Cloud security in a digital age

Lund University

2020-02-17, 13:00-15:00

Fredrik Hertz and John Kibuuka

The better the question. The better the answer.
The better the world works.

Building a better working world

Agenda

13:15-14:00

1. About us, about you
2. The Cyber risk landscape
3. What is cloud actually

14:00-14:15 Break

14:15-15:00

4. The risks and opportunities
5. Governance and regulatory
6. Insight into some cloud projects

But before we start...

... Who are you? Why did you chose Information- and cybersecurity?

About us

How and why did we end up at EY?

Fredrik Hertz

About me

- M Sc in Teleinformatics, KTH 1998
- 4+18 years in security consulting
- Armed forces, Police, Industrial, telecommunications, consumer products, banking and Insurance
- 3 kids, two dogs, one cat. Outdoor activities.

Why consultant and EY Advisory Services?

- You are surrounded by intelligent people
- Constant change, new people, new places
- Networking, access to and diversity of people

John Kibuuka

About me

- Consultant, Cybersecurity in Financial Services
- CCSP, CISSP, M.Sc. IT
- Active cyclist and father to two kids.

Why consultant and EY Advisory Services?

- Variety of tasks and clients
- Challenging projects
- Social networking
- Apply a wide set of skills
- International opportunities

EY is strong and globally integrated organization with local anchoring and over 1000 motivated Nordic consultants

Advisory | Assurance | Tax | Transaction | 230,000 professionals

> 150 countries

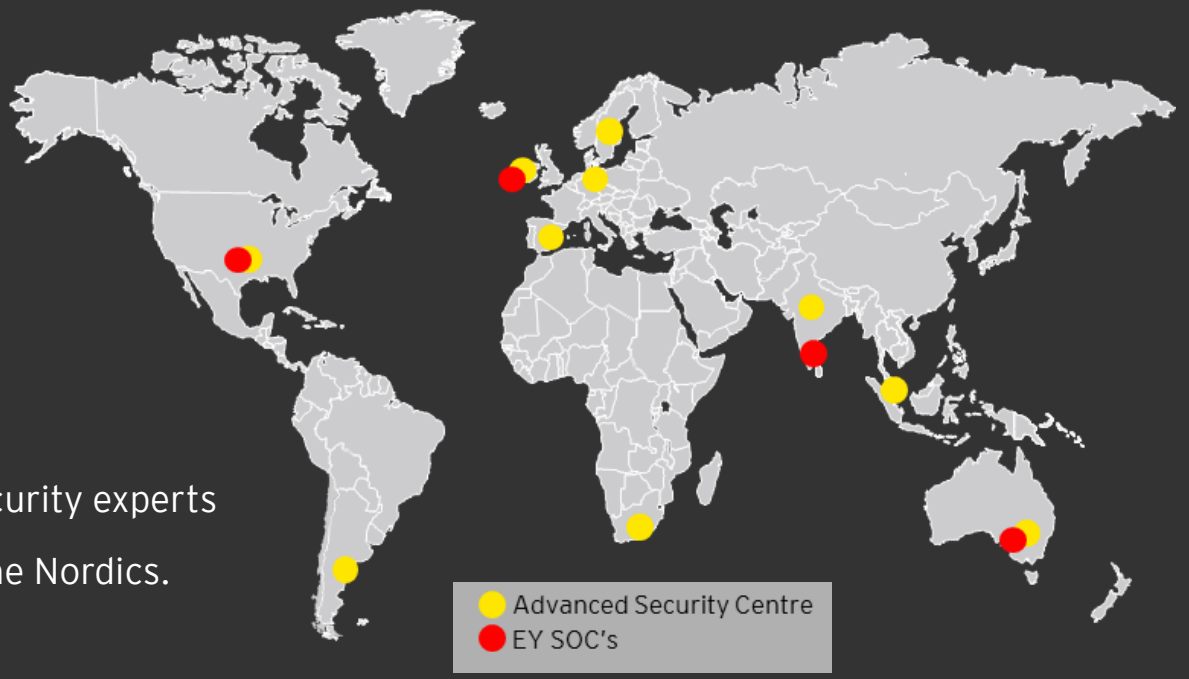
57,000 consultants

$8,53b revenue

- **Americas** 18,000 consultants
- **EMEIA** 23,000 consultants
- **APAC** 9,000 consultants
- **Japan** 1,000 consultants

Global leader in Information Security Consulting Services with full range of Information Security and IT risk services

7,200 global professionals with Information Security delivery capabilities



1,500 Information Security experts

100+ are working in the Nordics.

Examples of Nordic Cyber projects during FY 19:

Data Leakage Prevention implementation

GDPR assessments

Cybersecurity test of applications

Third party IT security review

Running the Cyber security program

Cyber risk assessment of private equity portfolio

Today, approximately…

300,000,000,000 emails are sent

3,850,000,000 people have an email address

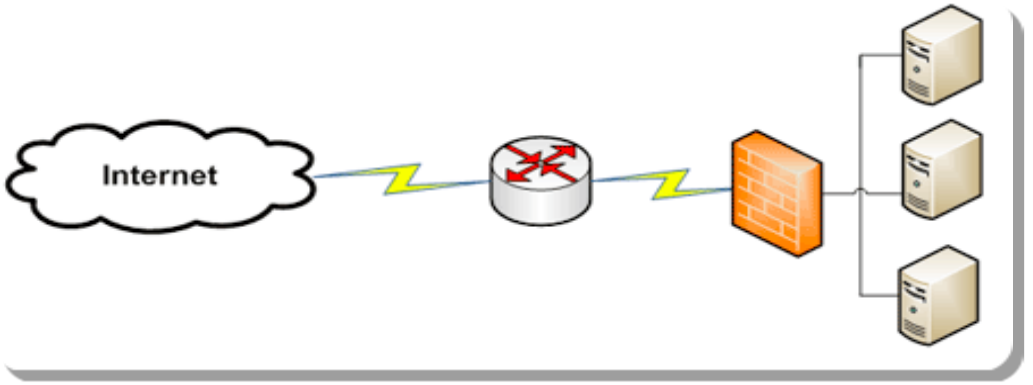
Which is the equivalent to 50% of the world population

1,000,000,000,000 phishing emails are sent in a year

30% of phishing emails get opened by targeted user

In The Beginning...

- System/Server centric – small number of systems, each secured individually
- Relatively simple functional applications
- Hacking was still primarily a hobby and required deep technical skills
- Targets were generally educational institutions, government and military systems and corporate data centers
- Events compromised a small number of systems
- Physical security applied; everything was encrypted



Other facts and figures…

2013 and early 2014, over 500,000 machines were infected by CryptoLocker

By 2016, TeslaCrypt made up 48 percent of ransomware attacks

But in mid-2017, two major and intertwined ransomware attacks spread like wildfire across the globe, WannaCry (more than 400k infections) and NotPetya, which was estimated by the US White House to have cost the over $10Billion in damages.

6.4 billion
The number of fake emails sent worldwide – every day[1]

1,464
The number of government officials in one state using "Password123" as their password

50%
The number of local authorities in England relying on unsupported server software

2 million
The number of stolen identities used to make fake comments during a US inquiry into net neutrality

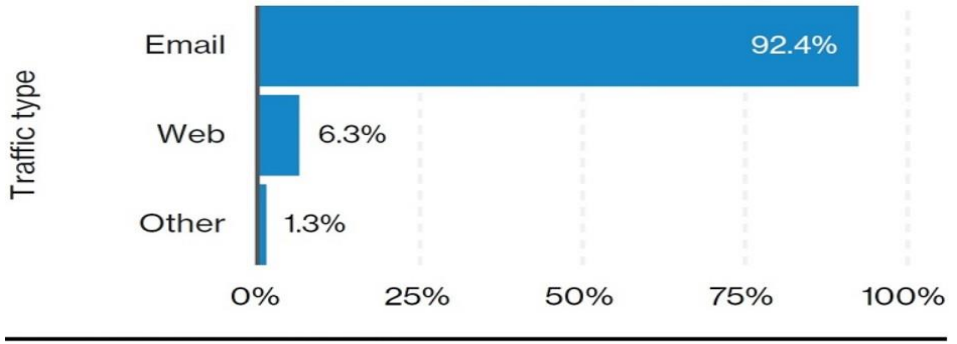
1,946,181,599
The total number of records containing personal and other sensitive data compromised between January 2017 and March 2018

US$729,000
The amount lost by a businessman in a scam combining "catphishing" and "whaling"

550 million
The number of phishing emails sent out by a single campaign during the first quarter of 2018

US$3.62m
The average cost of a data breach last year

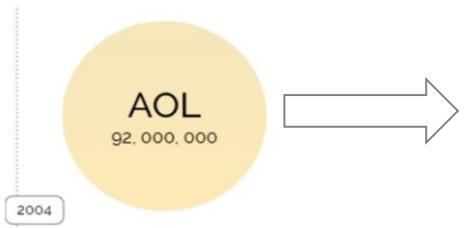
Frequency of malware vectors [2]



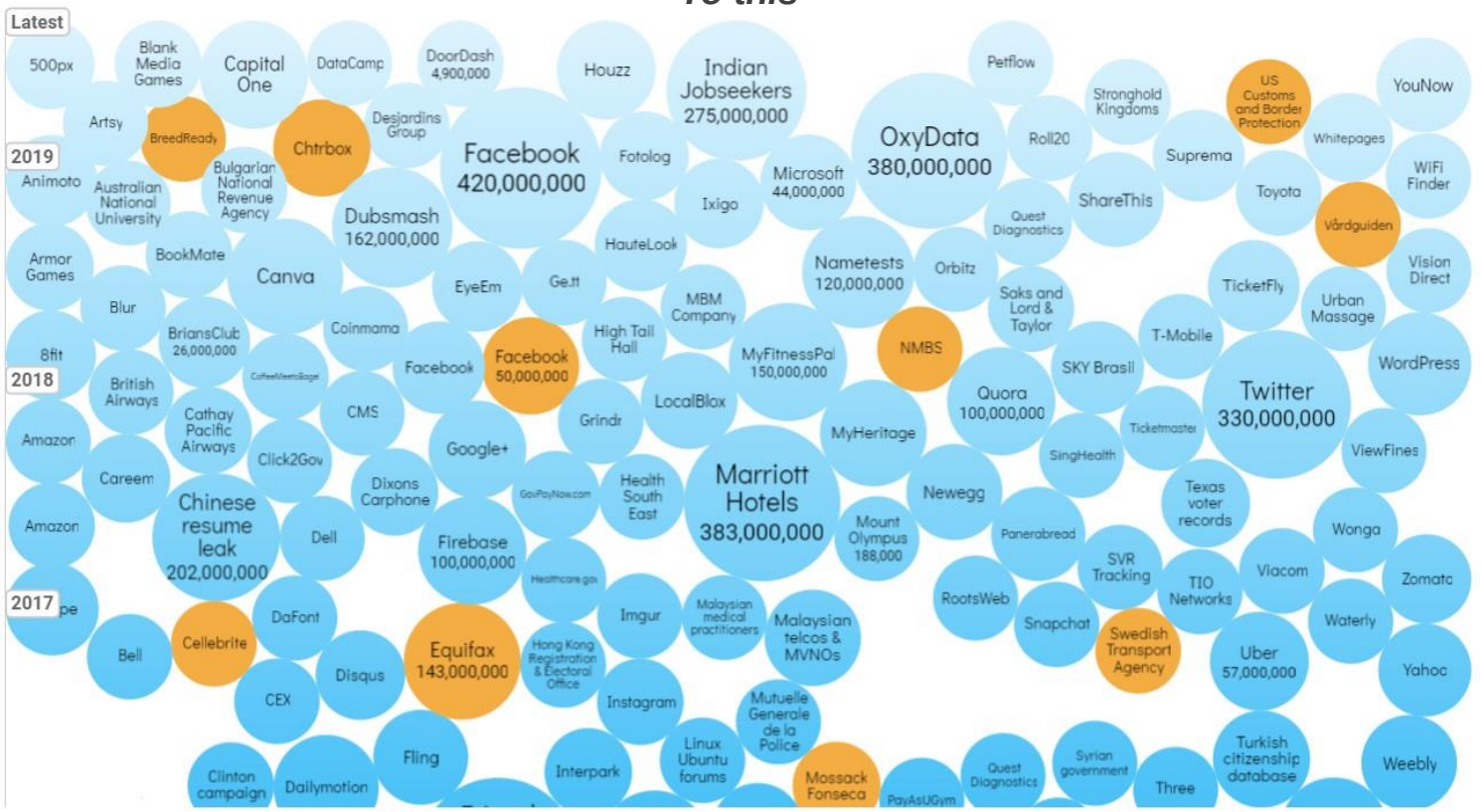
Why is this important?

The current cyber risk landscape
Evolution of the data breach…

From this



To this



Nearly one percent of global GDP is lost to cybercrime each year.

Global spend on cybersecurity products has gone from $4.5 Billion in 2004, to $77 Billion in 2015 to more than $120 Billion in 2017. It is expected that global spending on cybersecurity products and services will exceed $1 trillion cumulatively over the next five years

The current threat and vulnerability landscape

- The attack surface is increasing, driven by:
  - The adoption of emerging technologies
  - Convergence of IT, IoT and OT
  - Interconnectivity with third parties
- **Insiders** are an "unwitting" accomplice in 95% of incidents
- Cyber threats are increasingly using destructive methods to achieve their goals..

Key Takeaway
The cybersecurity threat is stealthy, the vulnerability attack surface is expanding

Swedish businesses experience increased cyber attacks, data leakage and breaches with costly outcomes

Swedish Transport Agency leaked private data about citizens, police and military - DG head rolled, SEK 70 000 in fine

School in Skellefteå fined SEK 200 000 for face recognition

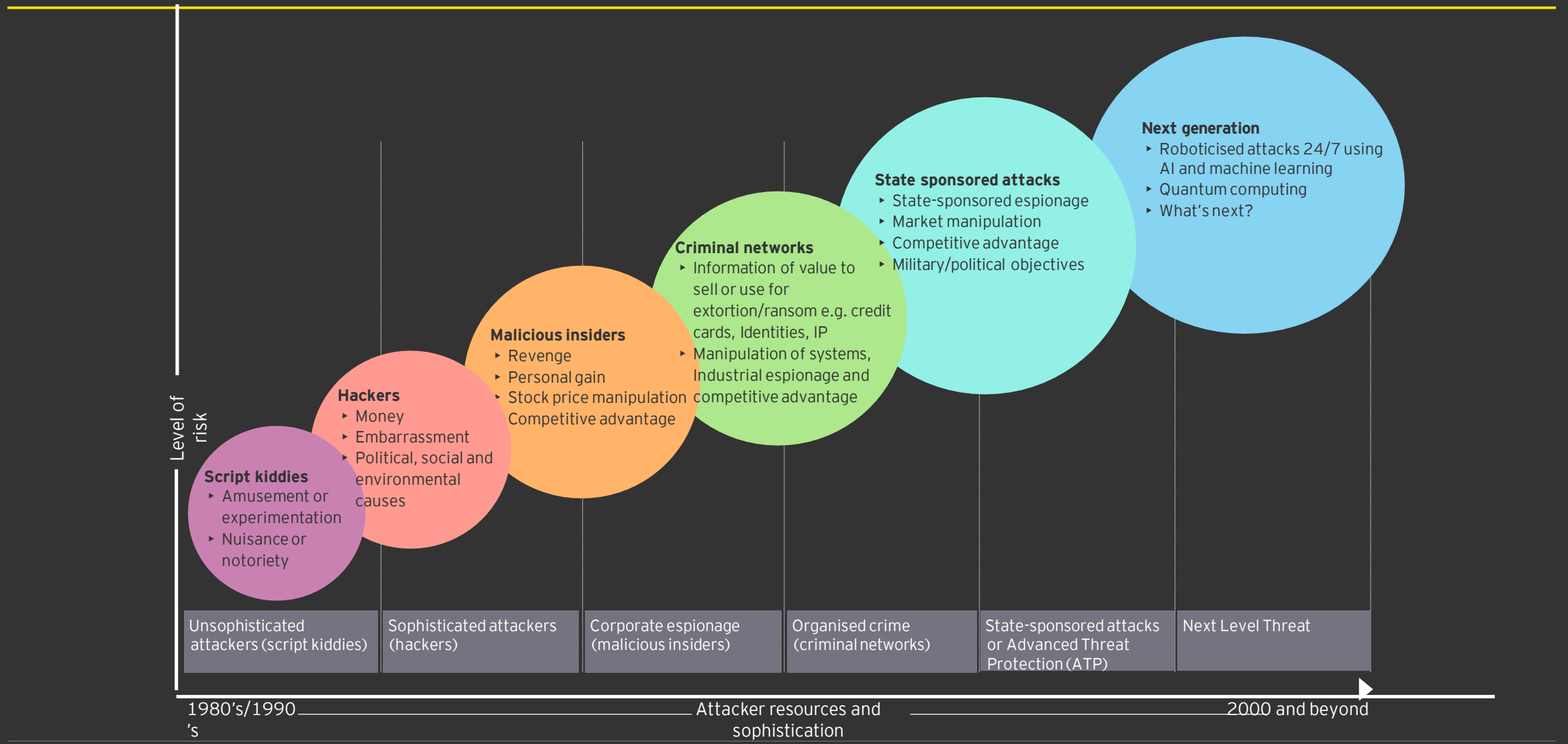
1177 leaked 2.7 million recorded healthcare phone calls leaked online – under investigation at Data Authority

Nasdaq Clearing and Nasdaq Stockholm fined 25 respective 30 millions SEK for insufficient management of cybersecurity risks

Ericsson suffered by the Cloud Hopper attack with potential leakage of confidential data to Chinese competitors

In 2020 we expect tens and potentially even hundreds of millions of euros in fines for GDPR data breaches

Cyber attacks are increasing in sophistication

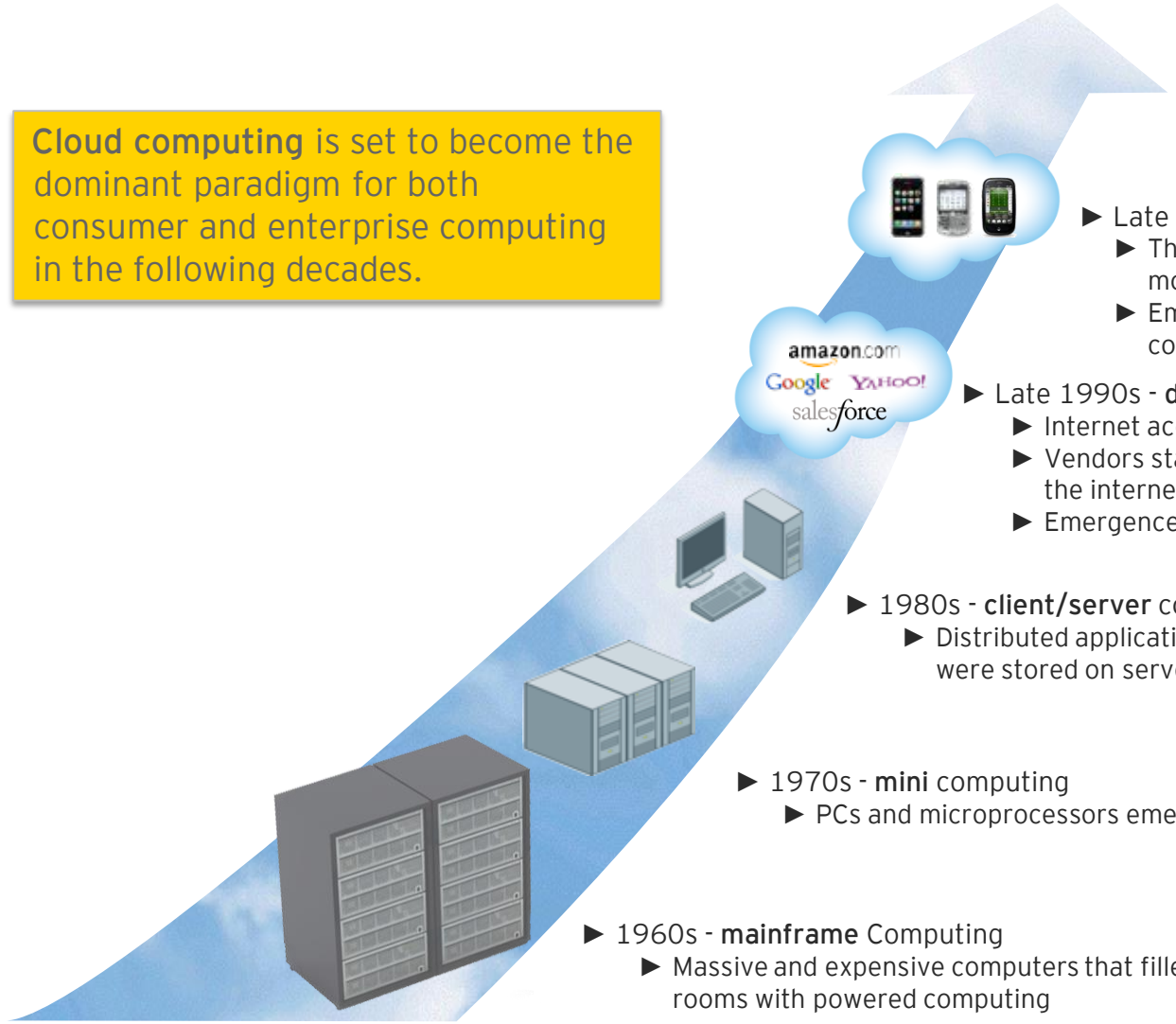


What is Cloud?

The evolution of computing

Computing has evolved from massive, centralised mainframe computing to distributed, elastic, multi-tenant cloud computing in the last few decades

Cloud computing is set to become the dominant paradigm for both consumer and enterprise computing in the following decades.



- 2010 and beyond – **cloud computing** emerging as the new computing paradigm
- Late 2000s - **mobile** internet computing
  - The internet is accessed more through mobile devices than through desktops
  - Emergence of Cloud Computing in consumer markets
- Late 1990s - **desktop** internet computing
  - Internet accelerated with content and search
  - Vendors started to deliver applications via the internet (download)
  - Emergence of Web applications
- 1980s - **client/server** computing
  - Distributed application model – software applications were stored on servers and accessible via the desktop
- 1970s - **mini** computing
  - PCs and microprocessors emerged
- 1960s - **mainframe** Computing
  - Massive and expensive computers that filled rooms with powered computing

What is cloud computing?

Cloud computing is an approach to computing infrastructure that links large pools of resources to be shared simultaneously by multiple businesses or users

- Cloud computing is not a **technology**, but a **sourcing paradigm** for IT services
- There are a number of different cloud deployment models emerging such as **public**, **private**, **community** and **hybrid** clouds
- There are also several types of services being delivered via the cloud including **software-as-a-service** and **infrastructure-as-a-service**
- Key characteristics of cloud computing include **virtualization**, **subscription-based** fees, ability to **match usage to costs** and **agile provisioning**

Cloud Service Models

Sophistication of offering

Software as a Service (SaaS)

Applications are delivered as services rather than on-premises software (e.g. Salesforce.com, Google Apps, MS Office 365)

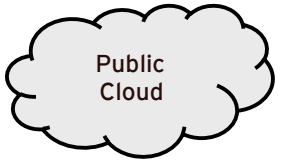
Platform as a Service (PaaS)

Execution platforms or middleware are provided as a service for software development, testing and operations

Infrastructure as a Service (IaaS)

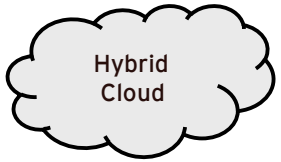
Infrastructure, storage and networking are provided as a service (e.g. Rackspace, Verizon, Amazon)

Cloud Deployment Models

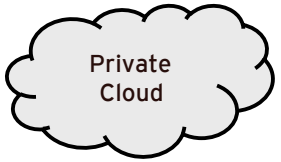


Available via the internet to the general public or a large industry group with third party ownership (eg Google, Amazon)

Supports a specific community of organisations that have shared concerns via a private network (e.g. UK G-cloud for government)



Combination of public and private cloud solutions e.g. an organisation may use a public cloud provider for email and collaboration services, but may set up a private cloud for business critical applications



Operated solely within an organisation and maintained by the internal IT department

Five essential cloud characteristics

Five Essential Characteristics:

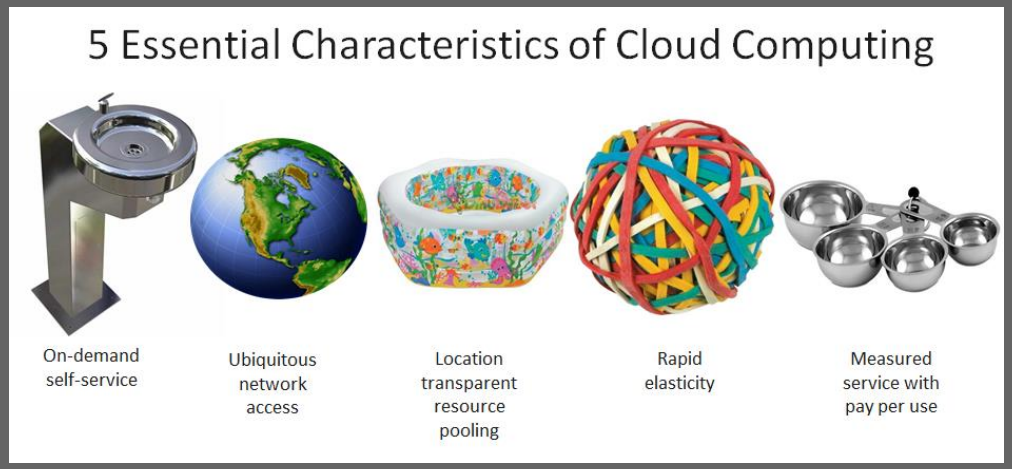
On-demand self-service. A consumer can obtain computing capabilities, such as server time and network storage, as needed without requiring human interaction with each service provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by multiple devices (e.g. mobile phones, laptops, tablets)

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Examples of resources include storage, processing, memory, network bandwidth and virtual machines.

Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out, and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and consumer of the service.



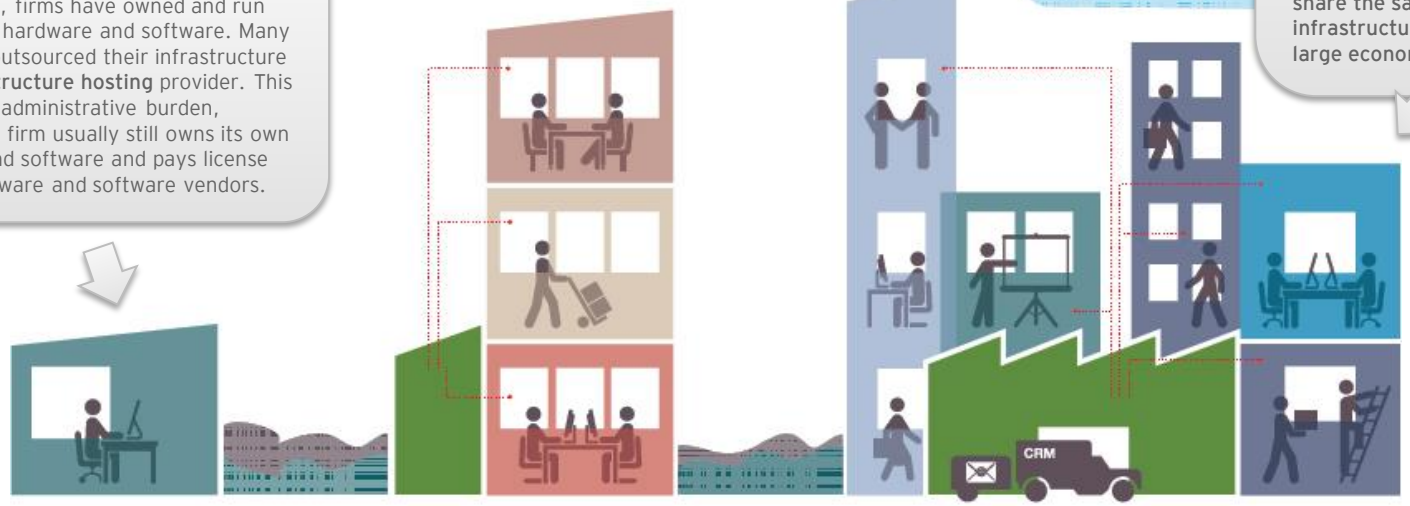
Moving from dedicated IT to the cloud

Firms are steadily moving from dedicated in-house IT infrastructure to publicly or privately hosted cloud solutions

Private Cloud
A private cloud offers some of the same benefits as the public cloud, however is used exclusively by one organisation resulting in less scale than Public Clouds

Public Cloud
The public consumer cloud is the most well-known form of the cloud. A cloud vendor provides infrastructure, software and platform services to customers either free or on a subscription basis. Multiple customers share the same physical infrastructure resulting in large economies of scale.

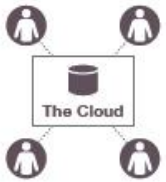
Dedicated IT
Traditionally, firms have owned and run their own IT hardware and software. Many firms have outsourced their infrastructure to an **infrastructure hosting** provider. This reduces the administrative burden, however the firm usually still owns its own hardware and software and pays license fees to hardware and software vendors.



Dedicated IT

Corporations own and manage their own IT resources, each having their own servers, software and hardware.

Private Cloud



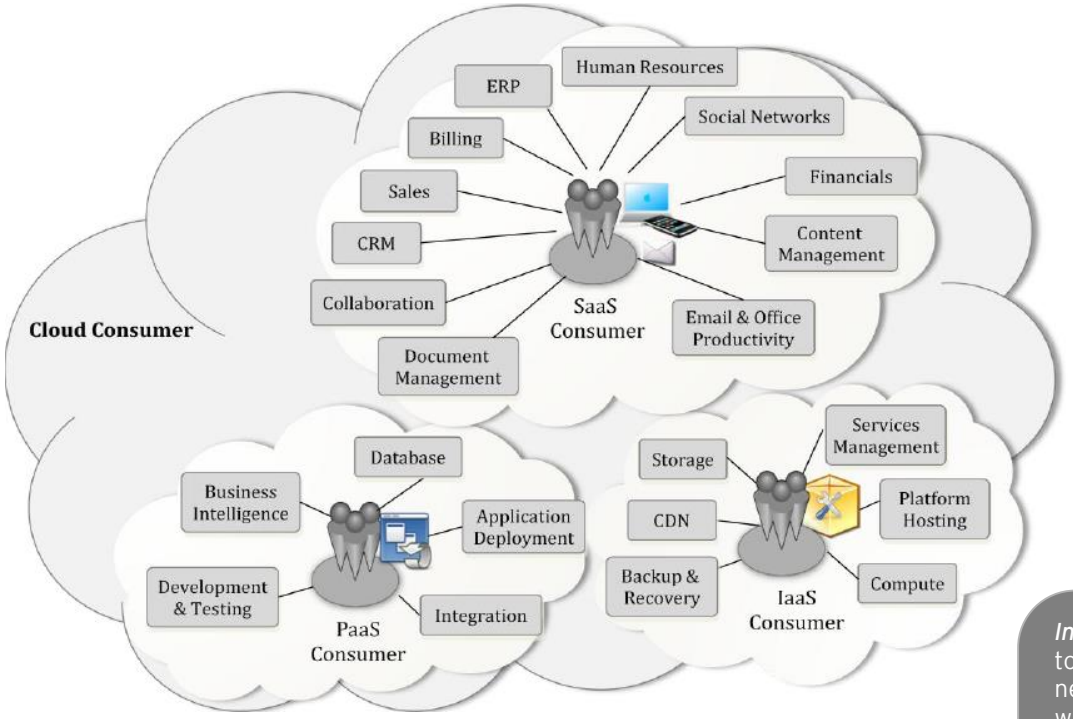
With a private cloud, IT resources are pooled and shared between different business units in the same organisation.

The Public Cloud

A public cloud delivers IT resources through specialist providers to different corporations. You only pay for the services that you use.

Cloud service models

IaaS, SaaS and PaaS are currently the three major cloud service models, firms may pick and choose the type of cloud service they want to use



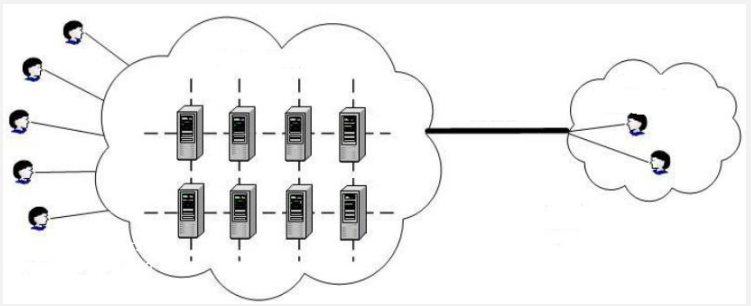
Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems or storage, but has control over the deployed applications and possibly application hosting environment configurations.

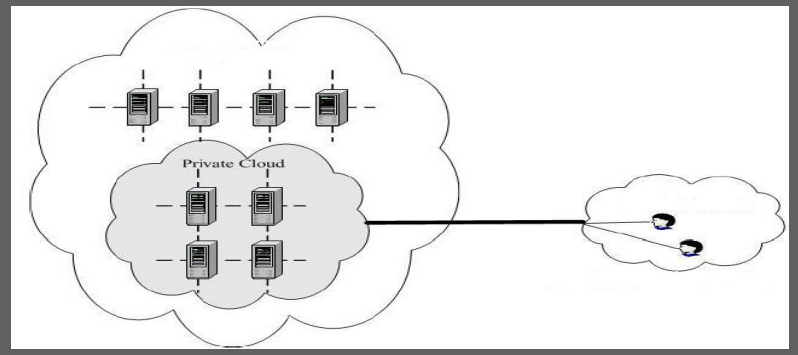
Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications and possibly limited control of select networking components (e.g., host firewalls).

Cloud deployment models

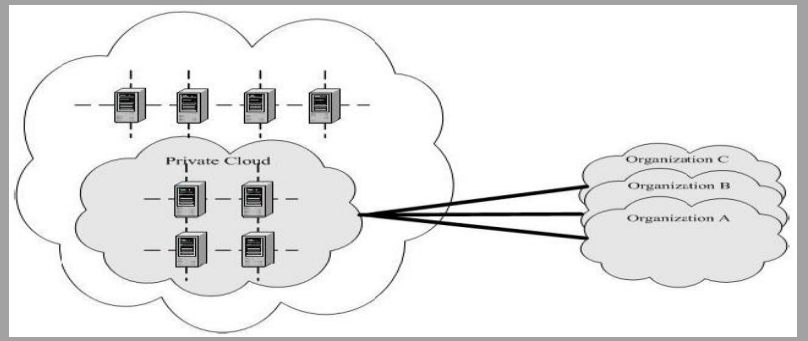
Firms can decide which cloud deployment model is most suited to their needs, and can opt to go for a hybrid of public and private cloud solutions



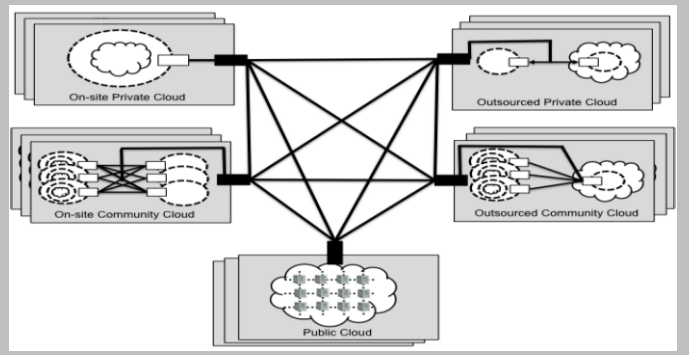
Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organisation selling cloud services.



Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organisation or service provider and may exist on premise or off premise.



Community cloud. The cloud infrastructure is shared by several organisations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy and compliance considerations). It may be managed by the organisations or a service provider and may exist on premise or off premise.



Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardised or proprietary technology that enables data and application portability (e.g. cloud bursting[1] for load balancing between clouds).

[1] Cloud bursting refers to a configuration where an application can 'burst' into a public cloud when it runs out of resources on a private cloud

Drivers of cloud adoption

Key market drivers

- **Proven delivery model.** The cloud computing (SaaS, in particular) model continues to prove its merit in the business applications market
- **Increasing adoption by the corporate market.** The adoption of cloud computing by the corporate market has been accelerating. In the past, SaaS adoption has been led by SMBs, but lately, the corporate market has also taken notice of the model.
- **Improving sentiment toward the cloud.** Many IT managers are becoming more comfortable with cloud computing, as it creates an opportunity to free up capital resources that can be used to fund other projects. And allows IT personnel to shift from systems and hardware management to more strategic activities.
- **Reduced costs.** The initial expenses associated with using cloud services are usually less than buying or internally developing traditional enterprise applications. Customers will typically spend less time and money on maintenance, integration, version upgrades and bug fixes.
- **Faster deployment time.** SaaS allows for faster deployment times due to less infrastructure costs for companies.
- **Shift in software delivery model by vendors.** Most new software companies currently entering the market are built on the SaaS model.

Drivers of cloud adoption

Key market drivers

- **Open source popularity helping cloud acceptance.** The increasing popularity and acceptance of open source software (OSS) has played a major role in the progress and development of cloud computing. The low development costs related to open source software and its free use makes it an attractive platform for cloud computing software development.
- **Reduced customer risks.** Software delivered on demand helps to reduce customer risk in terms of infrastructure and implementation of new and unknown systems
- **Allows corporate IT to be more strategic.** Cloud computing can reduce the time required to scope, procure, develop, test, deploy and support internal applications. As a result, corporate IT can focus on more strategic issues.
- **Making headway in various business functional areas.** SaaS is for presence within the customer relationship management (CRM) space, human resources, document management, compliance, collaboration and web conferencing.
- **Increasing popularity of the internet.** The increasing popularity of the internet, mobile computing, social computing and and the increasing pervasiveness of broadband access are key factors that are driving the shift in cloud computing.

Challenges of cloud adoption

Key market challenges

- **Lower customization capabilities.** With applications that touch the core of the enterprise, adoption and penetration is expected to experience some major hurdles due to the lack of additional customization capability.
- **Service reliability and disruptions.** Another major area of concern for the enterprise market is that interruptions in not only the cloud provider, but also the internet provider will cause service disruptions.
- **Integration challenge.** There is a major challenge when it comes to integrating SaaS applications with other enterprise applications and data source as custom code still accounts for about 60% of the enterprise market.
- **Concerns about data protection.** Security may still remain an impediment, especially when sensitive information is being handled. Certain businesses may remain hesitant to use a SaaS provider for applications containing sensitive information, since the perceived risks remain higher compared to handling this type of data in-house.

Challenges of cloud adoption

Key market challenges

- **Loss of control.** Cloud computing increases the reliance on the provider for functions such as infrastructure, application management, usability and technical support. Hardware, software and data all reside with an external vendor, so the user has less control over these factors compared to having on-premise applications.
- **No industry standards.** Given the early stage of cloud computing, there are no comprehensive standards, which are particularly important for application development platforms
- **Difficulty in choosing a vendor.** Certain platforms may become more dominant than others, leaving those customers that choose less successful platforms early on in a more tenuous position. This uncertainty makes choosing a vendor more difficult and could delay adoption of cloud services until a dominant player emerges.
- **Infrastructure limitations.** Since cloud-based services are delivered over the internet, these services are dependent on speed of internet access. This could pose problems, especially in third-world countries where communications infrastructure is not fully developed compared with in highly developed countries.

Challenges: What do users do with cloud services?

https://www.youtube.com/watch?v=Usq3SO_Fvjg

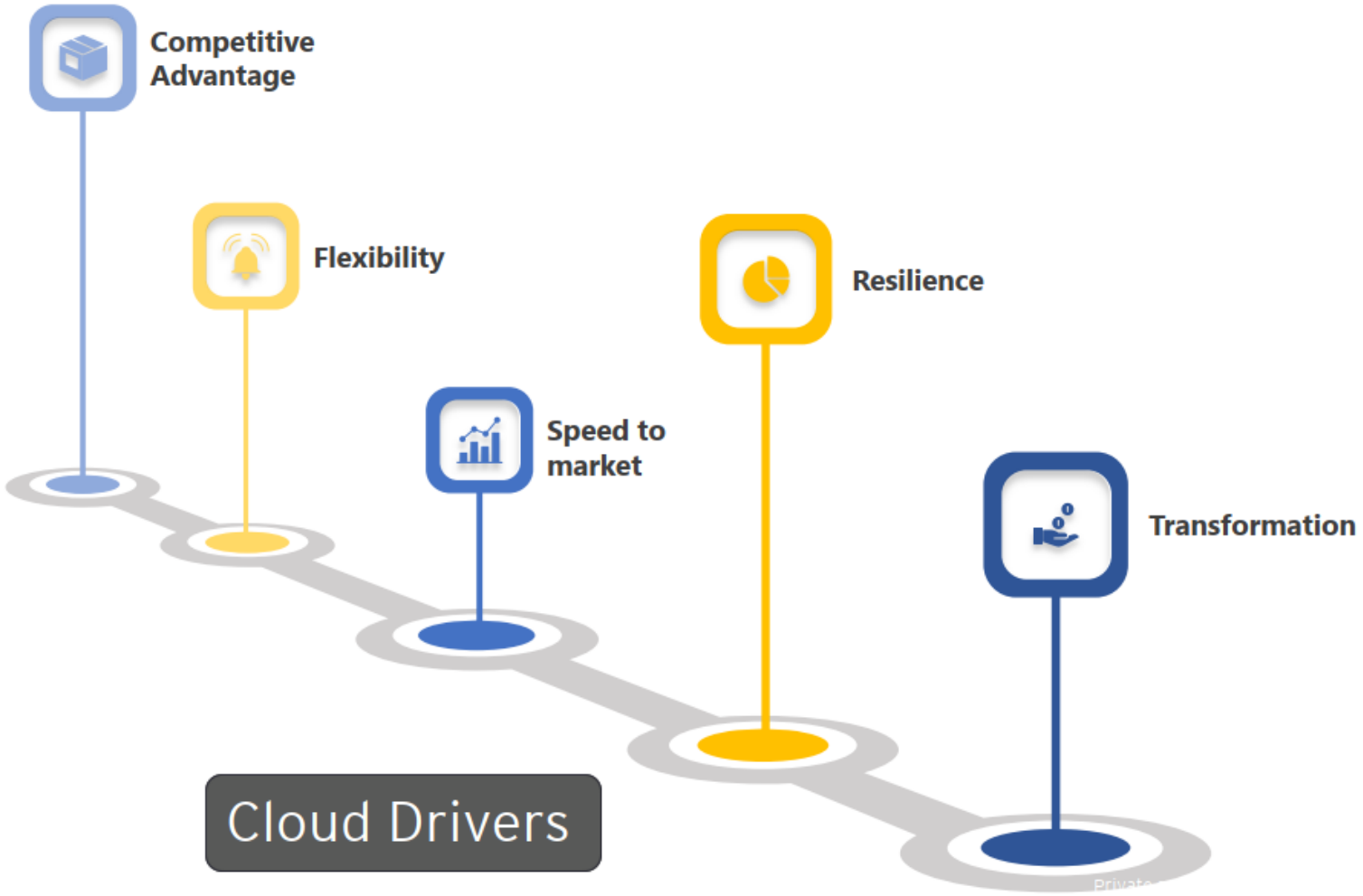
Break

The risks & opportunities

Why is cloud in every company strategy discussion?

Market Drivers

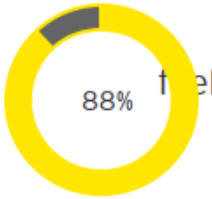
- Companies are finding it challenging to comply with new regulations (e.g. OpenBanking) due to legacy system limitations
- Cost-income ratio pressure
- Fintechs pressure



The future of cloud?

Prevalent technologies in the future

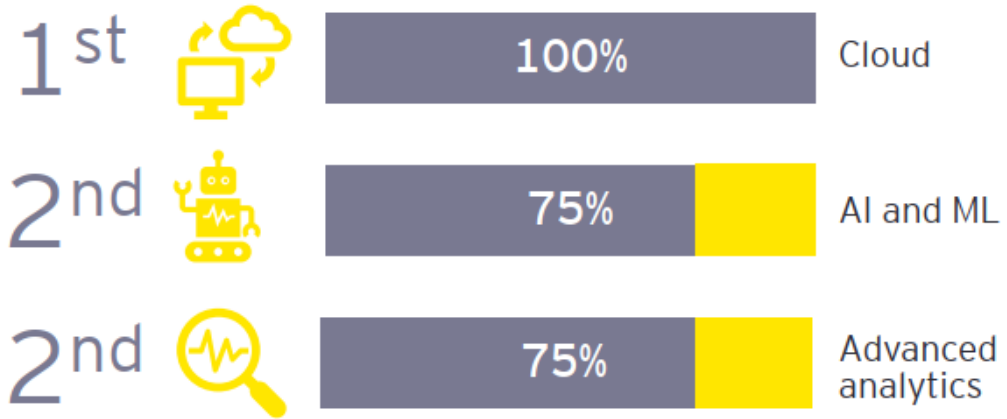
Do you think cloud adoption gives you an advantage against your competitors?



88% feel that cloud adoption gives an advantage against their competitors

Transformative technologies in next 12 months

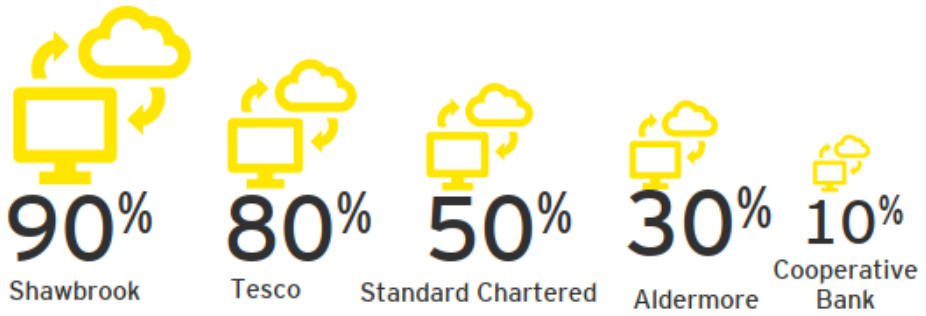
In priority order, what top 3 technologies do you feel will be the most transformative to your business in the next 12 months



Magnitude of migration of business to cloud

What % of your business are you planning to migrate to public cloud in the next 2 years?

38% banks intend to migrate more than 20% of their business to cloud in the next 2 years, with some banks targeting higher percentages ...



57% will move Digital (Marketing / CRM) to cloud

43% will move SaaS (Office365 / FinTech) to cloud

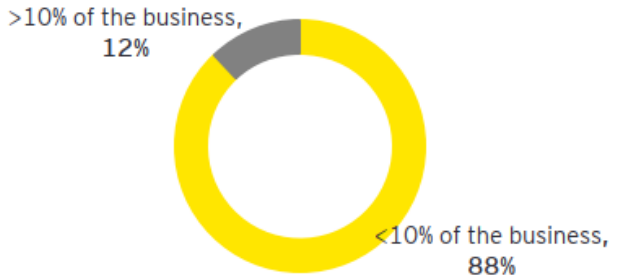
43%

will **not** move their "core engines" to cloud primarily due to legacy IT systems and change management

What do we do with the cloud - banking

Status of migration to public cloud

What % of your business has already been migrated to public cloud?



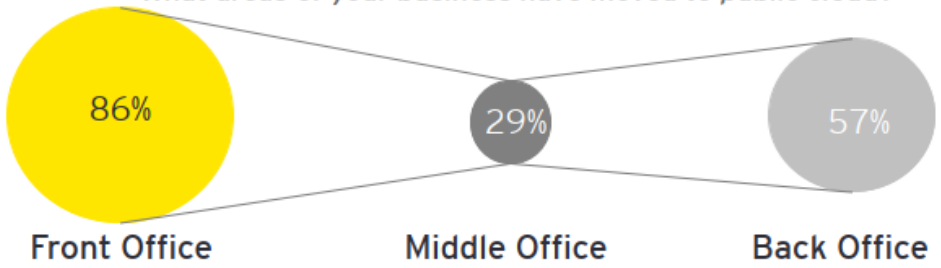
Leading cloud technology vendors

Which cloud vendors are you using?

Microsoft Azure	88%
Amazon Web Services	88%
Oracle Cloud	25%
Google GCP	25%
IBM	25%

Status of area-wise migration to public cloud

What areas of your business have moved to public cloud?



Aldermore hasn't moved to public cloud yet, but is planning to move front office applications and data warehousing platform to the cloud. **Cooperative Bank** moved digital channels and open banking.

Status of workload migration to public cloud

What workloads have you moved to public cloud (in production)?

86% moved SaaS (Office365 / FinTech)

43% moved Core Engine (Banking, Capital Markets, Asset Management)

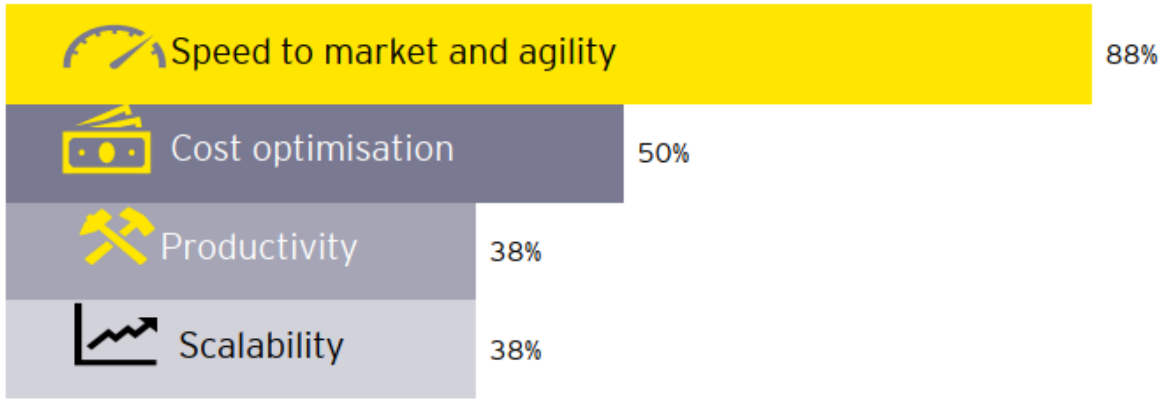
71% moved Digital (Marketing, CRM)

14% moved Risk (Market Risk, Credit Risk)

The risk of cloud - banking

Top business benefits of cloud

what are the top 3 benefits of using public cloud?



- Speed to market and agility cited as the top benefit for moving to cloud by 88% of the respondents
- Respondents also stated cost optimisation, productivity and scalability as other top benefits of cloud adoption
- Standard Chartered Bank and Tesco ranked risk mitigation over speed to market and productivity respectively

Barriers pertaining to shift to cloud

What are the top 3 barriers to public cloud adoption in your business?

88% Lack of knowledge and experience

75% Regulatory compliance

50% Culture change

38% Security of sensitive data

Risks of public cloud deployment

what are the top 3 risks that need to be addressed for ongoing deployment of public cloud in your business?

88% Regulatory risk

88% Data security risk

50% Third-party risk

The risk of cloud - banking

Triggers of cloud adoption

What triggered your business to move to cloud?

Technology and digital disruption (including digital shift) — 63%

1st — Most of the respondents say technology and digital disruption triggered their response to cloud adoption

Transformation — 63%

2nd — Transformation has also triggered the adoption of cloud in banks

Analytics — 25%

3rd — Banks also mentioned analytics as a trigger for cloud adoption

Competition — 25%

4th — Competition is also forcing banks to move their businesses to cloud

Regulatory adherence

What regulation is this helping you adhere to?

Open banking regulations — 50%

1st — Majority of the respondents are leveraging cloud to help them adhere to open banking regulations

Payments — 38%

2nd — Respondents are using it to comply with payments regulations

Cyber-security — 38%

2nd — Respondents are also seeing it useful to comply cyber-security regulations

Banks are also using cloud for Operational resilience and Risk Weighted Assets (RWA) regulations

Cloud Security Threats

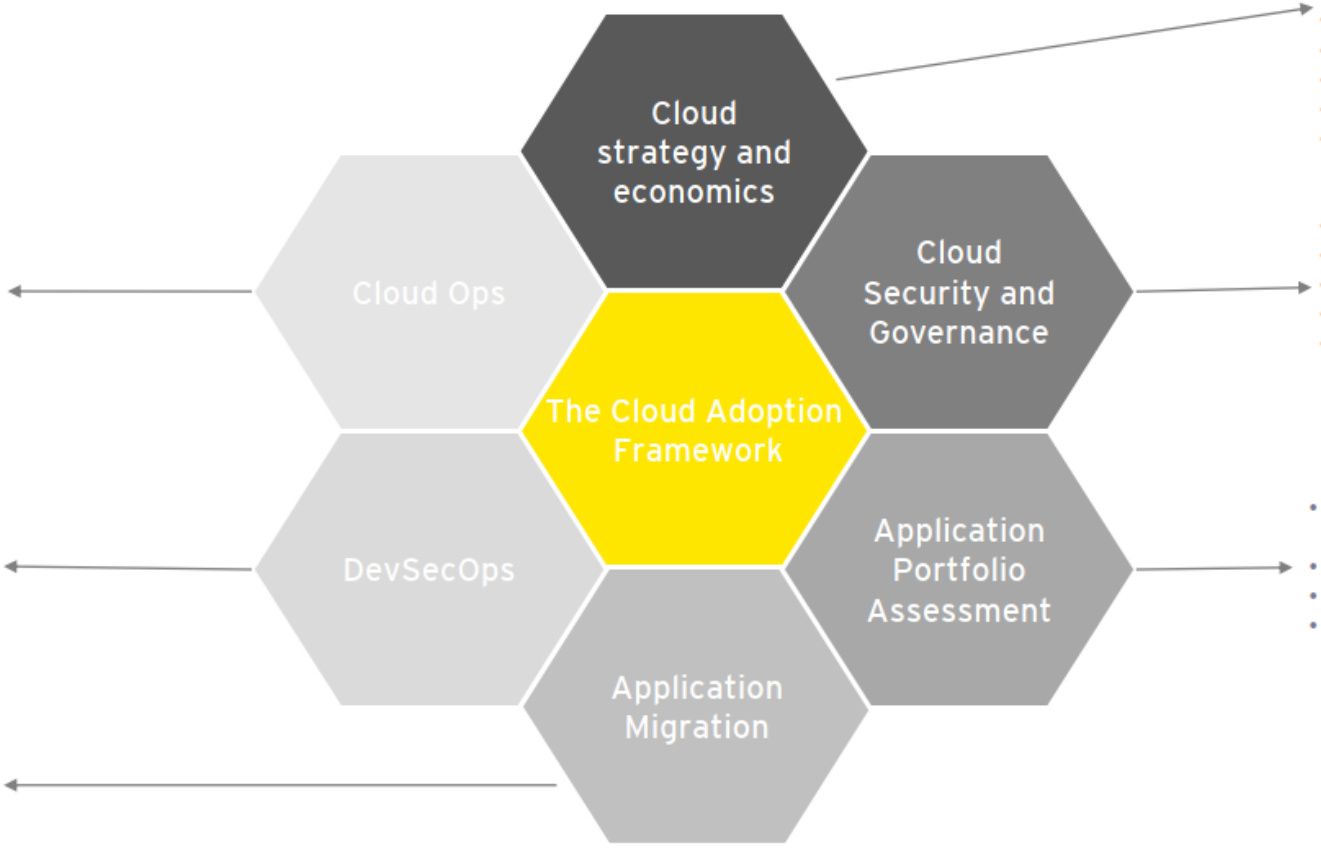
Threat	Description	Business Impact	Examples
1. **Credential theft, abuse and account hijacking**	Insufficient identity access management systems, failure to use multifactor authentication, weak password use/re-use, API reuse and a lack of ongoing automated rotation of cryptographic keys, passwords and certificates	Malicious actors can potentially masquerade as authorized users and can read/exfiltrate, modify and delete data, completely control cloud management functions, snoop on data in transit or release malicious software that appears to originate from a legitimate internal source.	a) Uber Paid Hackers to Delete Stolen Data on 57 Million People, https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data b) Sensitive client emails, usernames, passwords exposed in Deloitte hack, https://www.theregister.co.uk/2017/09/25/deloitte_email_breach/
2. Data exposure due to insecure applications, APIs and systems	CSPs provide APIs to their clients for provisioning, management, orchestrating and monitoring. The security and availability of general cloud services is dependent on the security of these APIs which are generally the most exposed part of the cloud systems and the target of heavy attacks.	It is critical for the firm to understand the security implication associated with use, management, orchestration and monitoring of cloud services using APIs. Reliance on weak interfaces and APIs exposes firm to variety of security issues.	Facebook Data Breach highlights API vulnerabilities, https://www.pingidentity.com/en/company/blog/posts/2018/facebook-data-breach-highlights-api-vulnerabilities.html
3. Unauthorized use of cloud services	Malicious actors may leverage cloud computing resources to target users, organizations or other cloud providers. Examples of misuse include email spam, DDoS, phishing campaigns and crypto miners	Malicious use of cloud services can reduce available capacity for legitimate users. Responding to malicious attacks reduces availability of response resources for addressing customer support issues.	Crypto-coin miners caught toiling away in hacked cloud boxes, https://www.theregister.co.uk/2017/10/17/cryptocoin_miners_turning_up_on_unprotected_cloud_instances/

Cloud Security Threats

Threat	Description	Business Impact	Examples
4. Shared technology vulnerabilities	CSP deliver cloud services at scale by sharing infrastructure, platforms or applications. Underlying components may not have been designed to offer strong isolation properties. This can lead to shared tech vulnerabilities that can be exploited in all delivery models.	A compromise of an integral piece of shared technology such as hypervisor, a shared platform component, or an application in a SaaS environment exposes more than just the compromised customer; rather it exposes the entire environment to a potential of compromise and breach.	a) The CPU catastrophe will hit hardest in the cloud, https://www.theverge.com/2018/1/4/16850120/meltdown-spectre-vulnerability-cloud-aws-google-cpu ; b) Microsoft Azure Flaws Could Have Let Hackers Take Over Cloud Servers, https://thehackernews.com/2020/01/microsoft-azure-vulnerabilities.html
5. Denial of Cloud based services	By forcing the target CSP to consume inordinate amounts of finite system resources such as processor power, memory, disk space or network bandwidth, the attacker(s) cause an intolerable system slowdown to prevent users from being able to access their data or applications	DoS frustrates the firm's customers and deteriorates client satisfaction, lowering their trust for the firm to continue to provide quality service and keep their data safe. Further, the CSP typically bill the firm on compute cycles and disk space, whereby an attack may consume so much processing time to cause significant charges.	a) Top IT Outages of 2019, https://statuscast.com/top-it-outages-2019/ b) Cyber Attack on Cloud Computing Company makes France news websites go dark, https://www.cybersecurity-insiders.com/cyber-attack-on-cloud-computing-company-makes-france-news-websites-go-dark/
6. Misuse due to malicious insiders at CSP facility	CSP employees have authorized access to the infrastructure platform or applications they provide as a service. Their intentional or misuse that privileged access control negatively affect the confidentiality, integrity or availability of organizations inform systems.	From PaaS to SaaS, CSP admins can have increasing levels of access to more critical systems and eventually to data. Malicious insider at CSP can potentially access and abuse the firms sensitive information or violate regulatory requirements in protecting the firm's customer data.	a) Insider Threats To Your Organization, https://cloudtweaks.com/2012/10/insider-threats/ b) Cloud's Privileged Identity Gap Intensifies Insider Threats, https://www.darkreading.com/vulnerabilities---threats/clouds-privileged-identity-gap-intensifies-insider-threats/d/d-id/1138974

Governance and standards

EY and the client´s cloud journey



- Executive Cloud Benefits
- Objectives & Goals
- Cloud Readiness Assessment
- Organizational Alignment
- ROI/TCO Analysis
- Economic Models

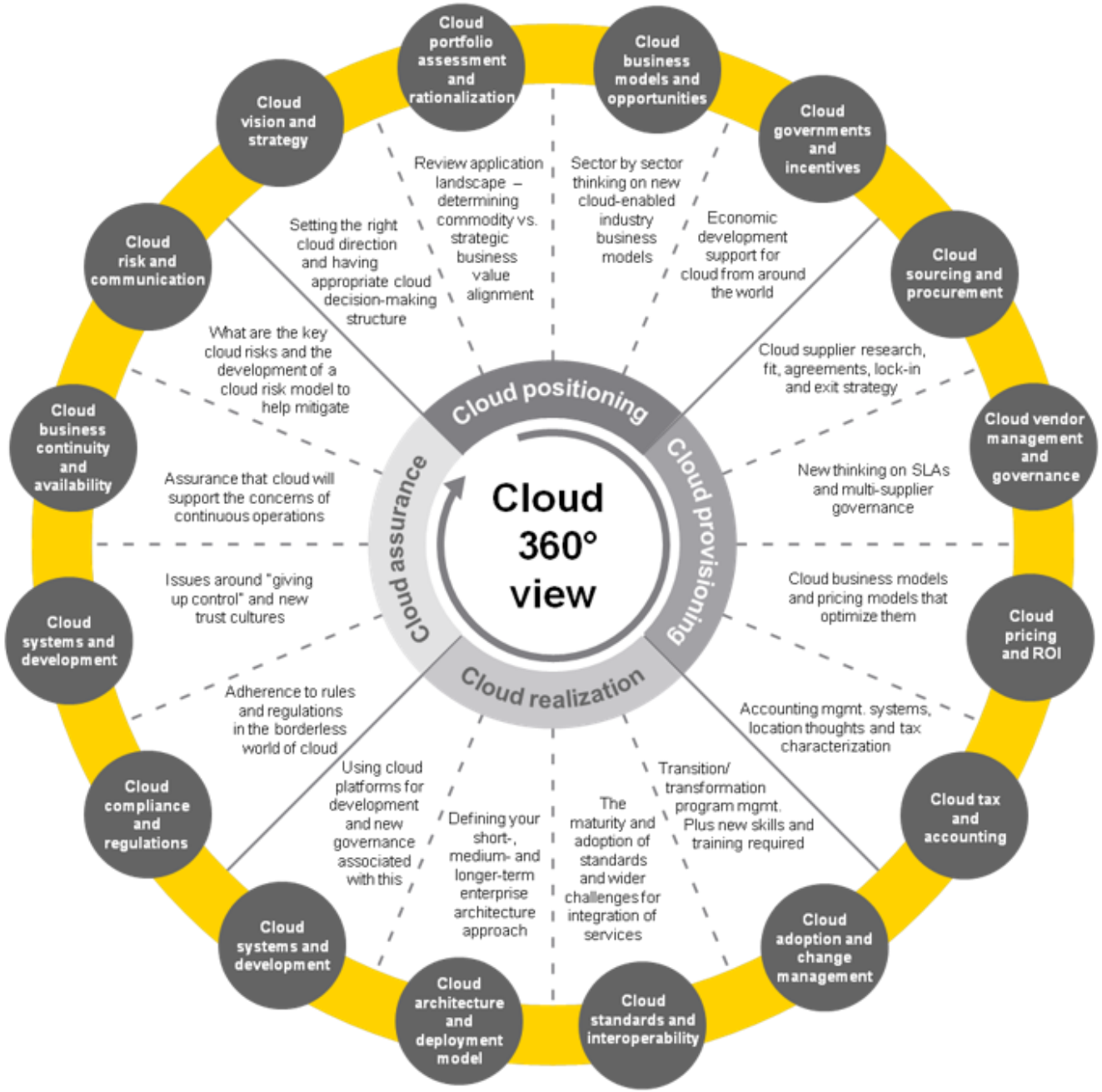
- Service Management
- Cloud Operational Model – Stakeholders provide metrics for what success looks like
- Governance, Billing, Chargeback, Audit, Logging, & Escalation
- Organizational Playbooks
- Training

- Security Controls and Assessment
- NIST/CSA/ISO Standards
- Security Technology Assessment
- Tools and Architectures
- Remediation & Implementation for a Secure Cloud

- DevSecOps Maturity Assessment
- DevSecOps Training
- DevSecOps Automated Services

- Portfolio and Application Readiness Assessment
- Cloud Reference Architecture
- Capabilities Matrix
- Application Cloud Roadmap & Plans

- Minimum Viable Cloud POCs and Pilots
- Infrastructure Automation
- Application Migration Factory


Cloud 360° view
Cloud positioning
Cloud provisioning
Cloud realization
Cloud assurance
Cloud portfolio assessment and rationalization
Cloud business models and opportunities
Cloud governments and incentives
Cloud sourcing and procurement
Cloud vendor management and governance
Cloud pricing and ROI
Cloud tax and accounting
Cloud adoption and change management
Cloud standards and interoperability
Cloud architecture and deployment model
Cloud systems and development
Cloud compliance and regulations
Cloud systems and development
Cloud business continuity and availability
Cloud risk and communication
Cloud vision and strategy
Review application landscape – determining commodity vs. strategic business value alignment
Sector by sector thinking on new cloud-enabled industry business models
Economic development support for cloud from around the world
Cloud supplier research, fit, agreements, lock-in and exit strategy
New thinking on SLAs and multi-supplier governance
Cloud business models and pricing models that optimize them
Accounting mgmt. systems, location thoughts and tax characterization
Transition/ transformation program mgmt. Plus new skills and training required
The maturity and adoption of standards and wider challenges for integration of services
Defining your short-, medium- and longer-term enterprise architecture approach
Using cloud platforms for development and new governance associated with this
Adherence to rules and regulations in the borderless world of cloud
Issues around "giving up control" and new trust cultures
Assurance that cloud will support the concerns of continuous operations
What are the key cloud risks and the development of a cloud risk model to help mitigate
Setting the right cloud direction and having appropriate cloud decision-making structure

Cloud Governance Framework

Inputs and Industry Standards

ENISA CSP CERT

Cloud Security Alliance

- The cloud security appliance (CSA) CCM lists key controls and considerations for cloud security
- CAIQ – Consensus Assessment Initiative Questionnaire

FFIEC Handbooks

- FFIEC provides guidance for outsourced cloud computing and directs organizations to leverage the risk management principles outlines in various handbooks

NIST 144 – 145 – 146

- NIST outlines various considerations, guidelines and recommendations for cloud computing

Public Cloud Vendor Leading Security Practices*

- Public cloud vendors (e.g. Amazon Web Services, Microsoft Azure, Google Cloud) publish best security practices for levering their platforms and define a shared responsibility model for security

EBA/EIOPA Outsourcing guidelines

National FSA guidelines

GDPR

National DSA guidelines

EY Cloud Governance Framework

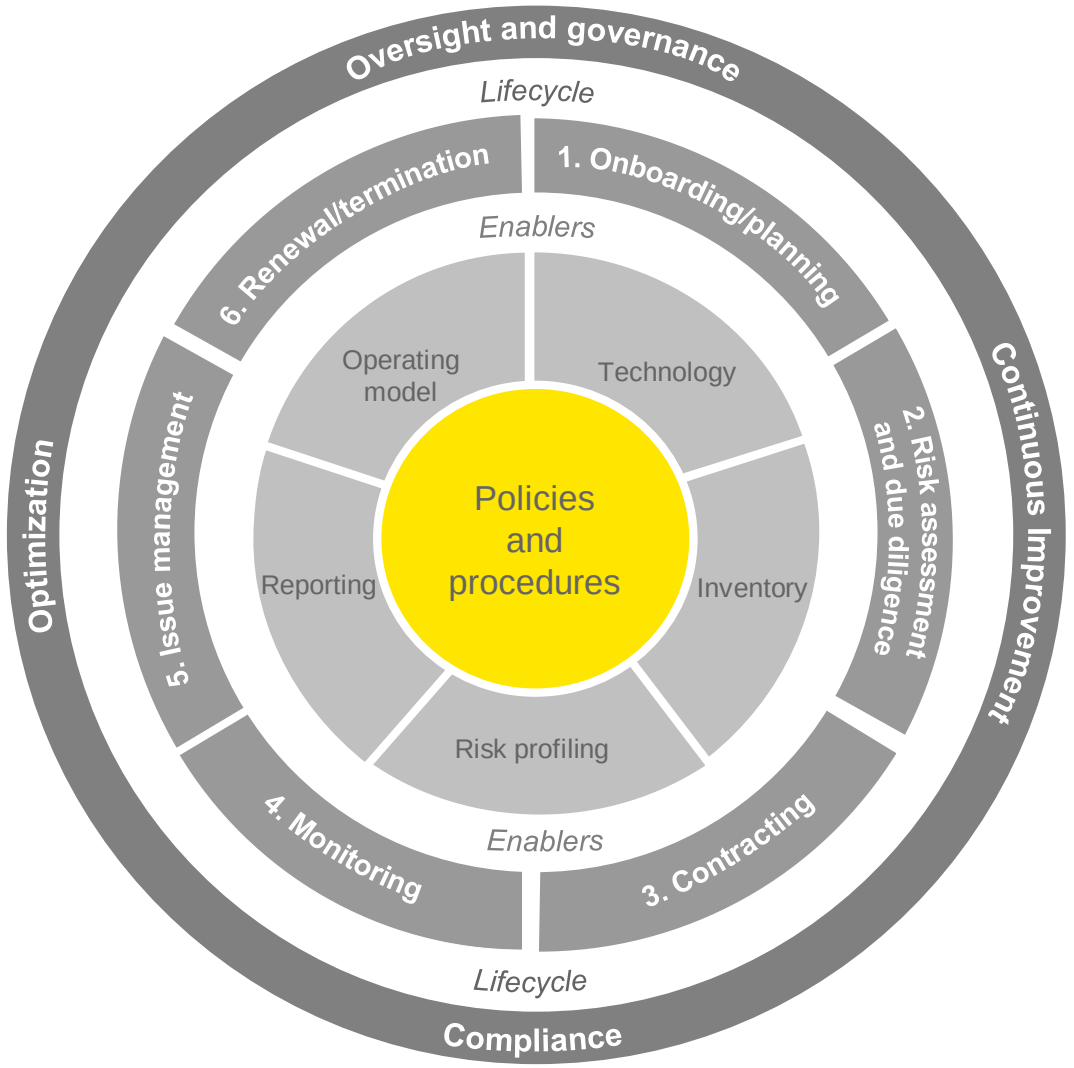
1. Risk, compliance and control
2. Security
3. Data, architecture and infrastructure
4. Finance Management
5. Cloud Service Provider Management
6. Operations

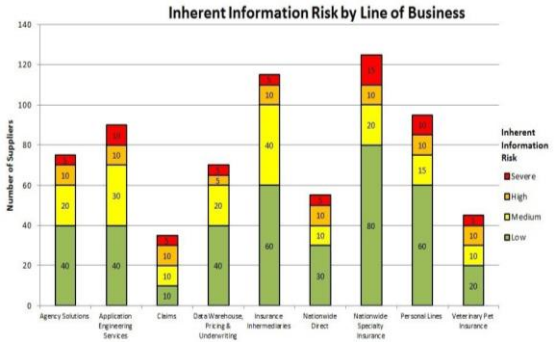
EY Cloud governance framework

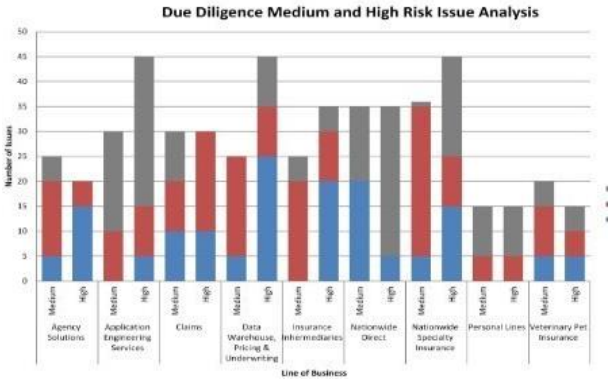
The 7 domains at a high level focus on:

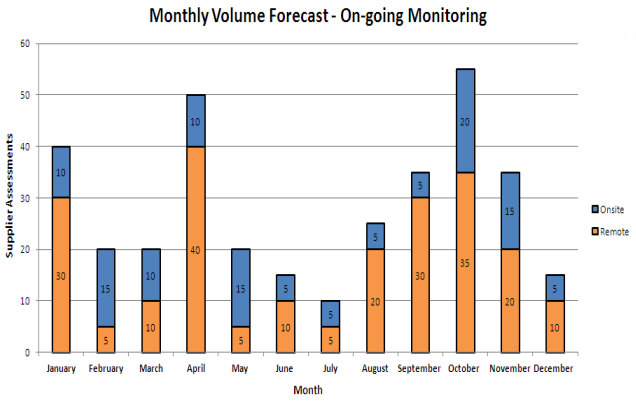
1. **Risk, compliance & control** – Governance and controls to manage, minimize and transfer risk.
2. **Security** – Governance to enable and manage confidentiality, availability and integrity of security operations and controls.
3. **Data, architecture and infrastructure** – Set of principles to support the privacy, confidentiality, availability, integrity and security of data across private and public clouds. Governance to articulate goals of stakeholders through the cloud enterprise architecture.
4. **Finance Management -** Governance around total cost of ownership of cloud services, service consumption and cost transparency.
5. **Cloud Service Provider Management –** Governance to understand accountability for managing cloud services within the organization and establish a framework by which IT and the business have a clear understanding of the performance metrics and contract requirements with cloud vendors.
6. **Operations** - Structured cloud service management and operations mechanism to deliver consistent cloud experience.
7. **Strategy, Resource, Organizational Management and Continual Improvement -** Governance to align improvements to strategy, report corrective actions, resource management and organizational change.

Third Party Risk Management









Example projects

Building a better working world

A few Nordic security related projects as example

New banking app

A “social media” inspired banking channel

Need for agile and fast development without maintaining the infrastructure

Compliance and security was key

Azure

BI functionality

Need for BI and partner integration

Using functionality but keeping data in-house

Large Nordic bank. High formal requirements on security and compliance

ORACLE

Cloud strategy

Options and way of working for 45 countries.

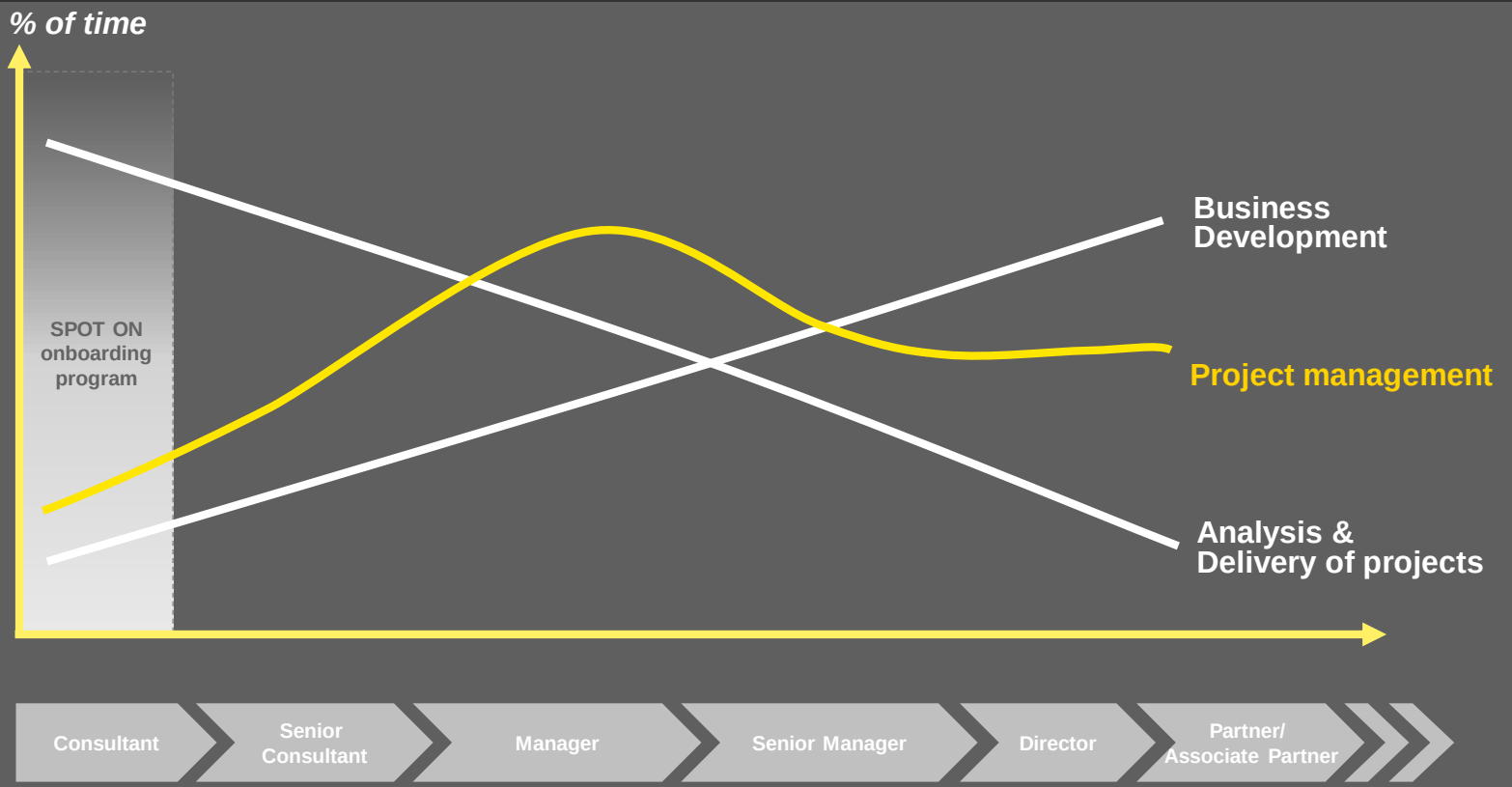
Do´s and don’ts for different legal jurisdictions

Based on EBA guidelines but national view added

amazon web services
Google Cloud
Microsoft Azure

Recruitment and Career Path

Your career at EY follows a clear and performance-based ladder that maximizes your development



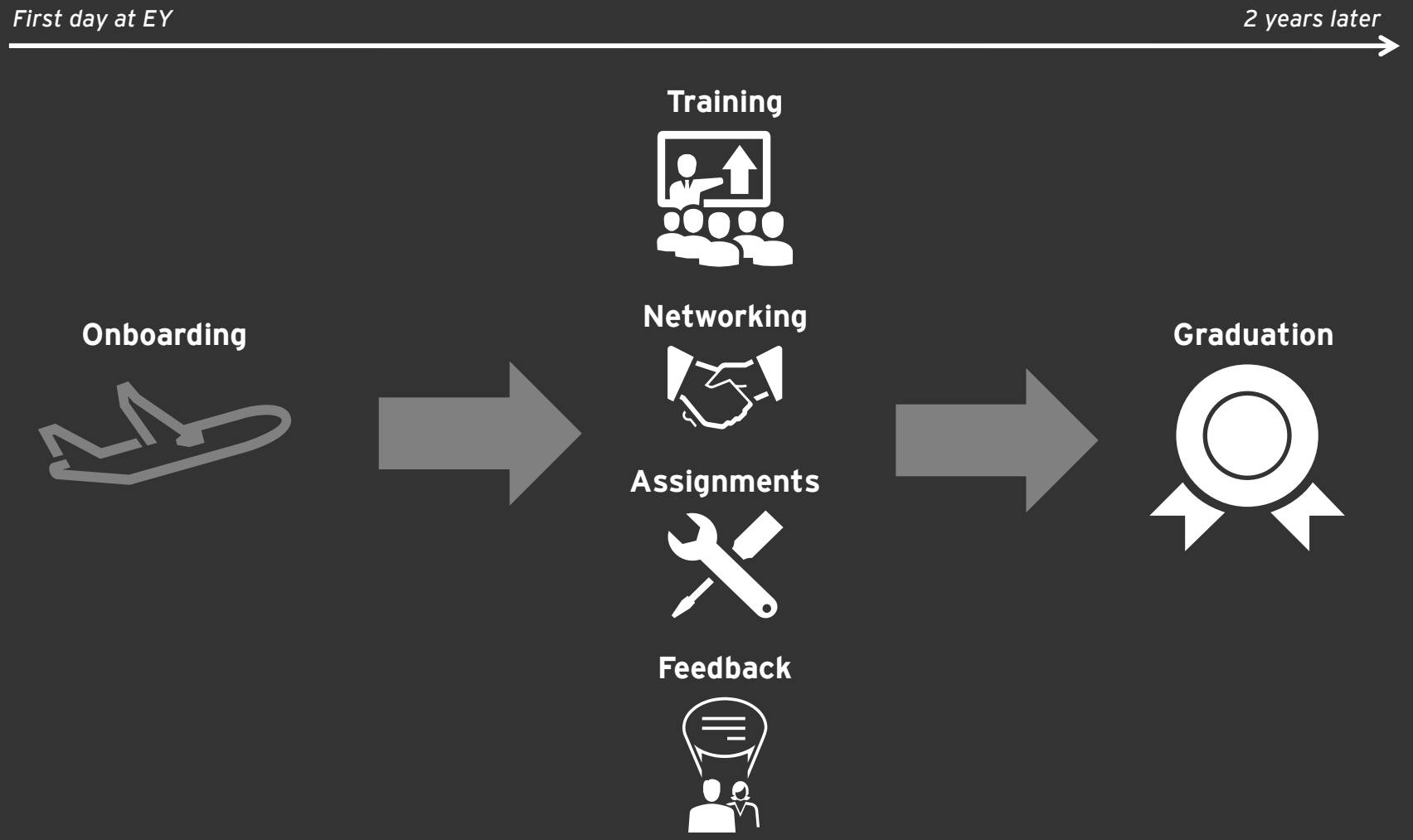
A successful career at EY Advisory Services requires both analytical skills and the ability to make a sustainable impact with clients

We are looking for responsive achievers who are great at working with people and who will thrive in our business

What we are looking for:

Who you are:

All new consultants are given the unique opportunity of the onboarding program SPOT ON from their first day




Q&A

Thank you!

Open opportunitites at EY
Cyber Risk Advisory – Stockholm and Gothenburg
FS Cyber Risk Advisory - Stockholm

Visit our social media sites for more insights into the life as a consultant
https://karriarbloggen.ey.com/
Instagram: eysecareers
Facebook: @EYCareers
Twitter: @EYcybersecurity

Contact us if you have any questions
Fredrik.hertz@se.ey.com
John.a.kibuuka@dk.ey.com