- **For Better** | we do what matters

These are our Values.

This is what we want to be

The Clear Choice:

- Our people are extraordinary
- Our clients see a difference in us
- The public trusts us

This is our Vision

This is how we want the world to see us

With passion and purpose, we work shoulder-to- shoulder with you, integrating innovative approaches and deep expertise to deliver real results.

Our Employer value proposition

Together we're changing the world

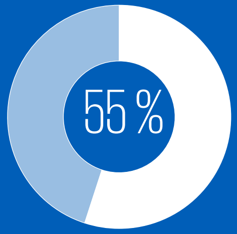
- Develop through challenging assignments
- Work with engaging colleagues
- Make a difference to companies and communities

This is KPMG

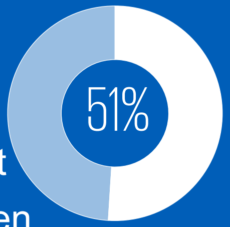
219 000 colleagues in 147 countries

Management

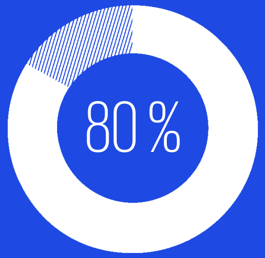
107 partners. Helena Arvidsson Älgne, Chairman of the Board & Patrik Anderbro Chief Executive Officer



women vs 45% men in the management board



49% men vs women works at KPMG in Sweden



of the largest companies in Sweden are KPMG clients

National and international companies,
Small and mid-sized owner-led companies,
Public sector, Non-profit organizations

Digital agenda

- Lighthouse
- Nordic Customer and Insights Center
- Sponsors AI-research

Inclusion & diversity

Internal team, leadership program, introduction e-learning, partner goals, ambassadors engaged through the whole organization

Proven successful

- National Tax Firm of the Year
- Top rated among Nordic consulting companies
- World leader in AI

- Womens Corporate directors
- Female digital engineer program
- Young entrepreneurs
- Jobbsprånget
- Climate investment in india

Career Journey

Associate

- Exciting, varied engagements
- Learning the job
- Training courses

Senior Associate

- More responsibilities in engagements
- More training, experience and development
- Coaching and feedback

Manager

- Leading engagements
- More client responsibilities, building relationships and discussing business opportunities
- Project Management
- Developing expertise in your area
- Developing leadership skills, client relationships and a thorough understanding of the business

Senior Manager

- You have client responsibility
- You are developing new client relationships and gain new business
- You are a leader, a role model with high expectations on leadership, coaching and to lead by example in all situations

Director

- You have responsibility for multiple major clients
- You have client teams and responsibility for budget
- You are a leader and a role model, and may be responsible for a market or sector

Partner

- You are a shareholder in KPMG and a leader and role model with responsibilities for KPMG in all situations – in the office, among co-workers, at the clients, and in social situations - both at work and outside of work.

Cyber Security

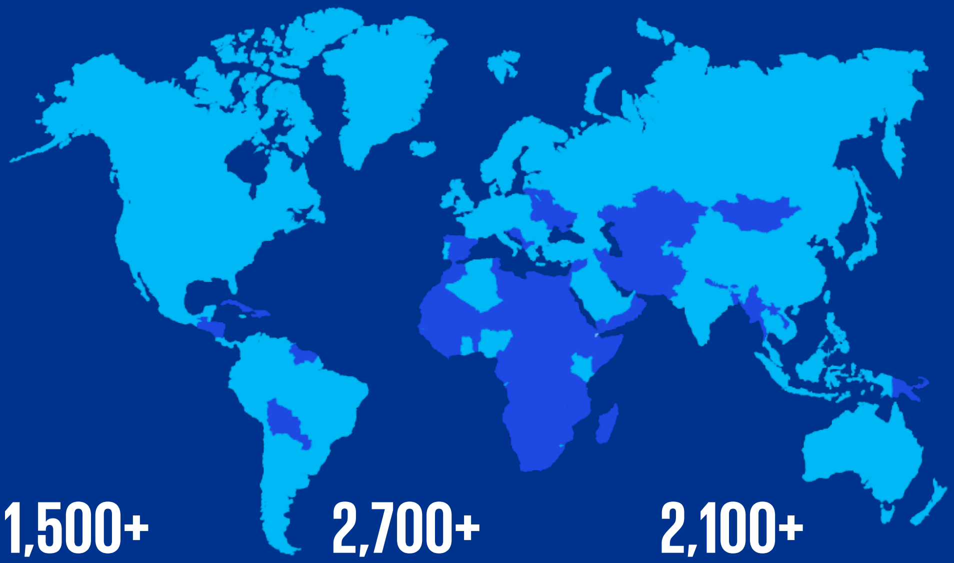
What your friends think you will do

What you actually will do

02

What does a Cyber Security Consultant do?

Our cyber security global delivery capability



1,500+ Americas

2,700+ EMEA

2,100+ Asia Pacific

Our global footprint:

Over 6,300 global cyber security professionals are supported by **over 45,000** risk-based consultants with a variety of backgrounds — including digital transformation, IT, regulatory and forensics.

Key markets and hubs include:

Americas:	US, Canada, Mexico, Brazil, Argentina
EMEA:	Sweden, Norway, Denmark UK, Germany, Netherlands, France, Spain, Italy, Switzerland, Finland, Austria, Ireland, Nigeria, South Africa, Kenya, MESA
ASPAC:	China, India, Australia, Singapore, Japan, Malaysia, New Zealand

Global cyber delivery centers: India, Belfast, Sofia, Malta and *Mexico (under development)*

We aim to deliver more efficiently for our clients through the use of skilled resources, powered assets, different delivery models and a range of tools and accelerator. Our teams across the globe operate as a global cyber practice so that our client receive a consistency of service.

Key investments and focus areas

- Managed detection and response
- Cloud security
- SecOps
- Risk quantification
- Digital identity and zero trust
- Third party security
- AI/ML/advanced analytics
- IOT/OT security

KPMG

Working as a Cyber Security Consultant

What we talk about

What we dont talk about

What we do – from strategies to technical implementations

Strategy & Governance

- Information security strategy / Governance
- Third party security risk management
- Security GRC
- Cyber maturity / Compliance assessments
- Cyber Assurance / IT Attestation
- Business resilience
- Security Awareness

Transformation

- Identity & access management
- Target operating model development
- Security architecture & analytics
- Information management & Privacy protection
- Security program delivery
- Enterprise architecture

Cyber Defense

- Technical assessments
- Security testing
- Application security
- DevSecOps
- Security operations & monitoring
- Threat Intelligence / Analysis
- Next-generation soc
- Cyber Managed Services

Cyber Response

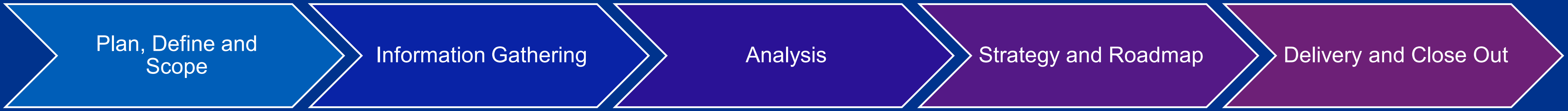
- Compromise assessment and simulations
- Incident response
- Digital investigations and remediation
- Red teaming
- Social engineering

Industrial control systems and OT security

Internet of things security

Cloud security audit & advisory

Planning and Executing a Project



Plan, Define and Scope

Information Gathering

Analysis

Strategy and Roadmap

Delivery and Close Out

Key Activities:

- Client kick-off meeting
- Understand the scope of work
- Define the timelines

Key Outcomes and Deliverables:

- Status update template
- Stakeholder map
- Project and engagement plan

Key Activities:

- Engage the business leaders, develop the understanding of risk, understand what sort of security capability is desired

Key Outcomes and Deliverables:

- High level view of key assets, risks and threats to crown jewels,
- Validation of current state controls through review and inspection of evidence

Key Activities:

- Assess current capability to understand current risk exposure
- Perform gap analysis (people, process and technology)

Key Outcomes and Deliverables:

- Threat Landscape
- Inherent and net risk exposure
- Risk Register with risks classified and prioritized

Key Activities:

- Propose options to manage risk to within tolerance, and offer roadmap from current to desired states.

Key Outcomes and Deliverables:

- Target State with roadmap that outlines activities over the 2 – 3 year timeline
- Strategy Improvements
- Executable project charters for improvement areas
- Board Presentation

Key Activities:

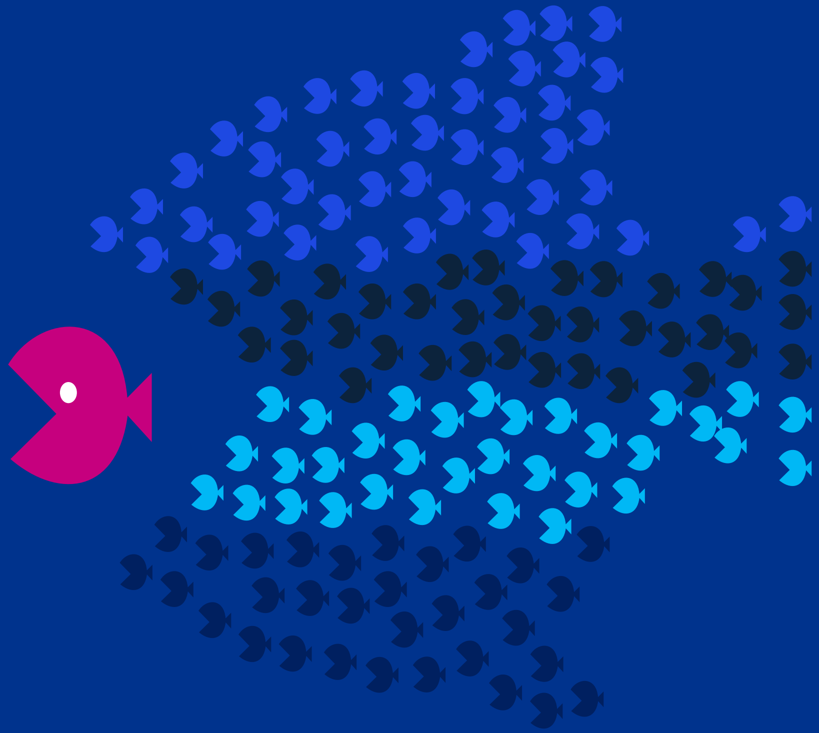
- Draft the report
- Deliver the report to the client

Key Outcomes and Deliverables:

- Board meetings and presentations

KPMG

Diverse clients requires diverse backgrounds and skillsets



International retailer - GDPR Implementation

13 consultants.
Backgrounds such as economy, system sciences, law, political science, HR–specialists.

Client - IAM Transformation Program

25+ consultants from several countries.
Backgrounds such as architects, developers, change management, compliance, risk management, IAM SME’s, project leaders, communicators, IT Operations etc.

One of Sweden’s Major Banks - Change management & SoD

4 consultants.
Review and development of segregation of duties within the change management process.

International telecom provider - ISMS

3 consultants.
Revamp of the global ISMS by implementing a information security baseline for the full organization.

Computer and Videogame developer - GITC Assessment & Continuity planning

3 consultants.
A assessment based on a framework of 17 general IT controls, applied to more than 90 systems.
Continuity planning to ensure backup procedures if, or when disruption hit critical processes

Benefits of consulting within Cyber

- Get to know organizations and industries in different sizes
- Experience different approaches and ways of working with cyber security – and identify success factors
- High variety in assignments will result in a broad knowledge
- Networking, both at the client and internally within the firm
- Several SME’s (Subject Matter Expert) within different fields at the firm. From Change Management to AI

Feel like KPMG Cyber is something for you?

- We are currently looking for Junior Cyber/Information Security Consultants –scan QR code below or see LinkedIn ad
- https://www.linkedin.com/jobs/view/junior-information-cyber-security-consultant-at-kpmg-sweden-3283749105/?originalSubdomain=se
- Interested in internships/master’s thesis? Email cecilia.olin@kpmg.se

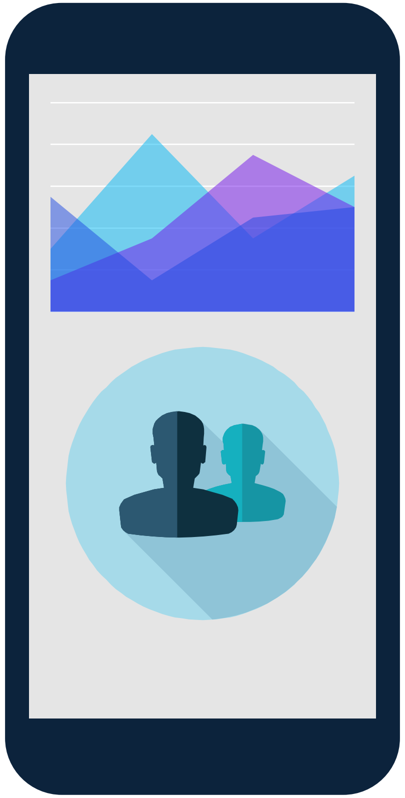
When you applied for the job
When you hear back from the recruiter

03

Identity and Access Management

- A deep dive into Identity and Access Management

What is an Identity?



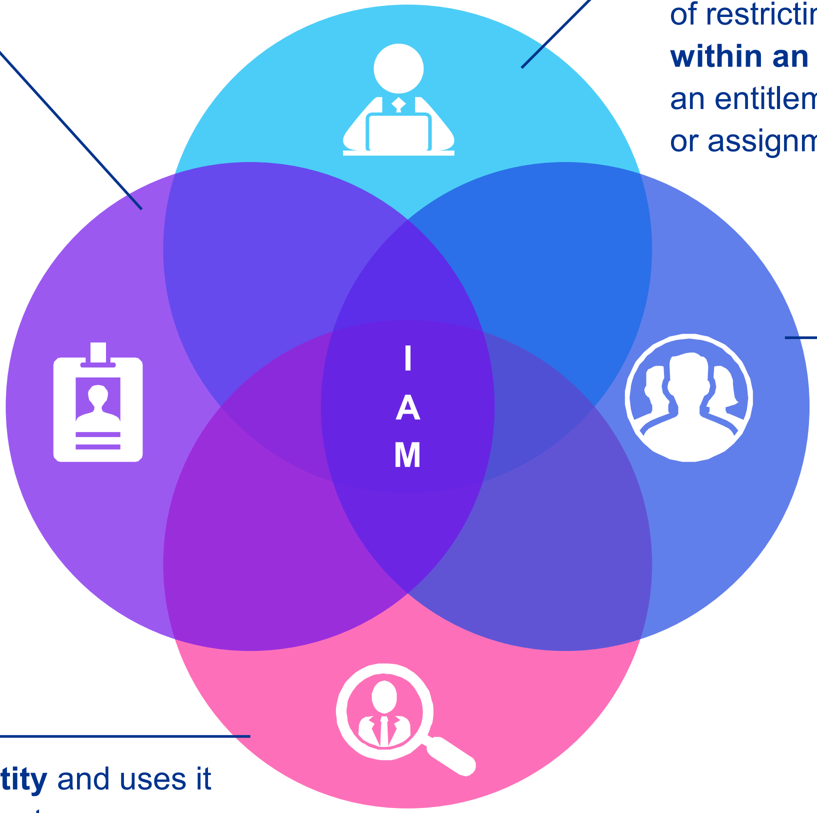
Identity

The digital representation of a **user**, comprising uniquely identifying attributes such as first name, last name, employee ID and email address, in addition to information that may describe their business function and relationship with an organization.

In most cases, a user should only have a single identity within each organizational domain, although there may be exceptions to this rule when a user requires the ability to access systems using different "personas" (e.g., an employee of a company who may also be a customer). Identities and personas are linked to accounts that enable users to access individual information systems and applications.

Entitlement

An account-level attribute that is used for the purpose of restricting the **user's capabilities or privileges within an information system**. Common examples of an entitlement include membership of a directory group or assignment of an application-level role



Account

A system-specific representation of an **identity**. Captures a user's authority to interact with a specific information systems or application.

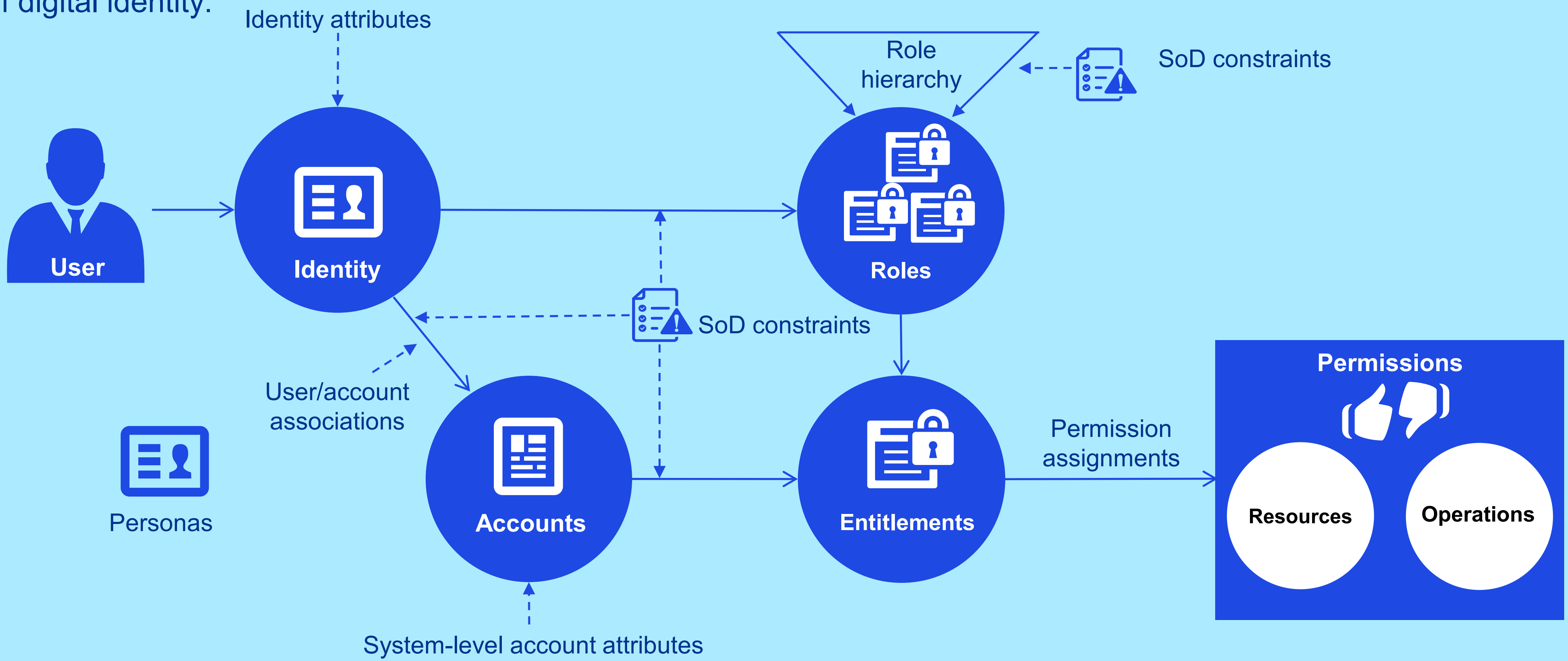
An account may contain attributes that are specific to the system or application. An attribute that describes the user's permitted capabilities or privileges is known as an entitlement.

User

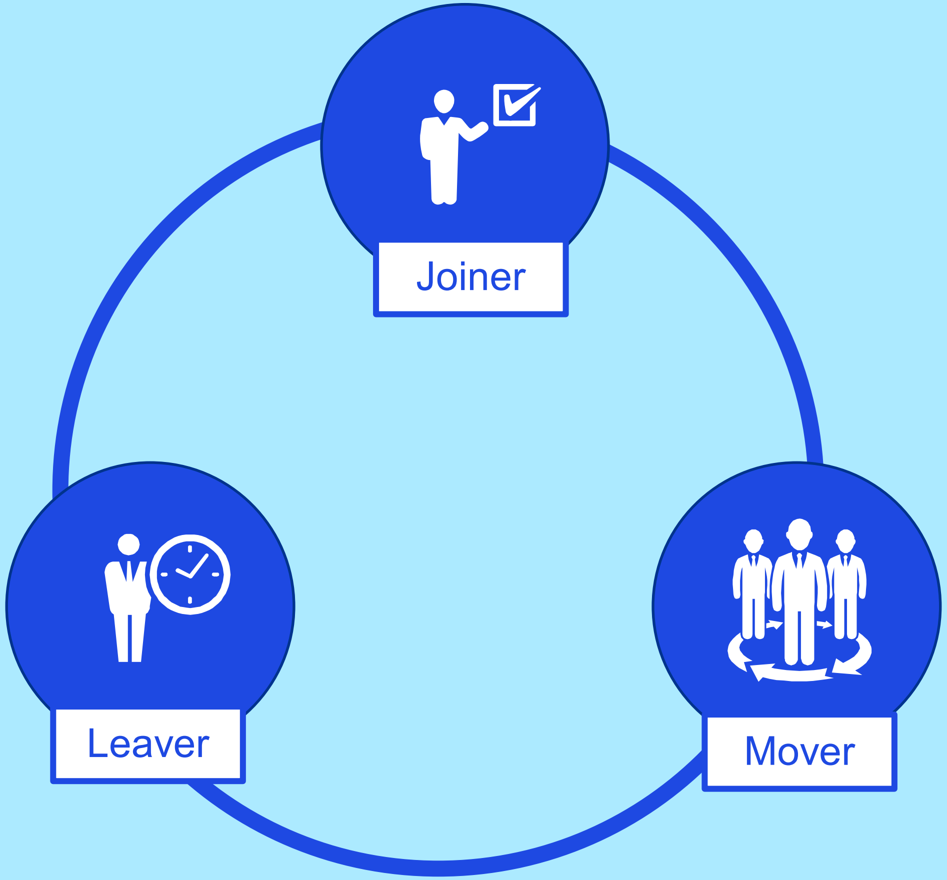
A person who owns an **Identity** and uses it to interact with information systems

Concepts – What is an Identity?

The following diagram illustrates the major entities and associations that constitute a model for describing the concept of digital identity:



Identity Management - User Lifecycle Management



Joiner

The process of creating a digital identity when onboarding a person such as a new employee

Mover

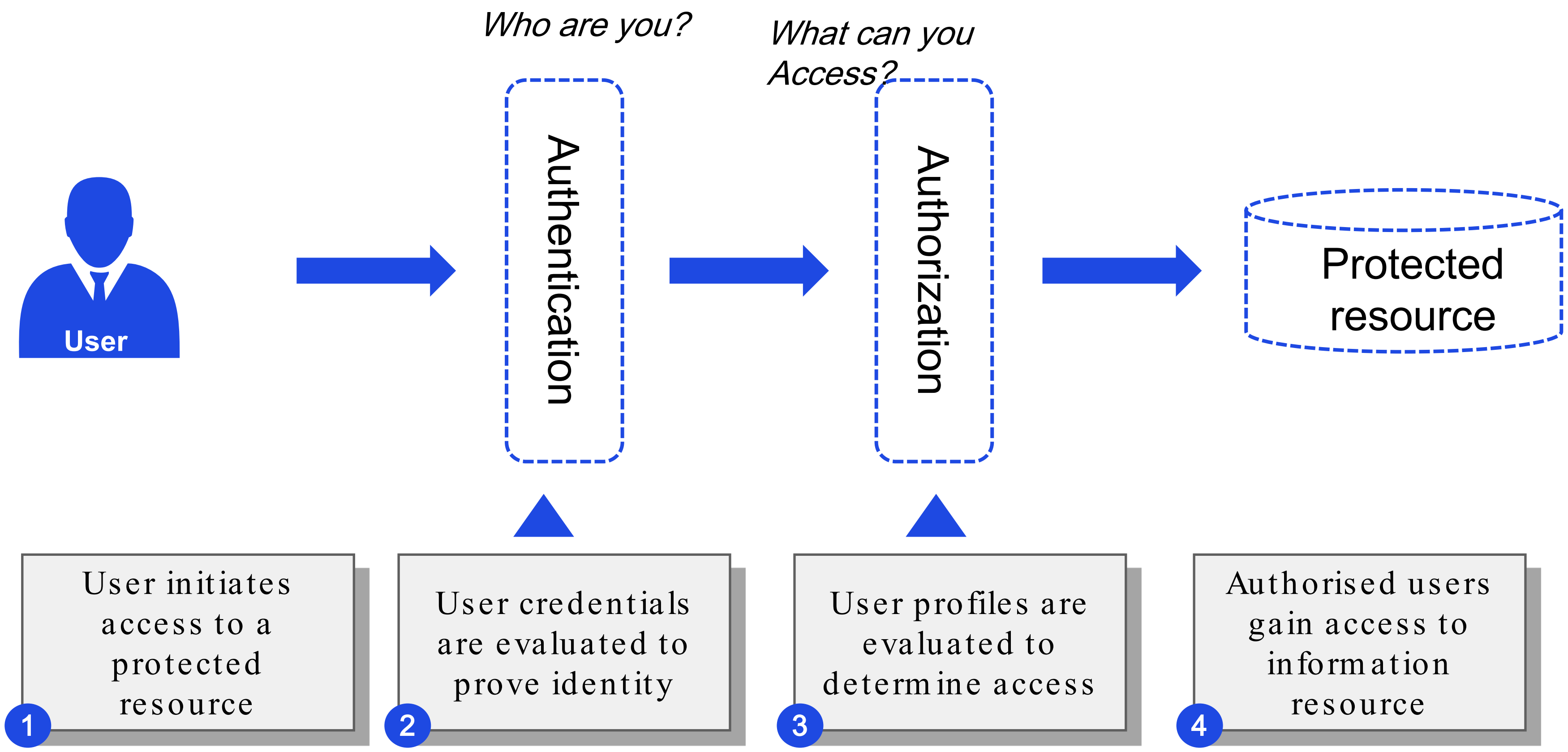
The process of changing an digital identity for example when the employee changes role, department or country

Leaver

The process of retiring an digital identity for example when the employee leaves the company

User Access Management

An Access Management solution provides Authentication and authorization services for controlling user access to protected information resources.



Who are you?

What can you Access?

User

Authentication

Authorization

Protected resource

1 User initiates access to a protected resource

2 User credentials are evaluated to prove identity

3 User profiles are evaluated to determine access

4 Authorised users gain access to information resource

Key Access Management Concepts

Authentication - Proof of who you are

Examples:

- Photo ID Card
- Biometric Data (fingerprint, facial recognition)
- Username/Password
- PIN

Real World Example:

- Want to collect a package at a postal service center, providing proof via driver's license proves that you are the person the package is made out to.

Authorization - What you can (or cannot) do

Examples:

- Learners Permit allows the owner to drive during certain hours
- First class airfare ticket allows passenger access to VIP lounge at the airport
- Hospital Guest Badge allows the visitor to see their own family member and visit the cafeteria but it prevents access to other patient and/or clinical rooms

Real World Example:

- A valid Driver's License/Photo ID (Authentication) doesn't mean you're allowed into the bar to drink alcohol. If you're not of age, it doesn't matter how valid the ID is.

KPMG

04

KPMG's IAM Framework

Identity and Access Management

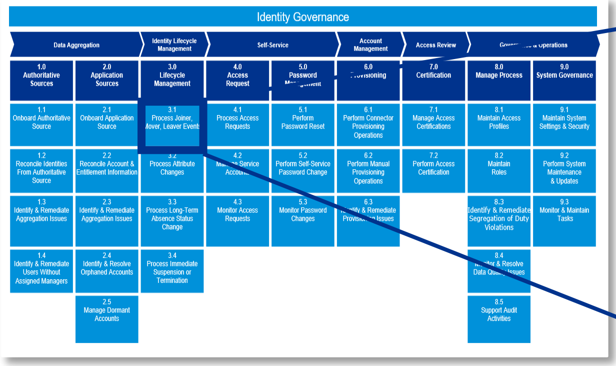
Target Operating Model

Functional Processes	People	Service Delivery Model	Technology	Performance Insights & Data	Governance
Process Taxonomy	Global Process Owners Overlay	Service Delivery Model Overlay	Supporting Technology Overlay	KPIs Linked to Benchmarks	Security & Controls
Maturity Models	Position to Role Mapping and Sizing by Function	Service Management Framework (Internal)	Application Architecture, Data Flow Diagram & Integrations List	Reporting Packages & Dashboards	Policies
Role Based Process Flows	Functional Position Job Profiles		Environment Architecture	MDM Design & Governance (NA)	
Leading Practices and Design Considerations					

Tech Agnostic ■	Platform specific ■

TOM Assets Overview

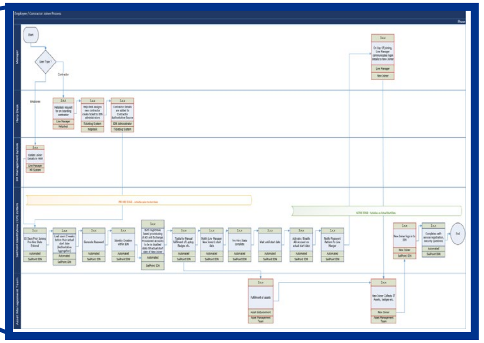
Process Taxonomy


Identity Governance
Data Aggregation
Identity Lifecycle Management
Self-Service
Account Management
Access Review
Governance & Operations
1.0 Authoritative Sources
2.0 Application Sources
3.0 Lifecycle Management
4.0 Access Request
5.0 Password Management
6.0 Provisioning
7.0 Certification
8.0 Manage Process
9.0 System Governance
1.1 Onboard Authoritative Source
2.1 Onboard Application Source
3.1 Process Joiner, Mover, Leaver Events
4.1 Process Access Requests
5.1 Perform Password Reset
6.1 Perform Connector Provisioning Operations
7.1 Manage Access Certifications
8.1 Maintain Access Profiles
9.1 Maintain System Settings & Security
1.2 Reconcile Identities From Authoritative Source
2.2 Reconcile Account & Entitlement Information
3.2 Process Attribute Changes
4.2 Manage Service Accounts
5.2 Perform Self-Service Password Change
6.2 Perform Manual Provisioning Operations
7.2 Perform Access Certification
8.2 Maintain Roles
9.2 Perform System Maintenance & Updates
1.3 Identify & Remediate Aggregation Issues
2.3 Identify & Remediate Aggregation Issues
3.3 Process Long-Term Absence Status Change
4.3 Monitor Access Requests
5.3 Monitor Password Changes
6.3 Identify & Remediate Provisioning Issues
8.3 Identify & Remediate Segregation of Duty Violations
9.3 Monitor & Maintain Tasks
1.4 Identify & Remediate Users Without Assigned Managers
2.4 Identify & Resolve Orphaned Accounts
3.4 Process Immediate Suspension or Termination
8.4 Monitor & Resolve Data Quality Issues
2.5 Manage Dormant Accounts
8.5 Support Audit Activities

End-to-end process taxonomy that depicts key processes of the end-to-end business process.

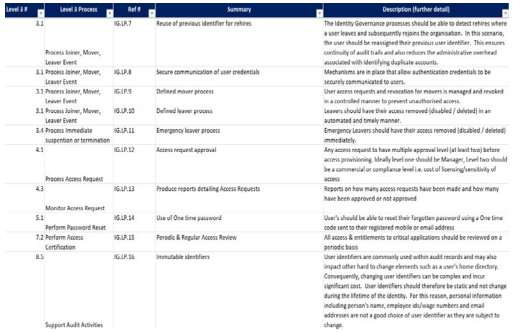
Role Based Process Flows

Joiner Process



Detailed role-based process flows that define the key roles, systems, activities, decisions and outputs for a given process

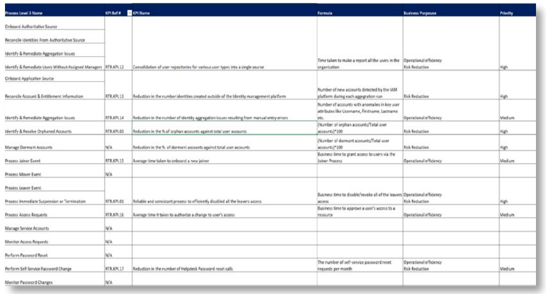
Leading Practices



Level 3 #	Level 3 Process	Ref #	Summary	Description (further detail)
3.1	Process Joiner, Mover, Leaver Event	IG.LP.7	Reuse of previous identifier for rehires	The Identity Governance processes should be able to detect rehires where a user leaves and subsequently rejoins the organisation. In this scenario, the user should be reassigned their previous user identifier. This ensures continuity of audit trails and also reduces the administrative overhead associated with identifying duplicate accounts.
3.1	Process Joiner, Mover, Leaver Event	IG.LP.8	Secure communication of user credentials	Mechanisms are in place that allow authentication credentials to be securely communicated to users.
3.1	Process Joiner, Mover, Leaver Event	IG.LP.9	Defined mover process	User access requests and revocation for movers is managed and revoked in a controlled manner to prevent unauthorised access.
3.1	Process Joiner, Mover, Leaver Event	IG.LP.10	Defined leaver process	Leavers should have their access removed (disabled / deleted) in an automated and timely manner.
3.4	Process Immediate suspention or termination	IG.LP.11	Emergency leaver process	Emergency Leavers should have their access removed (disabled / deleted) immediately.
4.1	Process Access Request	IG.LP.12	Access request approval	Any access request to have multiple approval level (at least two) before access provisioning. Ideally level one should be Manager, Level two should be a commercial or compliance level i.e. cost of licensing/sensitivity of access
4.3	Monitor Access Request	IG.LP.13	Produce reports detailing Access Requests	Reports on how many access requests have been made and how many have been approved or not approved
5.1	Perform Password Reset	IG.LP.14	Use of One time password	User's should be able to reset their forgotten password using a One time code sent to their registered mobile or email address
7.2	Perform Access Certification	IG.LP.15	Perodic & Regular Access Review	All access & entitlements to critical applications should be reviewed on a periodic basis
8.5	Support Audit Activities	IG.LP.16	Immutable identifiers	User identifiers are commonly used within audit records and may also impact other hard to change elements such as a user's home directory. Consequently, changing user identifiers can be complex and incur significant cost. User identifiers should therefore be static and not change during the lifetime of the identity. For this reason, personal information including person's name, employee ids/wage numbers and email addresses are not a good choice of user identifier as they are subject to change.

Provide a specific point of view on how something should be designed and have a benefit that can be realized.

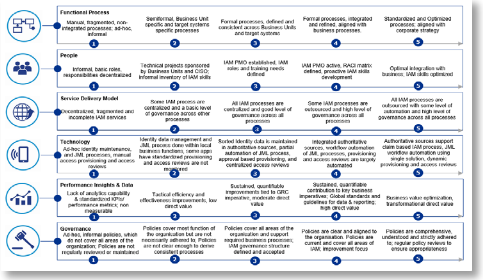
KPIs



Process Level 3 Name	KPI Ref #	KPI Name	Formula	Business Purpouse	Priority
Onboard Authoritative Source Reconcile Identities From Authoritative Source Identify & Remediate Aggregation Issues Identify & Remediate Users Without Assigned Managers	RTR.KPI.12	Consolidation of user repositories for various user types into a single source	Time taken to make a report all the users in the organization	Operational efficiency Risk Reduction	High
Onboard Application Source Reconcile Account & Entitlement Information	RTR.KPI.13	Reduction in the number identities created outside of the Identity management platform	Number of new accounts detected by the IAM platform during each aggregation run	Risk Reduction	High
Identify & Remediate Aggregation Issues	RTR.KPI.14	Reduction in the number of identity aggregation issues resulting from manual entry errors	Number of accounts with anomalies in key user attributes like Username, Firstname, Lastname etc.	Operational efficiency	Medium
Identify & Resolve Orphaned Accounts	RTR.KPI.03	Reduction in the % of orphan accounts against total user accounts	(Number of orphan accounts/Total user accounts)*100	Risk Reduction	High
Manage Dormant Accounts	N/A	Reduction in the % of dormant accounts against total user accounts	(Number of dormant accounts/Total user accounts)*100	Risk Reduction	High
Process Joiner Event	RTR.KPI.15	Average time taken to onboard a new joiner	Business time to grant access to users via the Joiner Process	Operational efficiency	Medium
Process Mover Event	N/A				
Process Leaver Event Process Immediate Suspension or Termination	RTR.KPI.01	Reliable and consistant process to efficiently disabled all the leavers access	Business time to disable/revoke all of the leavers access	Operational efficiency Risk Reduction	High
Process Access Requests	RTR.KPI.16	Average time it takes to authorize a change to user's access	Business time to approve a user's access to a resource	Operational efficiency	Medium
Manage Service Accounts	N/A				
Monitor Access Requests	N/A				
Perform Password Reset	N/A				
Perform Self-Service Password Change	RTR.KPI.17	Reduction in the number of Helpdesk Password reset calls	The number of self-service password reset requests per month	Operational efficiency Risk Reduction	Medium
Monitor Password Changes	N/A				

Robust list of functionally-aligned prioritized metrics on how to to measure success

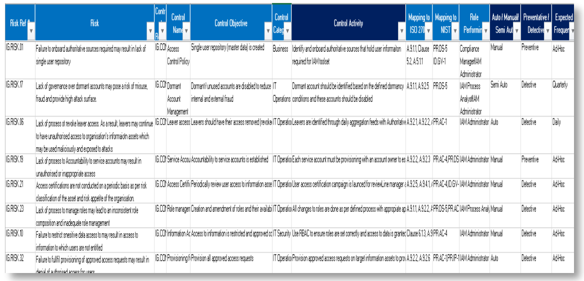
Maturity Model



	1	2	3	4	5
Functional Process	Manual, fragmented, non-integrated processes; ad-hoc, informal	Semiformal, Business Unit specific and target systems specific processes	Formal processes, defined and consistent across Business Units and target systems	Formal processes, integrated and refined, aligned with business processes.	Standardized and Optimized processes; aligned with corporate strategy
People	Informal, basic roles, responsibilities decentralized	Technical projects sponsored by Business Units and CISO; informal inventory of IAM skills	IAM PMO established, IAM roles and training needs defined	IAM PMO active, RACI matrix defined, proactive IAM skills development	Optimal integration with business; IAM skills optimized
Service Delivery Model	Decentralized, fragmented and incomplete IAM services	Some IAM process are centralized and a basic level of governance across other processes	All IAM processes are centralized and good level of governance across all processes	Some IAM processes are outsourced and high level of governance across all processes	All IAM processes are outsourced with some level of automation and high level of governance across all processes
Technology	Ad-hoc identity maintenance, and JML processes, manual access provisioning and access reviews	Identity data management and JML process done within local business functions, some apps have standardized provisioning and access reviews are not monitored	Sorted Identity data is maintained in authoritative sources, partial automation of JML process, approval based provisioning, and centralized access reviews	Integrated authoritative sources, workflow automation of JML processes, provisioning and access reviews are largely automated	Authoritative sources support claim based IAM process, JML workflow automation using single solution, dynamic provisioning and access reviews
Performance Insights & Data	Lack of analytics capability & standardized KPIs/ performance metrics; non measurable	Tactical efficiency and effectiveness improvements, low direct value	Sustained, quantifiable improvements tied to GRC imperative, moderate direct value	Sustained, quantifiable contribution to key business imperatives; Global standards and guidelines for data & reporting; high direct value	Business value optimization, transformational direct value
Governance	Ad-hoc, informal policies, which do not cover all areas of the organization; Policies are not regularly reviewed or maintained	Policies cover most function of the organisation but are not necessarily adhered to; Policies are not clear enough to derive consistent processes	Policies cover all areas of the organisation and support required business processes; IAM governance structure defined and accepted	Policies are clear and aligned to the organisation. Policies are current and cover all areas of IAM; improvement focus	Policies are comprehensive, understood and strictly adhered to; regular policy reviews to ensure appropriateness

Five point maturity rating scale for a level 1 (L1) process area describes level of maturity by TOM design layer.

Security & Controls



Risk Ref #	Risk	Contr R	Control Name	Control Objective	Control Categ	Control Activity	Mapping to ISO 270	Mapping to NIST	Role Performin	Auto / Manual/ Semi Aut	Preventative / Detective	Expected Frequer
IG.RISK.01	Failure to onboard authoritative sources required may result in lack of single user repository	IG.CO	Access Control Policy	Single user repository (master data) is created	Business	Identify and onboard authoritative sources that hold user informaiton required for IAM toolset	A.9.1.1, Clause 5.2, A.5.1.1	PR.DS-5 ID.GV-1	Compliance Manager/IAM Administrator	Manual	Preventive	Ad-Hoc
IG.RISK.17	Lack of governance over dormant accounts may pose a risk of misuse, fraud and provide high attack surface.	IG.CO	Dormant Account Management	Dormant / unused accounts are disabled to reduce internal and external fraud	IT Operations	Dormant account should be identified based on the defined dormancy conditions and these accounts should be disabled	A.9.1.1, A.9.2.5	PR.DS-5	IAM Process Analyst/IAM Administrator	Semi Auto	Detective	Quarterly
IG.RISK.06	Lack of process ot revoke leaver access. As a result, leavers may continue to have unauthorised access to organisation's informaiotn assets which may be used maliciously and exposed to attacks	IG.CO	Leaver access	Leavers should have their access removed (revoke	IT Operatio	Leavers are identified through daily aggregation feeds with Authoritativ	A.9.2.1, A.9.2.2, A	PR.AC-1	IAM Administrator	Auto	Detective	Daily
IG.RISK.19	Lack of process to Accountability to service accounts may result in unauthorised or inappropriate access	IG.CO	Service Accou	Accountability to service accounts is established	IT Operatio	Each service account must be provisioning with an account owner to es	A.9.2.2, A.9.2.3	PR.AC-4,PR.DS	IAM Administrator	Manual	Preventive	Ad-Hoc
IG.RISK.21	Access certifications are not conducted on a periodic basis as per risk classification of the asset and risk appetite of the organisation.	IG.CO	Access Certifi	Periodically review user access to information asse	IT Operatio	User access certification campaign is launced for reviewLine manager a	A.9.2.5, A.9.4.1, A	PR.AC-4,ID.GV-	IAM Administrator	Manual	Detective	Ad-Hoc
IG.RISK.23	Lack of process to manage roles may lead to an inconsistent role composition and inadequate role management	IG.CO	Role managen	Creation and amendment of roles and their availabi	IT Operatio	All changes to roles are done as per defined process with appropiate ap	A.9.1.1, A.9.2.2, A	PR.DS-5,PR.AC	IAM Process Analy	Manual	Detective	Ad-Hoc
IG.RISK.10	Failure to restrict snesitive data access to may result in access to information to which users are not entitled	IG.CO	Information Ac	Access to information is restricted and approved cc	IT Security	Use RBAC to ensure roles are set correctly and access to data is grantec	Clause 6.1.3, A.9	PR.AC-4	IAM Administrator	Manual	Detective	Ad-Hoc
IG.RISK.32	Failure to fullfil provisioning of approved access requests may result in denial of authorised access for users	IG.CO	Provisioning fi	Provision all approved access requests	IT Operatio	Provision approved access requests on target information assets to prov	A.9.2.2, A.9.2.6	PR.AC-1,PR.IP-1	IAM Administrator	Auto	Detective	Ad-Hoc

Matrix of key controls and risk mitigated by L1/L2 process level that includes GRC and automated intelligence opportunities and are mapped to NIST controls and ISO 27000

Questions?

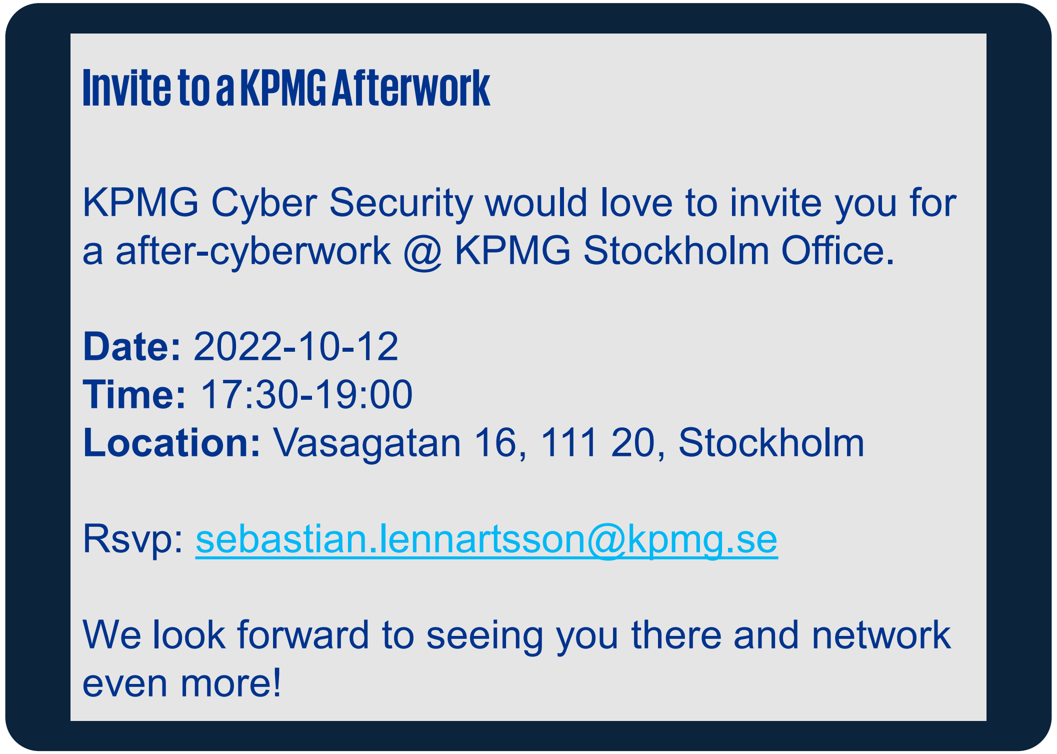
lukas.gronquist@kpmg.se

sebastian.lennartsson@kpmg.se

cecilia.olin@kpmg.se

carl.flodin@kpmg.se

Oh wait, what's next?



Invite to a KPMG Afterwork

KPMG Cyber Security would love to invite you for a after-cyberwork @ KPMG Stockholm Office.

Date: 2022-10-12
Time: 17:30-19:00
Location: Vasagatan 16, 111 20, Stockholm

Rsvp: sebastian.lennartsson@kpmg.se

We look forward to seeing you there and network even more!