www.pwc.com/ng

The Hypersonic Auditor

October 2020

pwc

What we will cover during this training

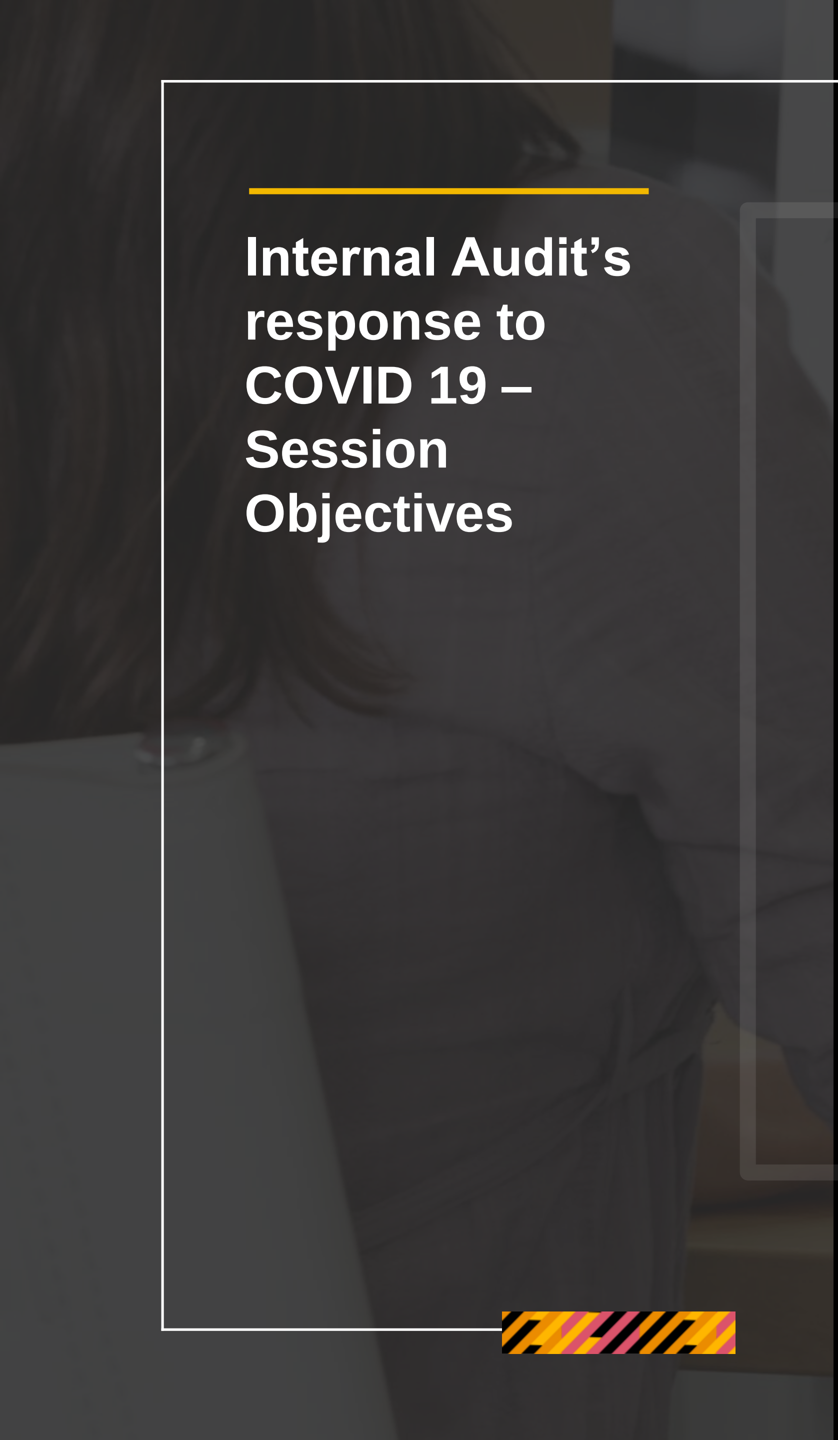
Day	Time	Session
Day 1	9.00 – 9.15am	Introduction to Webex
	9.15 – 9.30am	Opening remarks by ACAEBIN officials
	9.30 - 9.45am	Course welcome and team introduction by PWC
	9.45 - 9.50am	Short Break
	9.50 – 11.35am	Internal audit’s response to COVID 19
	11.35 - 11.50am	Tea Break
	11.50 – 12.20pm	Risk assessment and audit plan development
	12.20 – 12.25pm	Short Break
	12.25 – 1.00pm	Performing a virtual internal audit

What we will cover during this training

Day	Time	Session
Day 2	9.00 – 10.00am	IT Audit and the new normal
	10.00 - 10.15am	Tea Break
	10.15 - 11.00am	IT Audit and the new normal
	11.00 - 11.05am	Short break
	11.05 - 12.05pm	Auditing Cloud Security and Challenges with VPN Infrastructure
	12.05 - 12.10pm	Short break
	12.10pm – 1.00pm	Auditing Cloud Security and Challenges with VPN Infrastructure
	1.00 – 1.15pm	Course wrap-up and close
	1.15 – 1.30pm	Closing remarks by ACAEBIN officials

Internal audit's response to COVID 19

01



Internal Audit’s response to COVID 19 – Session Objectives

COVID 19 emerging risks - Overview

Internal Audit’s Role:

- Risks
- Opportunities

New delivery models and ways to add value

Overview

Background

The ongoing COVID-19 situation presents a substantial challenge for business, Governments and the community.

What does this mean for internal audit?

Immediate actions

- ✓ Ensure the continued safety and care of your team (including regular communication)
- ✓ Revisit the FY20 plan (re-prioritise, add, defer, cancel)
- ✓ Maintain regular contact with your key stakeholders (Chair, C-suite)
- ✓ Provide the required support to the business to respond to current events
- ✓ Consider the impact on FY21 Internal Audit planning

> “ These are challenging times for many of our organisations. Internal Audit have spoken about ‘agility’ and ‘value add’ for a long time. Our businesses need that now more than ever. This is our opportunity.
>
> **Jason Agnoletto**
> National Leader,
> Internal Audit, PwC
> Australia

Where are we?

The year 2020 witness unprecedented crisis in form of Covid-19 affecting most nations of the world. In Nigeria, the government implemented a number of measures ranging from nationwide lockdown, consequently resulting in a decline in economic activities. As the government is gradually easing the lock down measures, we expect a long road to recovery for Nigeria and businesses.

Fragile economy, declining GDP as at Q2 2020

Low revenue, rising debts and budget deficits (FG & states)

High unemployment rate, unequal access to limited opportunities

Insecurity: Boko Haram, kidnapping, ritual killing, internet scams, robbery etc

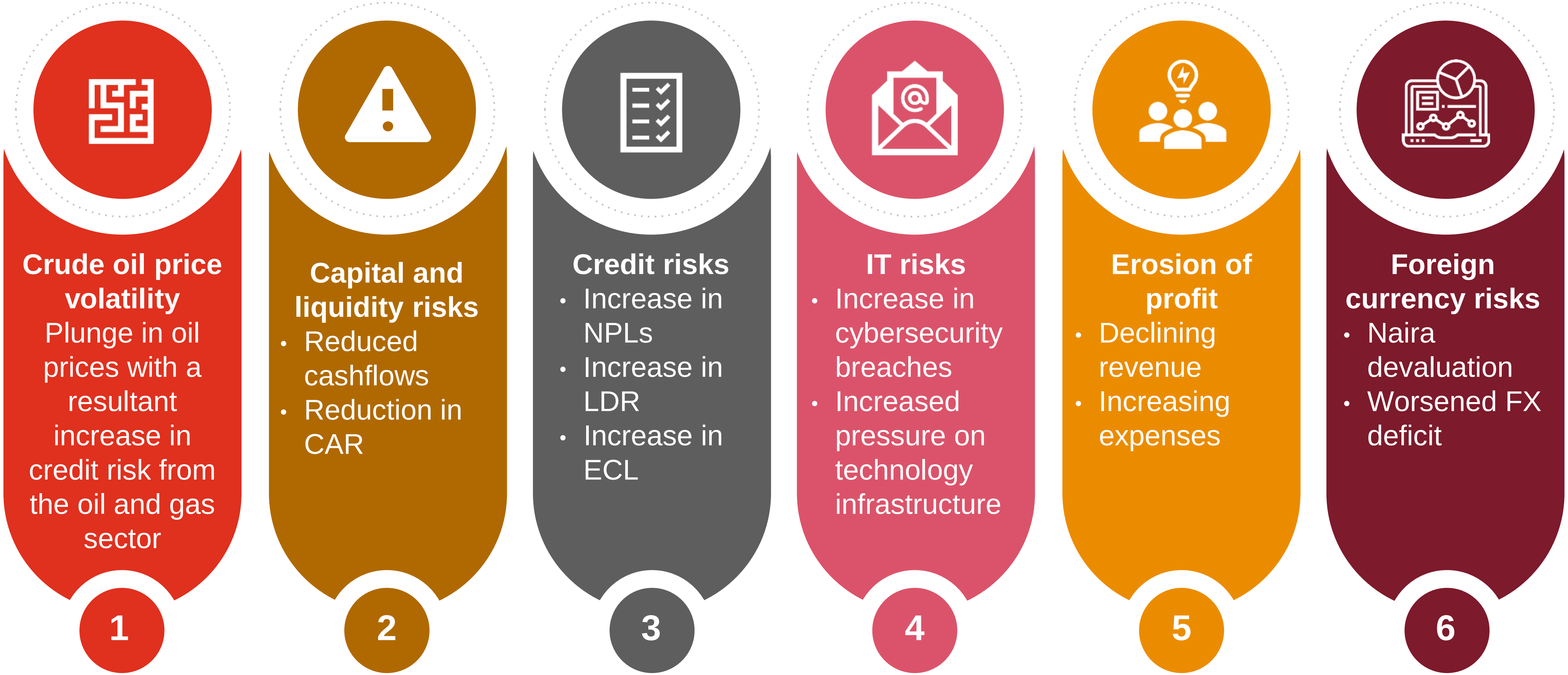
Rising poverty – Nigeria became the poverty capital of the world

Foreign exchange scarcity and devaluation of the Naira

Volatility in oil price and other commodities

Food security concerns

Impact on Nigerian banks



1. Crude oil price volatility

Plunge in oil prices with a resultant increase in credit risk from the oil and gas sector

2. Capital and liquidity risks

- Reduced cashflows
- Reduction in CAR

3. Credit risks

- Increase in NPLs
- Increase in LDR
- Increase in ECL

4. IT risks

- Increase in cybersecurity breaches
- Increased pressure on technology infrastructure

5. Erosion of profit

- Declining revenue
- Increasing expenses

6. Foreign currency risks

- Naira devaluation
- Worsened FX deficit

Major risk impact and priority areas for Banks

Earnings impact

- Reduced earnings due to lower interest rates and drop in economic activities
- Rise in impairment charge and loan restructuring

01

Capital impact

- Increased risk weighted assets
- Decrease in eligible capital due to increased provisioning
- Additional risk exposures

02

Compliance and Policy

- Limitations of systems on compliance and control activities
- Insufficiency of policies, procedures, people and technology

03

Liquidity impact

- Widening funding spreads
- Increased haircut for high quality liquid assets
- Breach in internal and regulatory limits
- Unrealistic behavioural analysis

04

Risk Model

- Internal models failing to capture correlation amongst asset classes
- Internal model assumptions not fit for purpose

05

Reporting Obligations

- Ability to continue meeting regulatory reporting requirements
- Possibility of regulators asking for extraordinary solvency/going concern tests

06

Key considerations as part of risk management strategies

Liquidity and Funding Management

- Monitor deposit fluctuations against your balance sheet strategy.
- Re- validate funding lines.
- Explore different scenarios to model your cash flows for the next few months.
- Assess / revisit existing contracts with counterparties most at risk.
- Redefine stickiness of deposits based on current realities
- Revise stress scenarios often and test extreme possibilities.
- Test your liquidity and funding lines.

Capital Management

- Re-evaluate exposures to material risk areas.
- Evaluate loan restructure requests against your balance sheet strategy.
- Consider how increases in expected losses and accelerated claims will affect earnings.
- Review and revalidate risk measurement and valuation models
- Redefine key risk and early warning indicators.
- Explore different options to cut your costs quickly.

Contingency / Recovery Planning

- Review and expand the scope of contingency plans to ensure organizational resilience.
- Re-examine crisis readiness, run tests, re-examine governance, and streamline decision-making and communication approaches.
- Determine activation and deactivation triggers and review continuity procedures
- Develop/ Update recovery plans.
- Review assumptions driving the value of recovery options
- Validate recovery and contingency plans.

Compliance Management

- Review and refocus the overall Compliance strategy.
- Consider an interim shift from traditional controls testing and towards increased compliance monitoring and surveillance.
- Improve reporting to senior management and the board during the crisis.
- Update policies and increase compliance awareness.
- Automation of Compliance Management function.

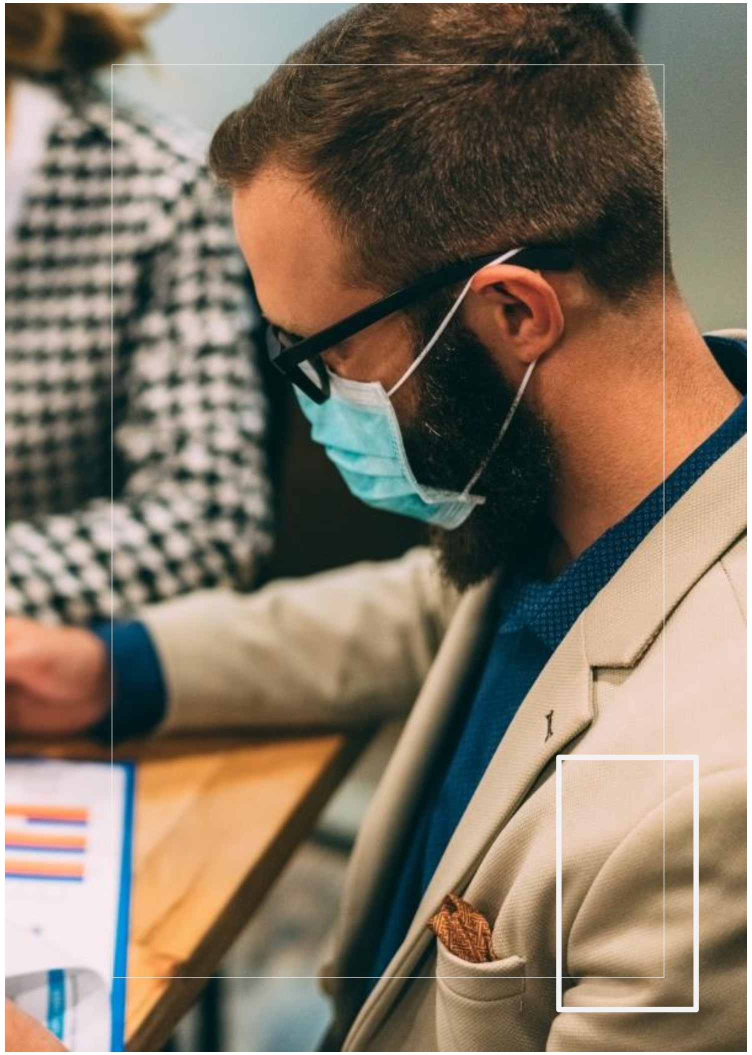
The new normal

Some things have come to stay:

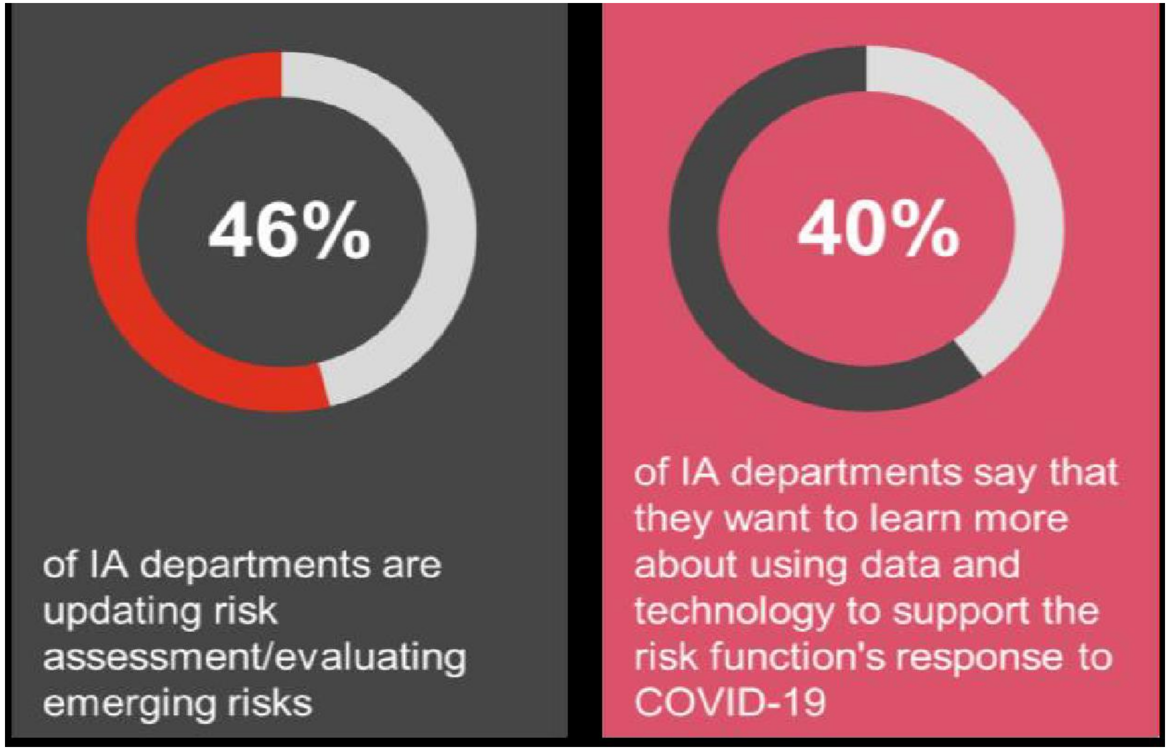
- Remote working
- Video conferencing
- Remote data analysis
- Increase use of digital channels by customers

Some Challenges organizations face:

- Lack of necessary technology and equipment for remote workers
- Lag time for VPN access
- Not enough teleconferencing licenses
- Employees’ home WIFI has low bandwidth
- Security & Secrecy rules
- Strain on supply chain



The role of Internal Audit

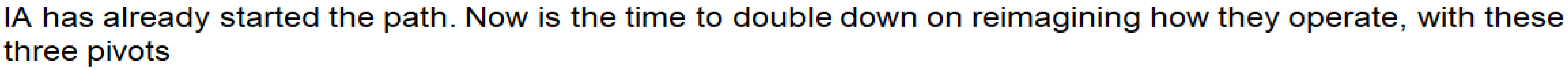


of IA departments are updating risk assessment/evaluating emerging risks

of IA departments say that they want to learn more about using data and technology to support the risk function's response to COVID-19

Source: PwC survey of IA departments, May 2020.

Re-imagining Internal Audit Operations



IA has already started the path. Now is the time to double down on reimagining how they operate, with these three pivots

Pivot 1: Ramp up virtual capabilities, including collaboration

Audit Executive Center's June 2020 Quick Poll indicated that remote working arrangements for internal auditors will continue over the next 12 months, reinforcing the need to ramp up virtual capabilities

Pivot 2: Embrace data and digital operating models

Agile and prepared IA teams were able to easily pivot to more tech-based and data-driven work during the early part of the pandemic

Pivot 3: Let people — not technology — lead the transformation

IA should get ready for upskilling, which challenges long-held beliefs and forces a pivot toward people-powered, business-led, results-oriented program design. The lack of an overall strategy for upskilling your current team may render a potentially valuable analytics ineffective

Internal Audit’s Role: What should IA be focused on?

Protect the business and manage risk

IT Risks	Internal Audit response
Changes to the control environment arising from activation of BCP arrangements Management and governance structures	• Process and control mapping of business critical functions • Review of BCP arrangements
New or elevated cyber security risks Increased use of remote working arrangements	• Incident monitoring and response
Privacy & Data Protection Potential exposure of customer information	• Revisiting data breach policy and practices
Fraud Lapse of key fraud controls and management attention	• Core processes impacted, the potential for fraud and the indicators to look for

What should internal audit be focused on?

IT Risks	Internal Audit response
Remote administration and IT Support Capacity	•Remote worker readiness assessment •Access and Communication Readiness
User Access Controls	•Monitoring controls in place •Detection of fraud risks and management overrides
Cybersecurity risks	•Raise awareness on the heightened risk of COVID-19 themed phishing attacks •Set up strong passwords, and preferably two-factor authentication, for all remote access accounts
Managing Rapid Infrastructure change. Pressure to implement major infrastructure changes in a short period	•Reviewing Policies and impacts by crisis management

What should internal audit be focused on?

Protect the business and manage risk

Other Risks	Internal Audit response
Compliance & Regulatory requirements Maintain compliance and plan for potential interim changes	• Continue to meet compliance/regulatory requirements • Be cognisant of potential regulatory/government enforced changes due to COVID-19: • Extension of moratorium • Interest rate reduction on CBN intervention facilities
Transparency & Employee management Protect employees during uncertainty	• Honouring employees’ entitlements
Risk Culture Consider impact on risk culture across the organisation	• Behavioural impacts of COVID-19

What should internal audit be focused on?

Support the business to deliver

Opportunities	Internal Audit response
Adopt Analytics providing valuable insights and assurance	• Accelerate the deployment of analytics • Increase coverage, focus on outliers
Integrated Assurance Collaborate with other assurance providers	• Work more closely with other assurance providers to reduce disruption to the business • Reduce audit fatigue
Remote auditing Lower expenses, less travels	• Adopt an Audit Management Software • Embrace better work life balance for IA teams
Agile Auditing Iterative planning on an on-going basis	• Encourage flexible, iterative planning on an ongoing basis • Focus on continuous communication among the audit team and with stakeholders
Process review Digitizing processes so information is available	• Advice on controls

New delivery models and ways to add value

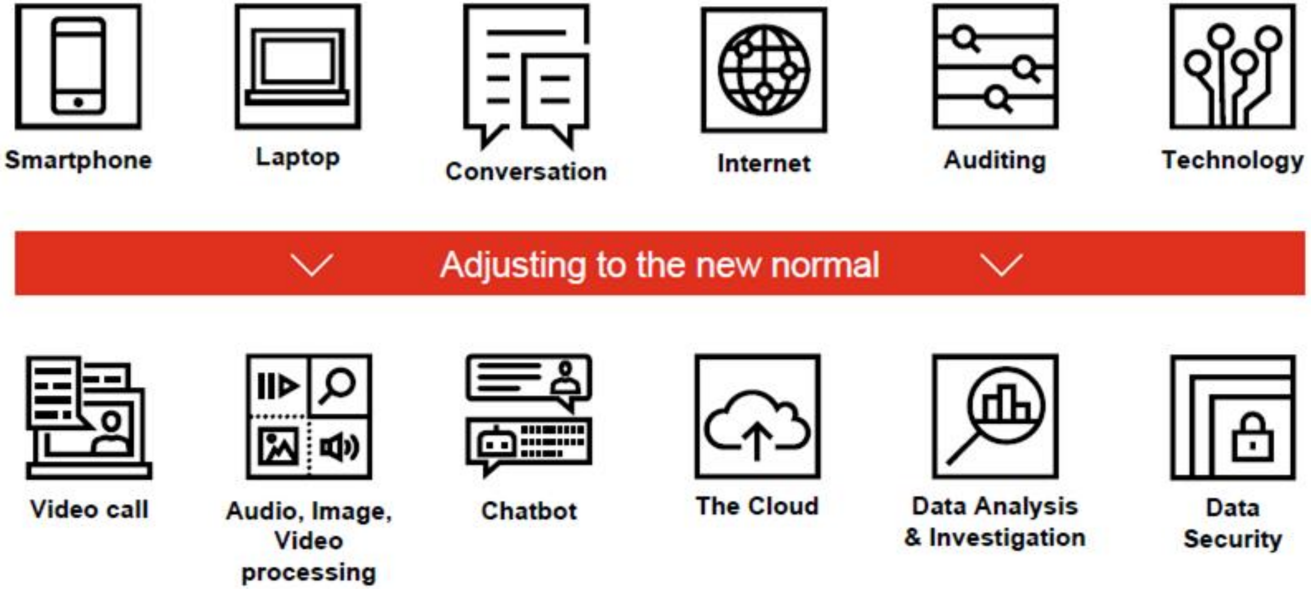
Identify new delivery models and ways to add value and mobilize accordingly

IA Consideration

Prioritize relevance, speed and flexibility—virtually	• Traditional auditing is likely on hold - focus on advisory projects related to crisis • Evaluate how can IA deliver value with reduced resources and/or capacity in virtual environment • Evaluate impact of virtually connected operating model embraced by the business
Encourage innovation through new ways of working that are as flexible as your business can support	• Leverage analytics to drive insights and assurance with less business disruption • Applying analytics and virtual collaboration tools to conduct end-to-end projects. • Relying on self-service for access to data and records.

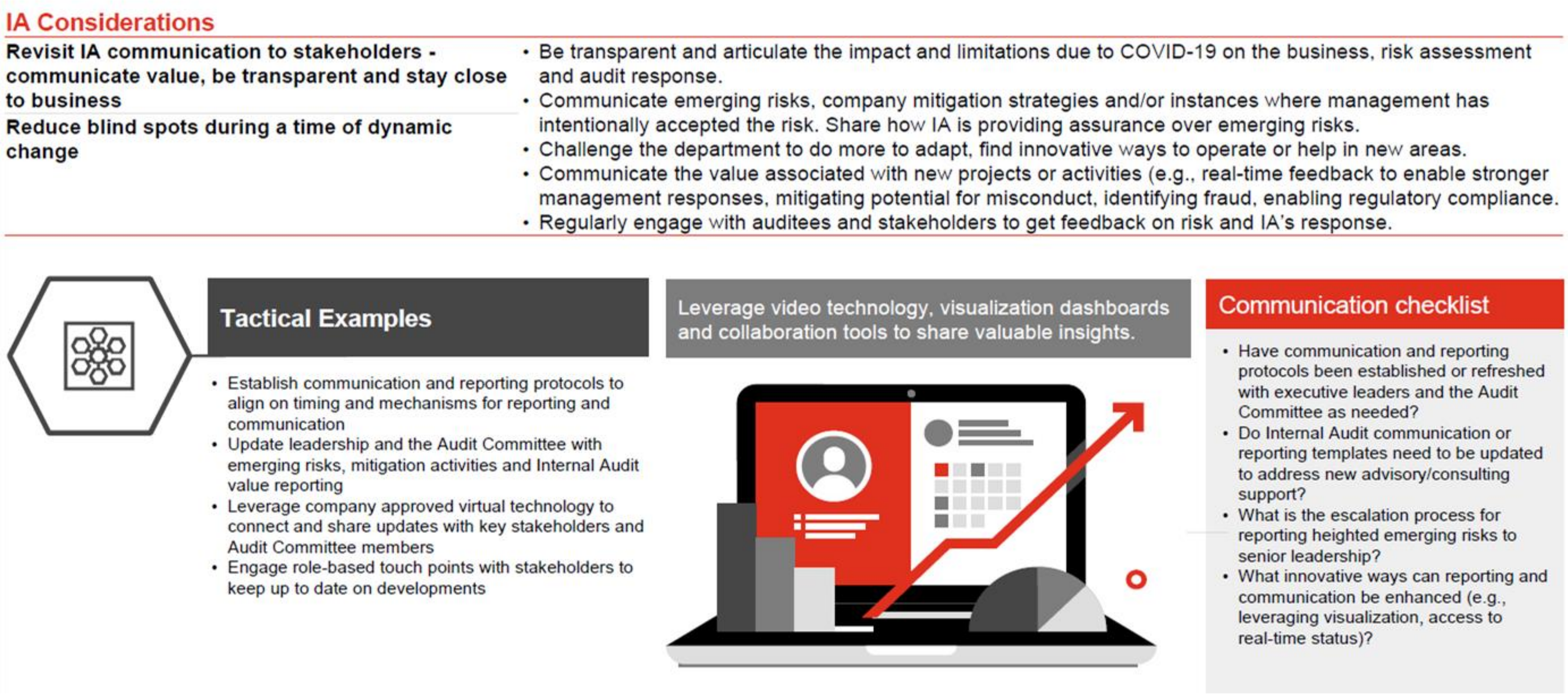
Tactical Examples

- Identify the impact to current audit plan and postpone, cancel audits as necessary and pivot focus to add real-time value through proactive advisory/consulting support. Consider updating communication and reporting mechanisms.
- Assess the most efficient and effective ways to deliver audits using various communication technologies, file-sharing tools, and remote-access mechanisms.
- Use data analytics capabilities throughout the audit to focus on higher risks and provide valuable insights to the business
- Evaluate the impact of the virtually connected operating model embraced by the business.



Communication with Stakeholders

Proactively communicate with management and audit committee stakeholders



IA Considerations

Revisit IA communication to stakeholders - communicate value, be transparent and stay close to business

Reduce blind spots during a time of dynamic change

- Be transparent and articulate the impact and limitations due to COVID-19 on the business, risk assessment and audit response.
- Communicate emerging risks, company mitigation strategies and/or instances where management has intentionally accepted the risk. Share how IA is providing assurance over emerging risks.
- Challenge the department to do more to adapt, find innovative ways to operate or help in new areas.
- Communicate the value associated with new projects or activities (e.g., real-time feedback to enable stronger management responses, mitigating potential for misconduct, identifying fraud, enabling regulatory compliance.
- Regularly engage with auditees and stakeholders to get feedback on risk and IA's response.

Tactical Examples

- Establish communication and reporting protocols to align on timing and mechanisms for reporting and communication
- Update leadership and the Audit Committee with emerging risks, mitigation activities and Internal Audit value reporting
- Leverage company approved virtual technology to connect and share updates with key stakeholders and Audit Committee members
- Engage role-based touch points with stakeholders to keep up to date on developments

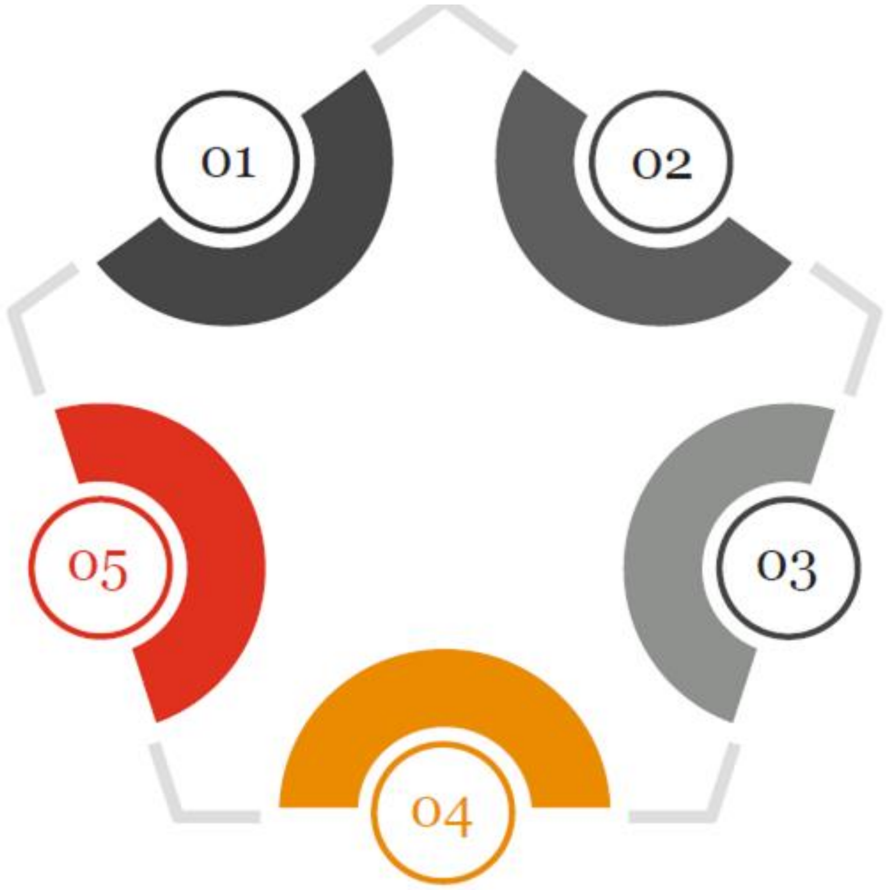
Leverage video technology, visualization dashboards and collaboration tools to share valuable insights.

Communication checklist

- Have communication and reporting protocols been established or refreshed with executive leaders and the Audit Committee as needed?
- Do Internal Audit communication or reporting templates need to be updated to address new advisory/consulting support?
- What is the escalation process for reporting heighted emerging risks to senior leadership?
- What innovative ways can reporting and communication be enhanced (e.g., leveraging visualization, access to real-time status)?

In summary:

Internal Audit should give considerations to the following:



01 Flexible and Remote working capabilities with the right controls in place

02 Operational resilience of middle and back office processes that are manual or require paper based approval

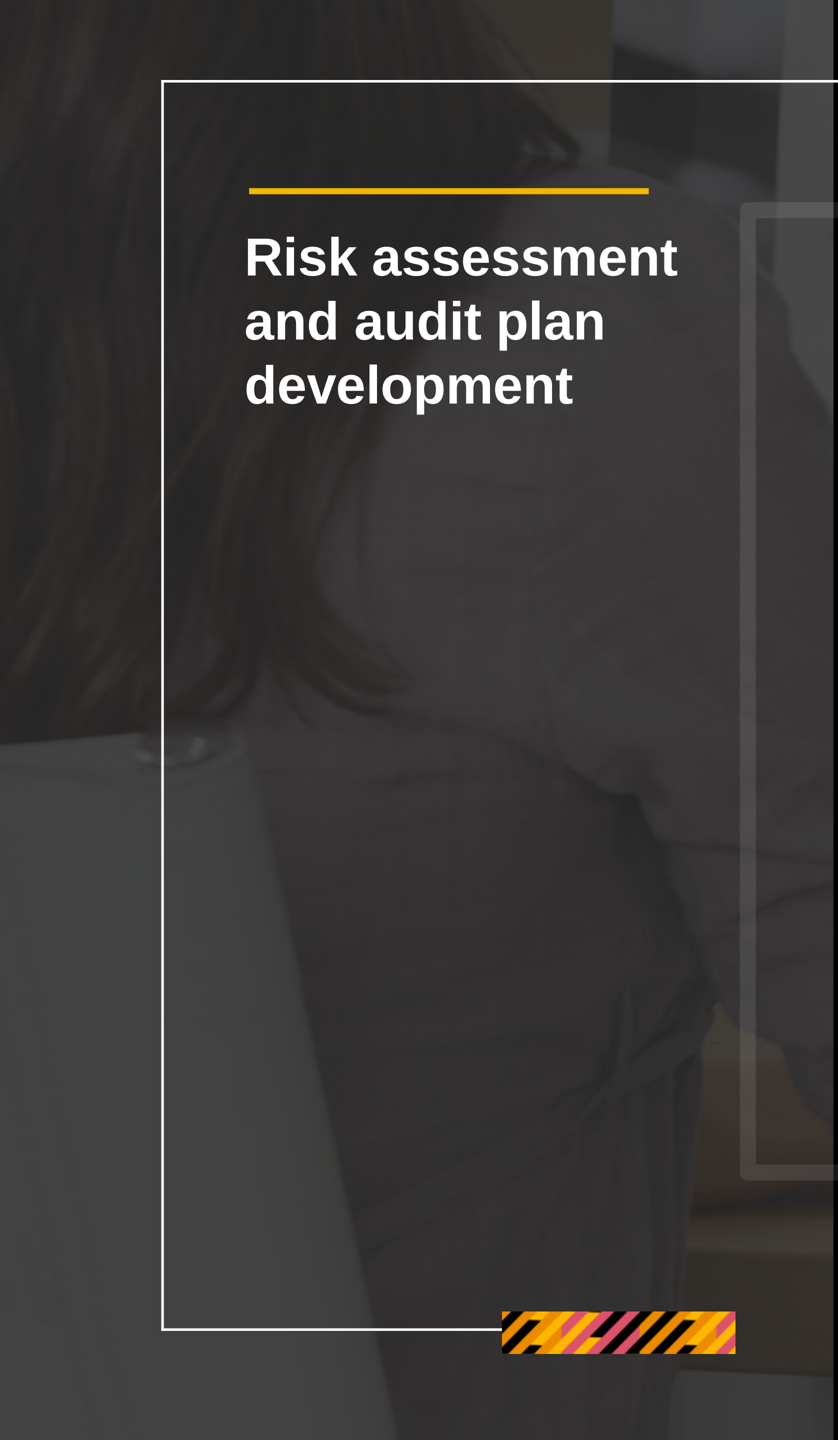
03 Availability of infrastructure and hardware for staff/organisation to execute their duties effectively

04 Cybersecurity breaches, Information security risks, social engineering and fraud incidents

05 Business Continuity Plan Rollout constrained by IT support & services

Risk Assessment and Audit Plan Development

02



Risk assessment and audit plan development

At the end of this session, we would have covered:

- The various steps in the risk assessment and audit plan development stage
- Performing a risk assessment
- Developing and communicating the risk based audit plan

Risk Assessment and Audit Plan Development

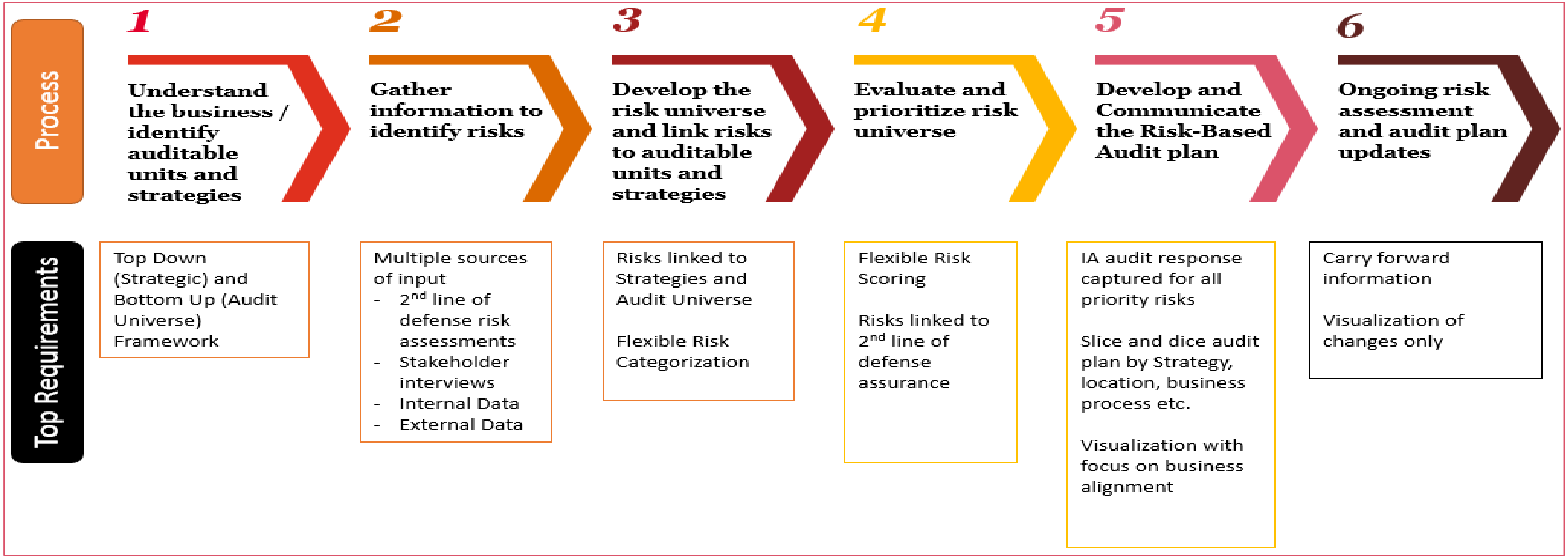
Risk Assessment
Audit Plan Development

Risk Assessment is internal audit’s identification (or validation) and prioritization of the organisation’s risks from Internal Audit’s perspective, independent of other risk assessments done by the business or other assurance functions. The process of formally documenting risks involves thorough understanding of the business, including identification of external trends and insights, and strong stakeholder communication

Audit Plan Development is the activity of internal audit determining the response to the risk assessment. Internal Audit uses the results of the risk assessment to develop a formal audit plan. The process of formally documenting what internal audit is and is not providing assurance over involves an understanding of the historical and current organisational control environment and other assurance activities throughout the organisation.

Risk Assessment and Audit Plan Development

IIA Standards Internal Audit Activity 2000 and Planning 2010 address Internal Audit's participation in the risk assessment activity.



	1	2	3	4	5	6
Process	Understand the business / identify auditable units and strategies	Gather information to identify risks	Develop the risk universe and link risks to auditable units and strategies	Evaluate and prioritize risk universe	Develop and Communicate the Risk-Based Audit plan	Ongoing risk assessment and audit plan updates
Top Requirements	Top Down (Strategic) and Bottom Up (Audit Universe) Framework	Multiple sources of input - 2nd line of defense risk assessments - Stakeholder interviews - Internal Data - External Data	Risks linked to Strategies and Audit Universe Flexible Risk Categorization	Flexible Risk Scoring Risks linked to 2nd line of defense assurance	IA audit response captured for all priority risks Slice and dice audit plan by Strategy, location, business process etc. Visualization with focus on business alignment	Carry forward information Visualization of changes only

Understanding the Business

It is critical that internal audit fully understands the business and reflects this understanding in the risk assessment and audit plan. Any omission of key business characteristics at this stage could mean important risks are not being considered at a later stage, particularly in the audit plan.

1

Understanding the organisational structure

An organisation may have various structures and Internal Audit should understand and consider all of these during the risk assessment.
Examples include legal entities, reporting lines, operational and support processes, geographical spread, and in-house vs. outsourced functions.

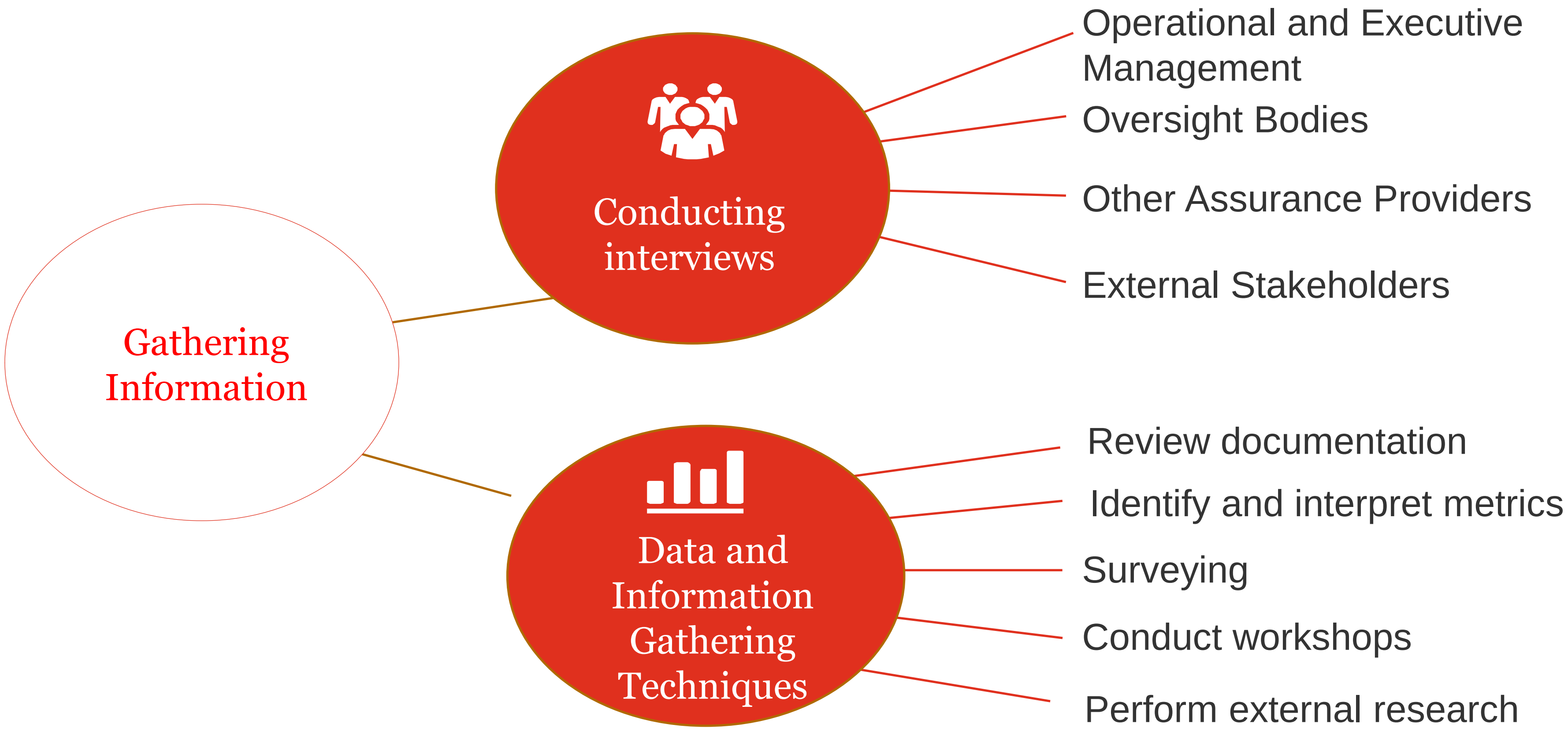
2

Understanding stakeholder expectations

It is important internal auditors refresh their understanding of the landscape of stakeholders in order to effectively manage expectations throughout the risk assessment exercise. This will allow efforts to be focused appropriately and ensure the audit plan is aligned effectively for stakeholders to perceive Internal Audit as adding value.

Gather Information to Identify Risks

This step guides the collection of financial, strategic, compliance, and regulatory information based on the balanced approach (top down / bottom up perspectives).



Gathering Information

Conducting interviews

- Operational and Executive Management
- Oversight Bodies
- Other Assurance Providers
- External Stakeholders

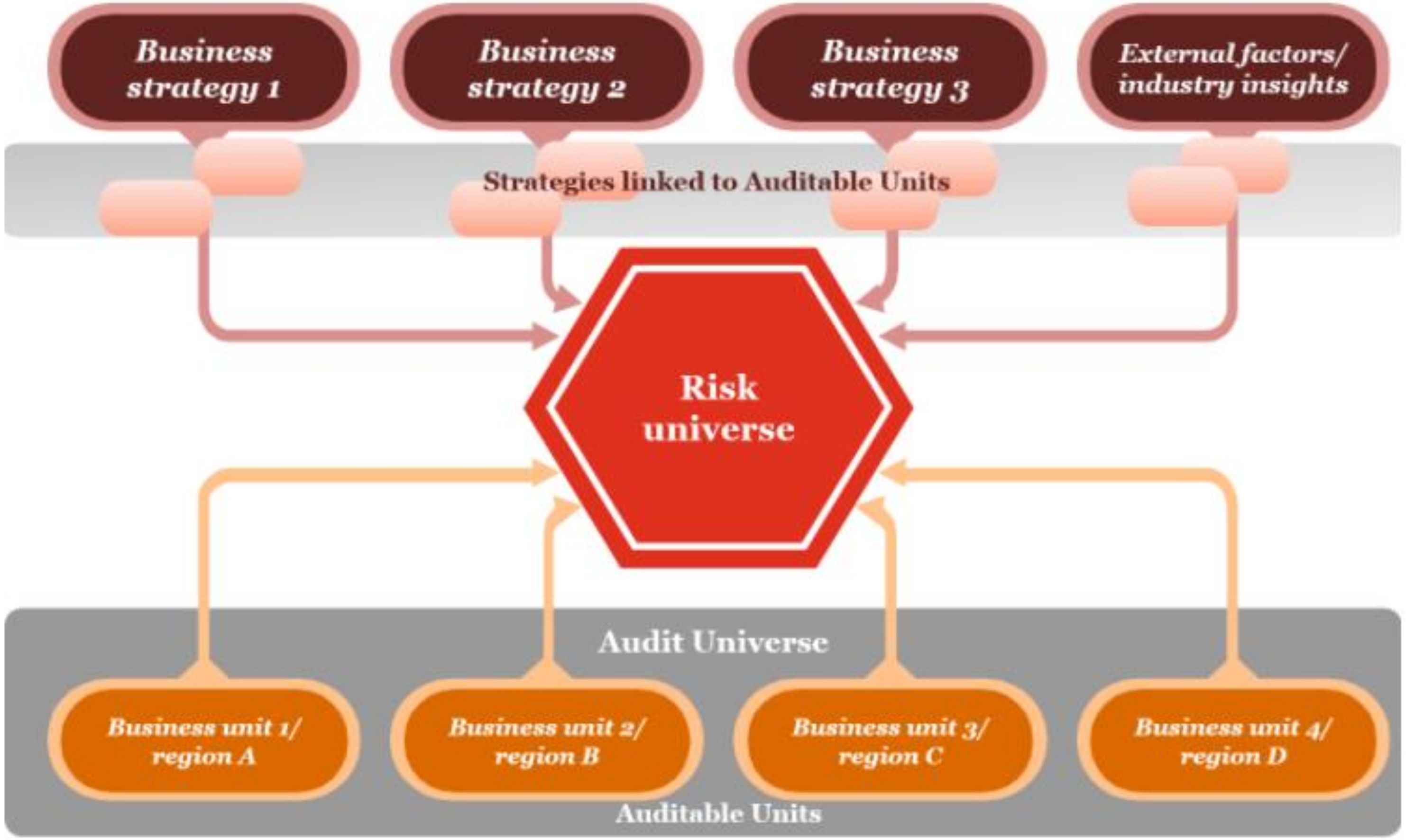
Data and Information Gathering Techniques

- Review documentation
- Identify and interpret metrics
- Surveying
- Conduct workshops
- Perform external research

It is ideal to use these techniques prior to interviews so that relevant data and information can be discussed during the interviews. At a minimum, identifying sources of data and information prior to interviews is advisable to allow for the opportunity to ask for assistance in gathering data with appropriate points of contact.

Develop the Risk Universe

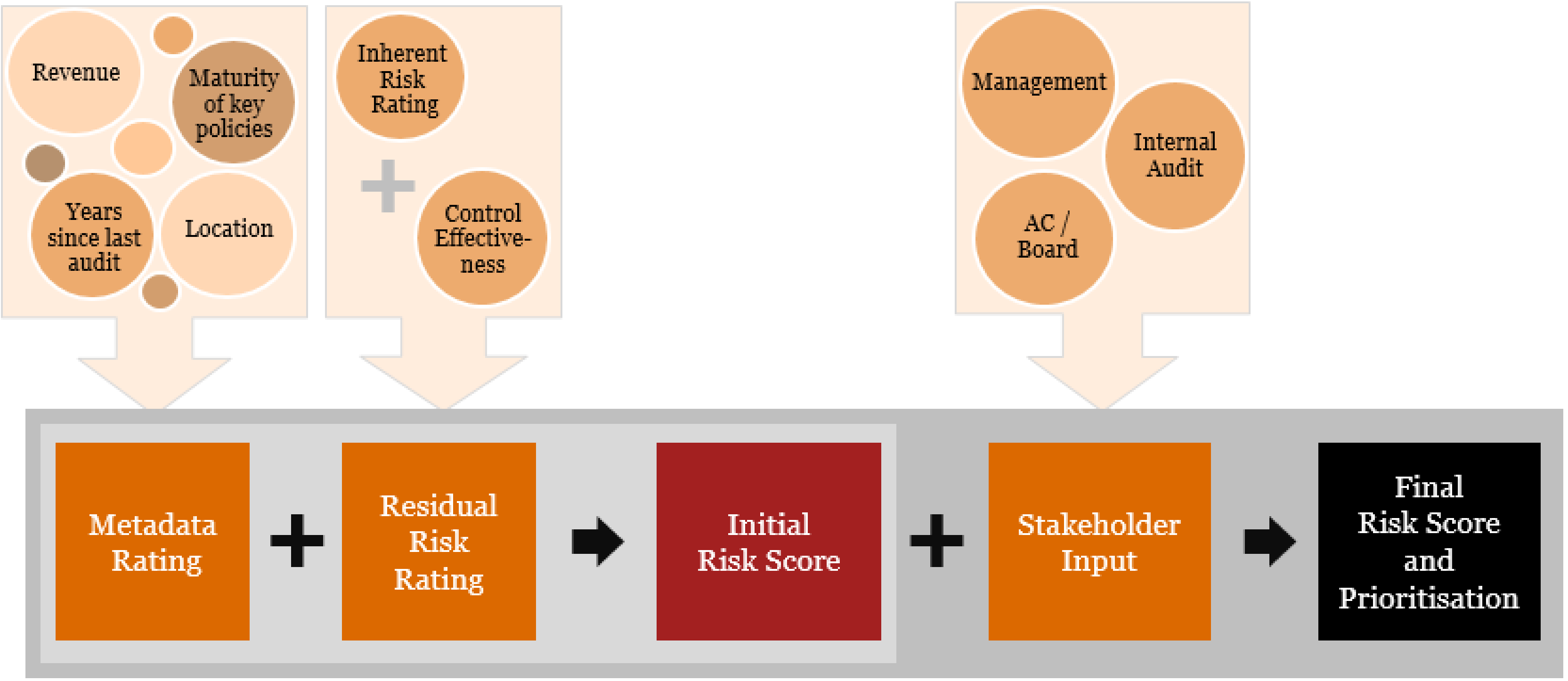
Here you identify risks both from the top down (enterprise perspective) and bottom up (auditable unit perspective) to compile a comprehensive risk universe.


Business strategy 1
Business strategy 2
Business strategy 3
External factors/ industry insights
Strategies linked to Auditable Units
Risk universe
Audit Universe
Business unit 1/ region A
Business unit 2/ region B
Business unit 3/ region C
Business unit 4/ region D
Auditable Units

Evaluate and Prioritise Risk Universe

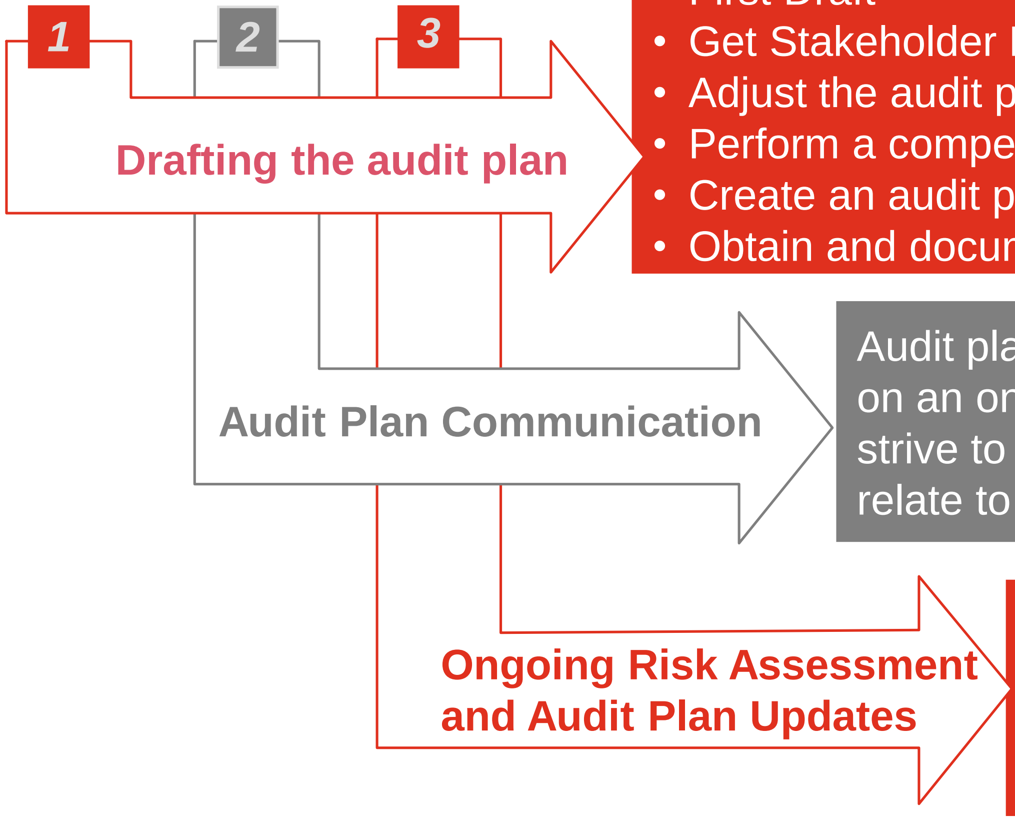
This step involves first rating the risks and then prioritising them based on the relative rating. The ultimate goal of prioritising risks is to develop an internal audit plan focused on key risks.

The outcome of this step is to determine the set of risks that could be in scope for the upcoming audit plan. Those risks with higher priority are most likely to be included in the preliminary scope of the audit plan. This preliminary scope is then used as your starting point for the next step in the process, developing the audit plan.



Develop and Communicate the Risk-Based Audit Plan

This involves both developing and communicating the audit plan, which follows the initial risk prioritization. The output of this step is the final audit plan for the upcoming period, which is communicated to stakeholders and approved by the Audit Committee, Board or equivalent.



Drafting the audit plan

- Audit plan duration
- First Draft
- Get Stakeholder Feedback
- Adjust the audit plan based on stakeholder input
- Perform a competency analysis
- Create an audit plan report
- Obtain and document formal approval

Audit Plan Communication

Audit plan should be communicated to stakeholders on an ongoing basis. Further, internal audit should strive to communicate the audit plan as it would relate to the business or particular stakeholder.

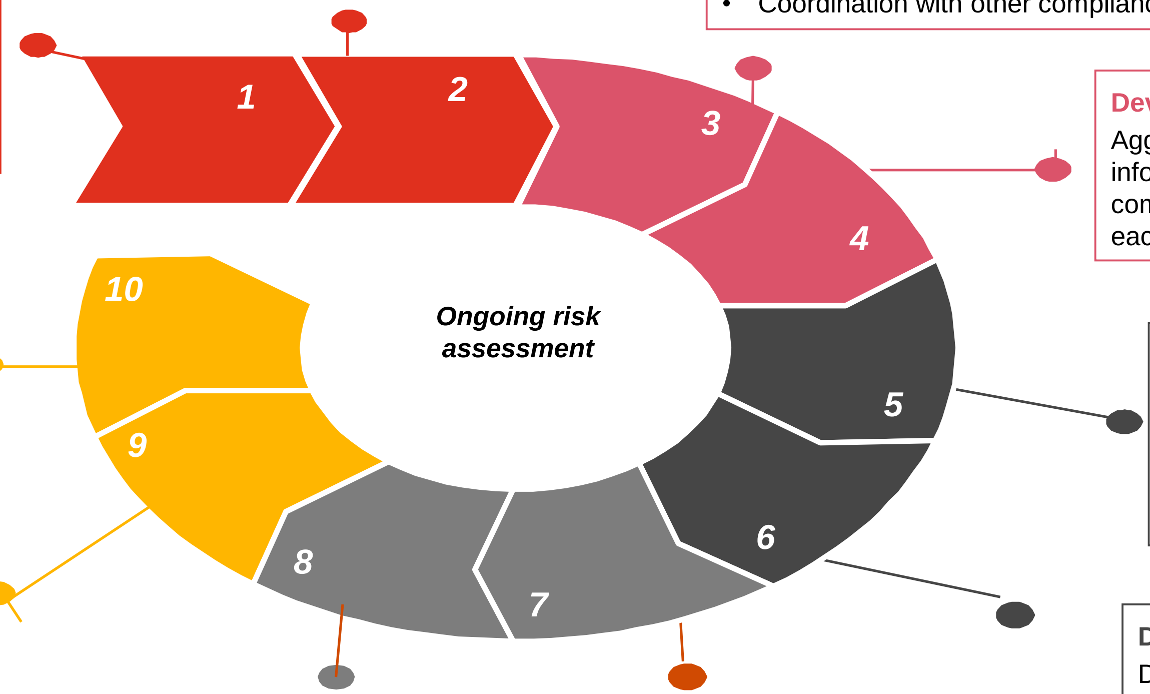
Ongoing Risk Assessment and Audit Plan Updates

Ongoing Risk Assessment

- Frequent Monitoring
- Continuous Monitoring

Audit Plan Changes

Overview of internal audit risk assessment activities



Understand stakeholder objectives
Understand stakeholder's view of Internal Audit's role in helping the organization achieve it's strategic objectives. Gain alignment on internal audit's approach to assess and audit risks.

Identify key risk areas and define audit universe
Understand the company's business and identify key risk areas relevant to ongoing operations and financial performance Audit universe are auditable units within the organization. They could be functions, processes or locations

Gather information
Perform information gathering activities to understand current and future business plans that could impact each risk area. These activities may include:

- Industry research
- Interviews with functional business leads
- Business stakeholder questionnaire
- Review of prior year risk assessment and reports
- Coordination with other compliance functions

Develop risk universe
Aggregate and synthesize results from information gathering activities. Develop comprehensive view of relevant risks within each key risk area.

Evaluate and prioritize risks
Analyze risks and identify the most critical risks threatening the organization's ability to achieve its strategic objectives, now and long term. Incorporate stakeholder views of risk .

Develop audit plan
Develop a plan that is strategically aligned to key business objectives and stakeholder expectations, with a focus on addressing the most critical risks at the right time.

Operationalize the plan
Plan each audit, evaluating risks at the project level to focus the scope. Leverage specialists to deliver specialized audits.

Report
Report on results of internal audit projects and facilitate stakeholders understanding of risk impact.

Perform ongoing monitoring
Periodically monitor performance of IA function and remediation of observations identified through internal audit project.

Continually reassess risk
Continually reassess risk s to determine the impact of environmental changes (internal and external) to the organization's risk profile and audit priorities.

Performing a virtual internal audit

03

Performing a virtual internal audit – Session Objectives

At the end of this session, we would have covered:

Introduction to virtual auditing

Challenges of working remotely

Technology required for virtual auditing

Performing a virtual audit – preparation, planning, fieldwork, reporting, issue management

Conducting a virtual interview

What is Internal Audit?

> “Internal auditing is an **independent**, **objective assurance** and **consulting** activity designed to **add value** and **improve** an organisation’s operations.
>
> It **helps** an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of **governance, risk management and control processes**.”

The Institute of Internal Auditors (IIA)

Types of internal audit

Standard Internal Audits	Internal audit consulting engagements	Investigations and unplanned audit requests	Internal audit follow up	Continuous auditing
Objectives: Provide independent objective assurance over controls in place for risks identified **Examples:** Risk based audits	**Objectives:** Provide advice or consultation **Examples:** Risk management Internal controls	**Objectives:** Investigate a breakdown of controls that occurred **Examples:** Fraud	**Objectives:** Perform additional audit procedures related to previous internal audits **Examples:** Follow up audit	**Objectives:** Analyse control activities as they occur **Examples:** Payroll Order to cash

Introduction to virtual auditing

Remote auditing is not a new concept, what is new is the fact that we are all doing it at the same time

Remote or Virtual audits are audits that are conducted without physical (face to face) interaction. All information are shared virtually.

Things to consider

1. Is the audit suitable for virtual audits
2. Can the engagement plan be adjusted
3. Are stakeholders happy with virtual audit

Challenges of working remotely and solutions

What are some of the challenges we face as auditors when working remotely?

1. Technology breakdown - Internet connectivity issues, laptop failure
2. Light issues
3. Isolation
4. Reduced productivity
5. Communication/collaboration challenges amongst team members
6. Security risks
7. Disconnecting from work
8. Prioritizing work
9. Interruptions

Solutions to challenges of working remotely

1. Invest in a good internet service provider

2. Invest in alternative power supply

3. Working remotely does not mean working alone. Depending on your personality type, you need to find what works best for you. You can also include social breaks on your calendar

4. Avoid multitasking, remove unnecessary distractions and if possible work in short bursts. There are apps that can help you track your productivity

5. Establish an effective communication channel. Emails do not solve this problem. You need something instant and flexible. Examples are google drive, Slack, etc

6. Use of a VPN to connect to the internet securely, installing antivirus on all devices

7. Completing the tasks you set out to do gives you sense of achievement and makes it easier for you to disconnect at the end of the day. In addition, you can set up an appointment on your calendar for end of day

8. Do the most important task first.

9. Have your own workspace at home and as much as possible have a schedule and stick to it

Things to continue doing:

1. Obtain sufficient appropriate audit evidence
2. Perform effective review and supervision of audit work
3. Be available to your team and auditees
4. Comply with all relevant information protection policies
5. Maintain the appropriate degree of information confidentiality, privacy and security.

Technology required for virtual auditing

1. Stable and secure Internet connectivity
2. Good working laptop
3. Uninterrupted power supply
4. Secure collaboration tools

Tips for working remotely

- Align your working hours to normal business hours as much as possible.
- Be available.
- When you're sick, take a sick day.
- Mute your phone while on a call until you are speaking in a meeting, or if there is a possibility of background noise.
- Shut down your laptop when you are done working. Especially when working at home, it can be easy for work and personal hours to blend.

Tips for staying productive while working remotely

1. Create a workspace

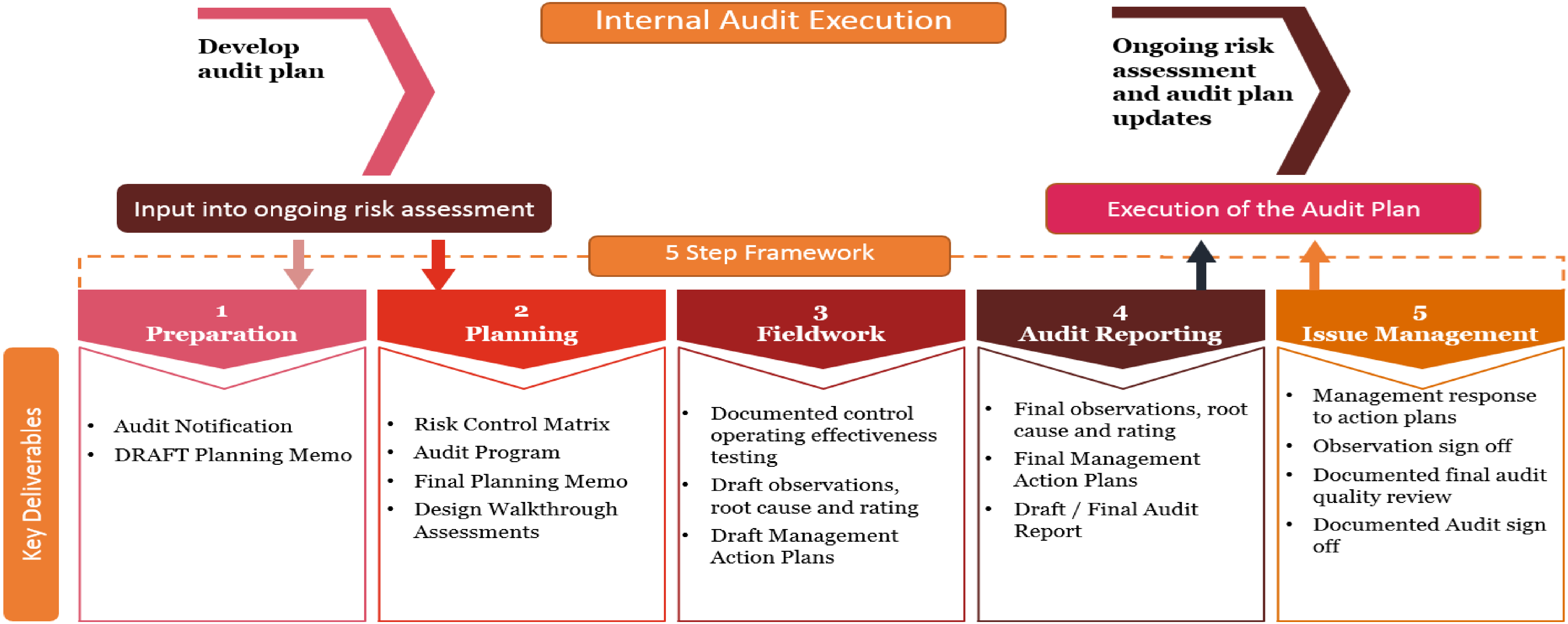
2. Give yourself breaks throughout the day.

3. Set clear boundaries with your family and friends about your working situation.

4. Don't let technology and social media interfere with your daily job responsibilities

Performing a virtual audit

The Execution stage sets out the requirements for delivering high quality internal audit services that meet stakeholder expectations and add value to the organisation. The five steps are preparation, planning, fieldwork, audit reporting and issue management.



Develop audit plan

Internal Audit Execution

Ongoing risk assessment and audit plan updates

Input into ongoing risk assessment

Execution of the Audit Plan

5 Step Framework

Key Deliverables

1 Preparation

- Audit Notification
- DRAFT Planning Memo

2 Planning

- Risk Control Matrix
- Audit Program
- Final Planning Memo
- Design Walkthrough Assessments

3 Fieldwork

- Documented control operating effectiveness testing
- Draft observations, root cause and rating
- Draft Management Action Plans

4 Audit Reporting

- Final observations, root cause and rating
- Final Management Action Plans
- Draft / Final Audit Report

5 Issue Management

- Management response to action plans
- Observation sign off
- Documented final audit quality review
- Documented Audit sign off

Step 1: Preparing the Audit

Considerations for a virtual audit

1. Obtain support from the auditees for the virtual audit

2. Ensure availability of enabling technology

3. Obtain approval from the audit committee and the Managing Director to conduct a virtual audit

4. Obtain access to data

Step 1: Preparing the Audit

Preparation of the audit is the first step in the audit process. The primary purpose of preparation is to communicate the intent to audit and to confirm scope.

Key preparation tasks

1. Understand and confirm audit objective and scope
2. Coordinate logistics
3. Identify and confirm audit resources
4. Establish project milestones
5. Communicate responsibilities and assignments
6. Establish a feedback process

Key preparation deliverables

1. Audit notification
2. Documentation request list
3. Draft planning memo

Step 2 - Planning

Planning is the project initiation step where much of the fact-finding effort occurs, including all research, coordination with the second line of defense, and gathering of business intelligence.

Key tasks of the Planning step include

- Conduct Kick-Off Meeting
- Provide Initial Documentation Request List
- Conduct Fact Finding
- Confirm Risks
- Identify Controls
- Perform Design Walkthroughs
- Finalize Scope and Audit Program

Key tasks of the Planning step include

- Risk & Control Matrix
- Audit Program
- Design Walkthrough Assessment
- Final Planning Memo

Establishing engagement objectives

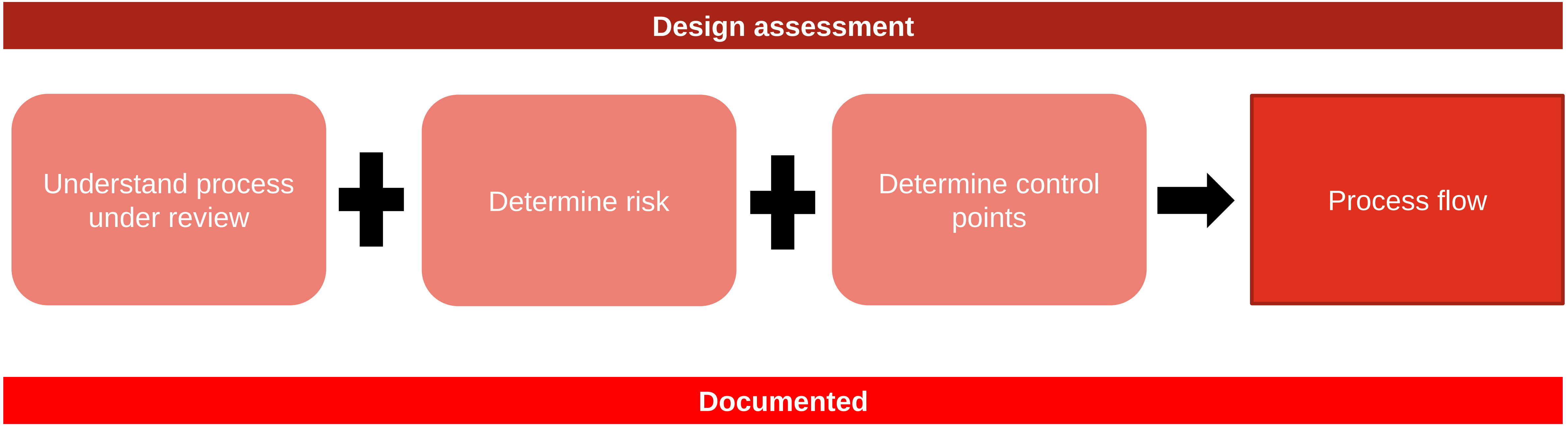
- During the planning phase, the objectives of the engagement should be clearly established and documented

- Engagement teams should leverage the details outlined in the planning memo drafted during the preparation phase when completing this activity.

Perform Fact Finding

The level of detail for an internal audit risk assessment will vary by client. It is important to understand the risks identified or reason this area was included in the audit plan during fact finding. Linking fact finding back to the risk assessment will better ensure the audit work program focuses on the priority risks and adds the most value to the organization. If there is not enough detail in the risk assessment, the fact finding phase needs to be more extensive to identify the priority risks and audit focus.

Design Assessment



Design assessment

Understand process under review

Determine risk

Determine control points

Process flow

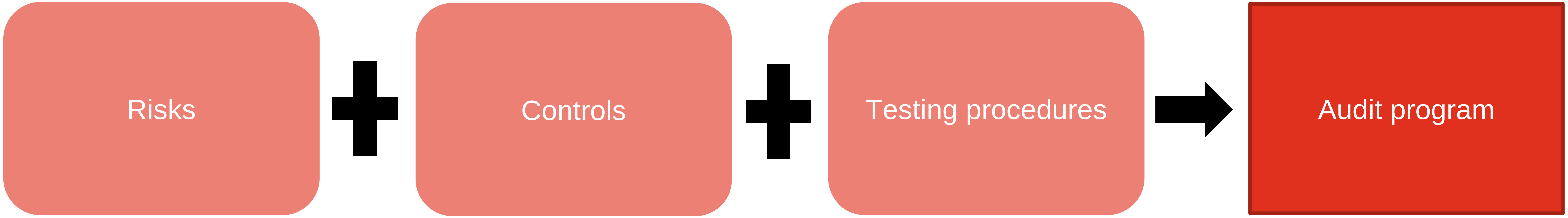
Documented

- Helps audit team gain understanding of process under review
- Determines where risk and controls points exist
- Documents design assessment using process narrative and/or process flow format

Audit program

The audit program is a key document that is created during the planning step but completed during the Fieldwork step

Audit program

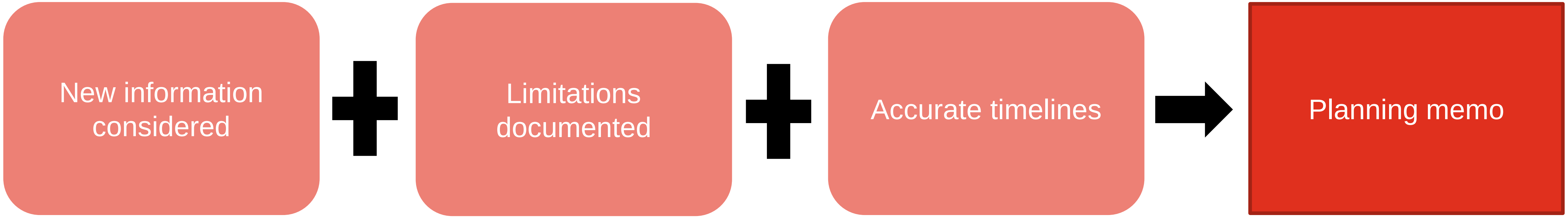


Risks + Controls + Testing procedures → Audit program

Documented and Reviewed

Planning memo

Planning Memo



New information considered

Limitations documented

Accurate timelines

Planning memo

Documented and Reviewed

The importance of the planning memo.

- Ensure any new information learned during fact finding and design walkthroughs that might alter the scope are considered
- Ensure any limitations are documented
  - ○ Key data or stakeholders are not available
- Ensure timelines for all phases are accurate

Step 3 - Fieldwork

Considerations for virtual audit

1. Access to data required for the audit should be provided. It can be read only
2. Collaboration with the second line of defence
3. Provision of a collaboration platform for document sharing
4. Discuss issues and get clarification real time

Step 3 - Fieldwork

Planning is the project initiation step where much of the fact-finding effort occurs, including all research, coordination with the second line of defense, and gathering of business intelligence.

Key tasks of the fieldwork step

1. Document Operational Effectiveness Testing
2. Analyze Conclusions & Observations
3. Perform Quality Review Workpapers
4. Management Administrative Items (Status Meetings, Project Plan Monitoring)
5. Coordinate Testing Results & Issues
6. Conduct Closing Meeting

Key tasks of the fieldwork step

1. Process Narratives, Flowcharts & Test Scripts
2. Completed and Reviewed Working Papers
3. Completed and Reviewed Risk & Control Matrix
4. Completed and Reviewed Audit Program
5. Draft Observations and Recommendations

Operational Effectiveness Testing

Operational effectiveness means that the controls are functioning as designed on a consistent basis over the period under examination. Regardless of the approach used, the audit team will need to determine the appropriate sample size to assess operating effectiveness.

Sampling for testing during an internal audit is subjective and based on auditor judgement.

Data Analytics

By leveraging analytic tools and techniques, auditors may be able to replace traditional sampling procedures, and instead, test the whole population to target outliers using a risk-based approach

Controls Testing

Control testing assesses design issues, the auditor evaluates whether the control steps performed by management have been properly designed to prevent or detect unfavorable impacts to the organization as a result of weakened or ineffective controls (e.g., material misstatements).

Substantive Testing

Substantive testing assesses activities performed by management to detect errors or departures from established processes or procedures. There are two categories of substantive tests - analytical procedures and tests of detail.

Approaches include:

- Confirmation
- Physical Examination
- Inquiry
- Observation
- Cut-Off Testing
- Tracing/Vouching

Documenting & Drafting Operational Effectiveness

Finding/Observation Analysis

When analyzing a finding or observation, the audit team should consider:

- The potential effect of the objectives of the control.
- The significance and impact of the finding.
- Whether the issue is recurring.
- Is there a broader risk associated with this control as it relates to the process as a whole?

Determine Root Cause

Common factors that cause control breakdowns include people, systems, organizational culture or unexpected events. Whatever the cause, it is important that the audit team determine why the breakdown occurred and if this breakdown still exists and/or could recur.

People – competency, skill gap, human error, demand on time or deliberate fraudulent acts.

Systems – configuration, security, suitability, stability or functionality

Internal environment – management culture, working conditions or performance pressures

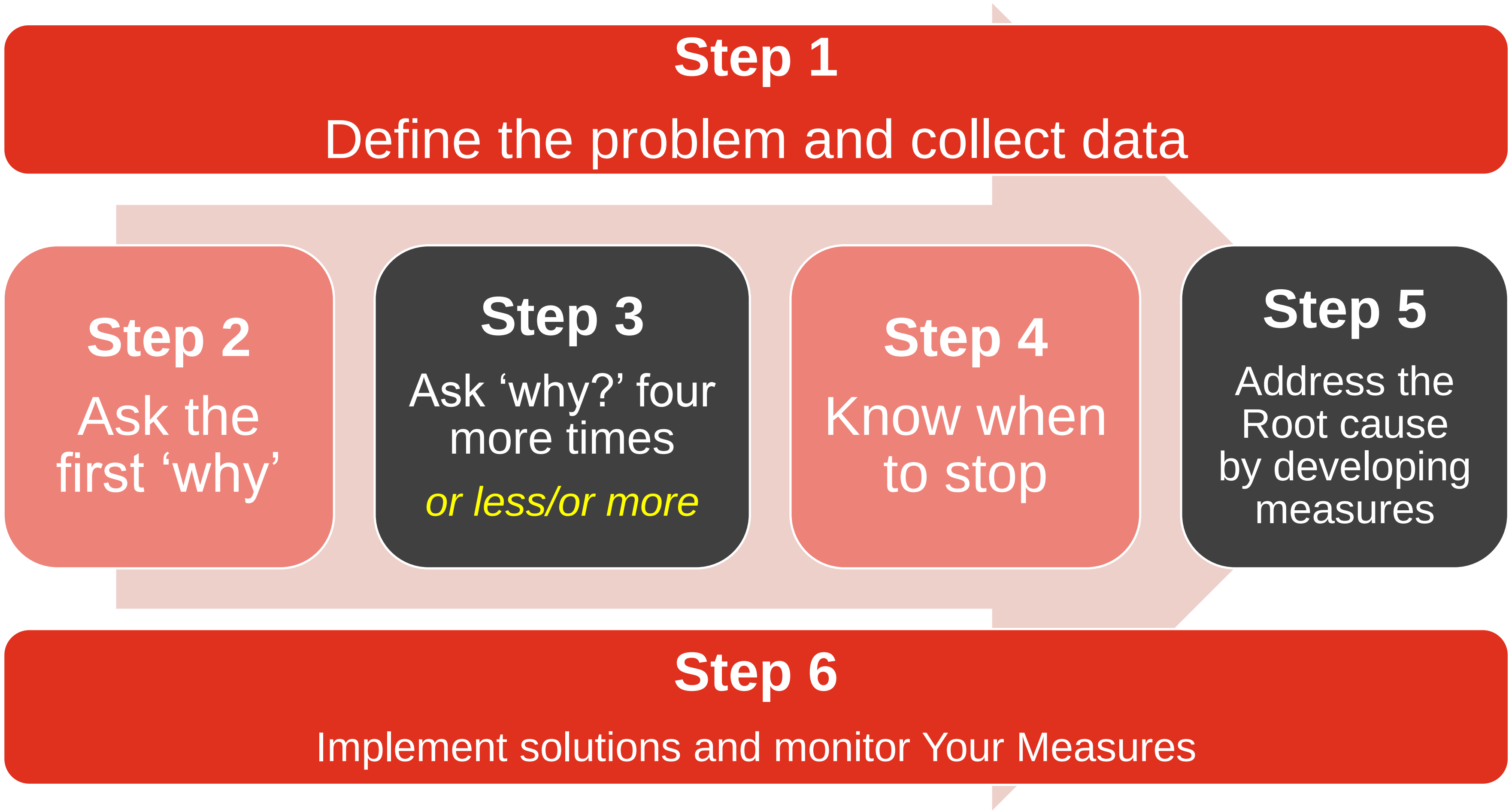
External factors – right relationships, unexpected events, regulatory environment or economic factors

Classify Findings & Observations

When determining the rating for a finding, the internal audit team should assess the severity of the issue by considering the probability of occurrence and significance of impact.

Performing root cause analysis – the 5why model

- **Identifying root causes** of known performance gap or deficiencies **is vital** to business process improvement.
- **Distinguish the problem from its symptoms** - examine all the issues and identify the ones that are key drivers of the problem.
- Successful application of root cause analysis **should result in elimination of the problem**



Step 1

Define the problem and collect data

Step 2

Ask the first ‘why’

Step 3

Ask ‘why?’ four more times

or less/or more

Step 4

Know when to stop

Step 5

Address the Root cause by developing measures

Step 6

Implement solutions and monitor Your Measures

Remember - Successful application of root cause analysis should result in elimination of the problem!

Closing Meeting

Upon completion of an audit, at the end of Fieldwork, a closing meeting, or exit meeting, is an important activity

During this meeting, the final results of the audit should be presented and the audit team should discuss all observations and findings noted during the audit to ensure agreement with the client.

Remediation plans should also be discussed and agreed upon for each finding.

Any observations or findings noted during the audit should be discussed with the client on a real time basis so there are no surprises at the closing meeting.

Closing the audit

A closure/ exit meeting should be held to discuss the results of fieldwork. The closure meeting should be attended by the primary auditee and the team manager and used to formally present the documented findings.

The purpose of the closure meeting is to:

- Allow the auditee to discuss and comment on the conclusions arrived at during fieldwork, including any findings and potential risks that arise as a result
- Provide an opportunity to address any gaps in testing execution or request additional procedures
- Discuss options for practical recommendations to address the risks
- Prevent surprises when the draft report is issued

Step 4 - Reporting

Key reporting tasks

1. Finalize Observation and Recommendations
2. Finalize Management Action Plans
3. Finalize Audit Report
4. Perform Quality Review of Workpapers

Key reporting deliverables

1. Process Narratives, Flowcharts & Test Scripts
2. Completed and Reviewed Working Papers
3. Completed and Reviewed Risk & Control Matrix
4. Completed and Reviewed Audit Program
5. Draft Observations and Recommendations

The audit report is a key deliverable as a result of the audit performed and it is critical that the report be high in quality, accurate and visually impactful.

Key reporting sections:

1. Executive summary
2. Background
3. Scope
4. Findings and observations
5. Management responses
6. Risk rating definitions, if applicable

Step 5 – Issue management

Key tasks of the issue management step

1. Monitor & Validate Management Response to Action Plans
2. Sign-off of Observations
3. Final Sign-off on Audit Documentation

Key tasks of the issue management step

1. Closed Corrective Action Plans/Ongoing Issue Monitoring Status Reports
2. Document Final Quality Review
3. Client Survey Feedback & Report

Monitoring & Validating Management Actions

- Ensure the responses provided by management for each finding are completed in a timely manner.
- Each response should have a due date for implementation.
- After that assigned date, the internal audit team must follow-up with the issue owner according to the issue remediation protocol to determine whether the finding was fully remediated. Documentation may be requested to validate completion.
- Status of findings are regularly communicated to management and oftentimes the audit committee.
- Any delays should be explained in this communication.

Conducting a virtual interview

Tips for conducting a virtual interview

Meeting management

State the purpose and objective of the interview

Check in with participants to ensure that they are following

Recap key points at the end of the meeting

Don’t assume the technology works

Ensure you have backup plans if the technology were to fail in the middle of your meeting/interview.

Also ensure its working

Meeting duration

Respect the time of all present

Confirm time commitment at the start of the meeting

Notes taking

Have someone that is responsible for taking notes during the meeting

If possible record the meeting but ensure you obtain permission first

Eliminate background noise

We are all working from home but as much as possible we should to reduce this to the barest minimum

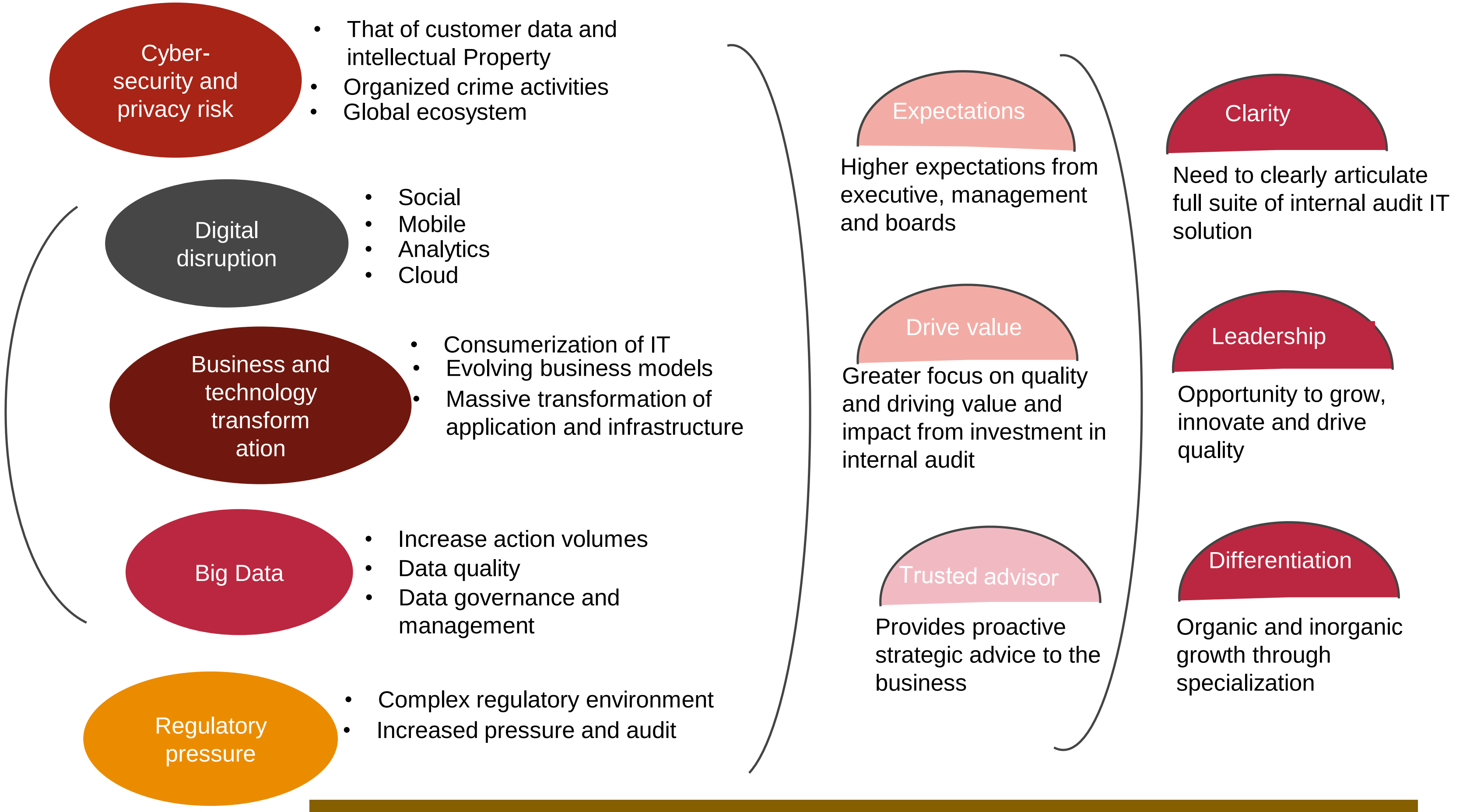
Prepare for the meeting

Prepare interview questions ahead of the meeting/interview

The Role of IT Audit in New Normal

04

Technology disruption is resulting in increased expectations of Internal Audit



Key Trends

Cyber-security and privacy risk

- That of customer data and intellectual Property
- Organized crime activities
- Global ecosystem

Digital disruption

- Social
- Mobile
- Analytics
- Cloud

Business and technology transform ation

- Consumerization of IT
- Evolving business models
- Massive transformation of application and infrastructure

Big Data

- Increase action volumes
- Data quality
- Data governance and management

Regulatory pressure

- Complex regulatory environment
- Increased pressure and audit

What this means for our internal audit

Expectations

Higher expectations from executive, management and boards

Drive value

Greater focus on quality and driving value and impact from investment in internal audit

Trusted advisor

Provides proactive strategic advice to the business

What this means for internal technology audit

Clarity

Need to clearly articulate full suite of internal audit IT solution

Leadership

Opportunity to grow, innovate and drive quality

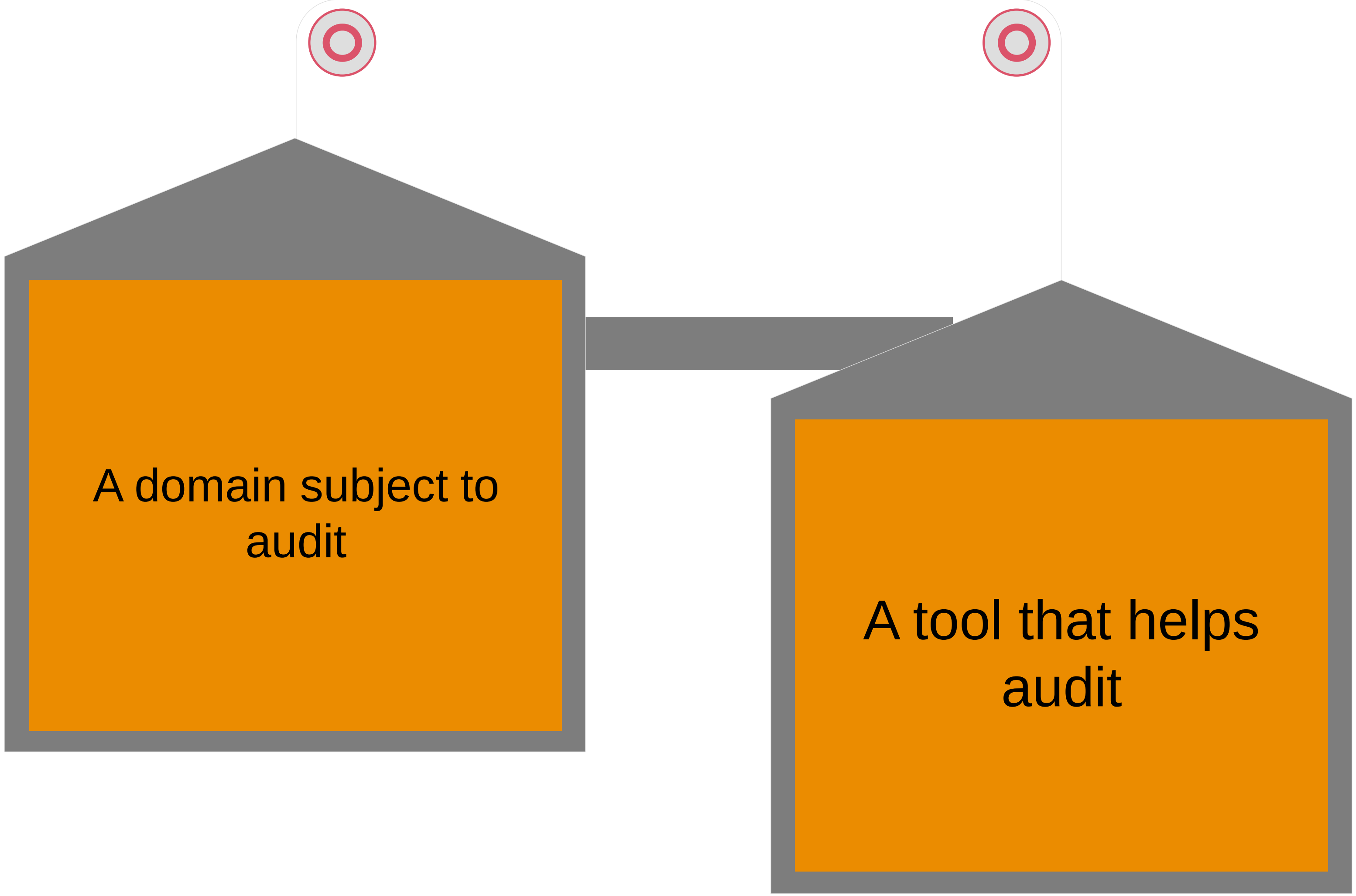
Differentiation

Organic and inorganic growth through specialization

Growing expectations that internal audit is addressing these risk

A Quick Overview of IT

To internal auditors, IT is two things:

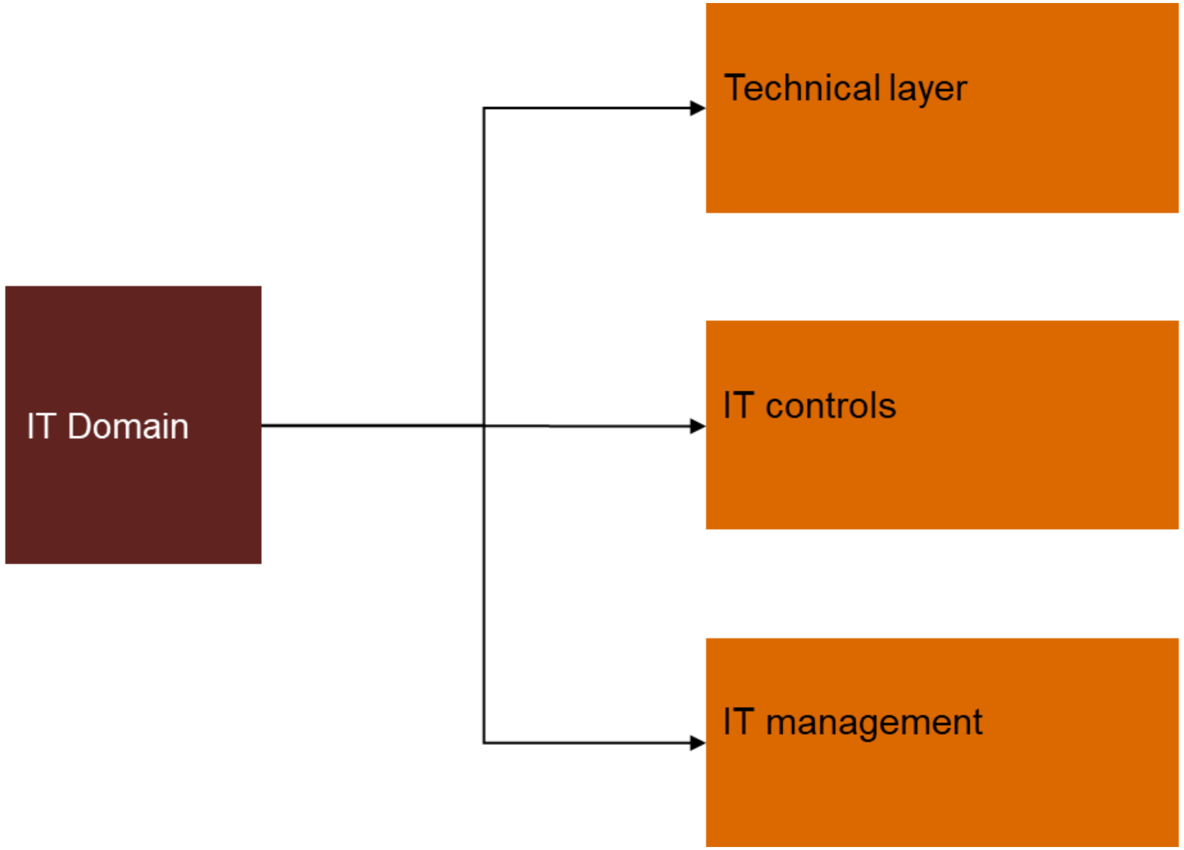


A domain subject to audit

A tool that helps audit

A Quick Overview of IT (cont’d)

IT Domain has 3 Dimensions/Layers:



IT Domain

Technical layer

IT controls

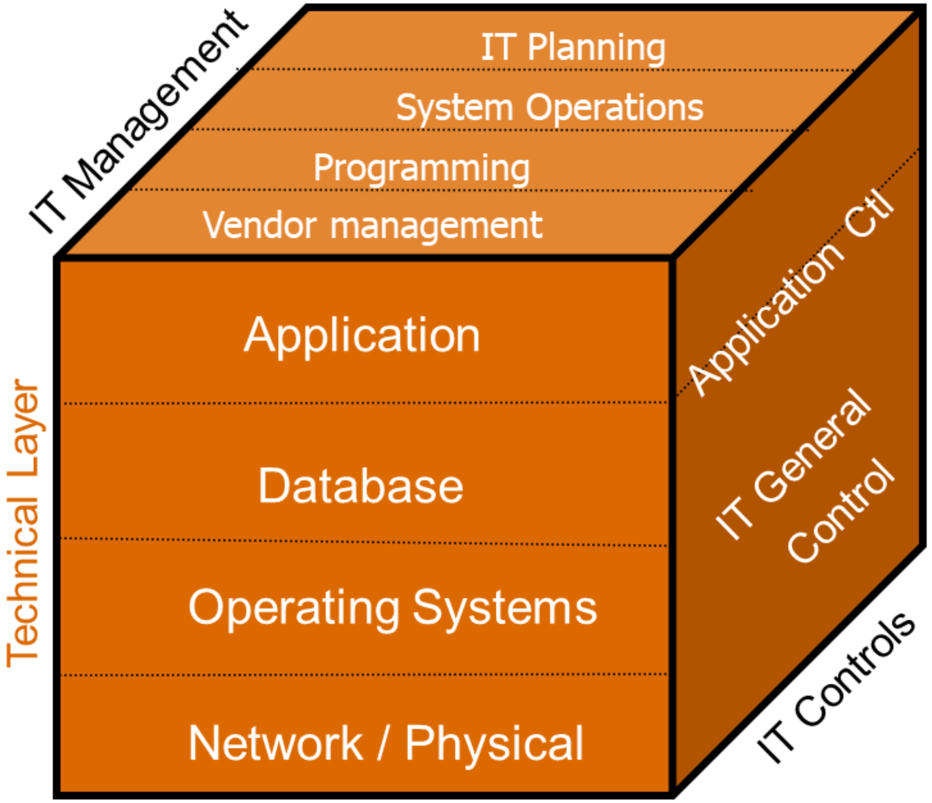
IT management

- Technology
- Process
- People

Layer 1 - Technical Layer

Includes business applications, and the IT infrastructures that underlie, support, and enable the applications.

- Application systems
- Databases
- Operating systems
- Networks



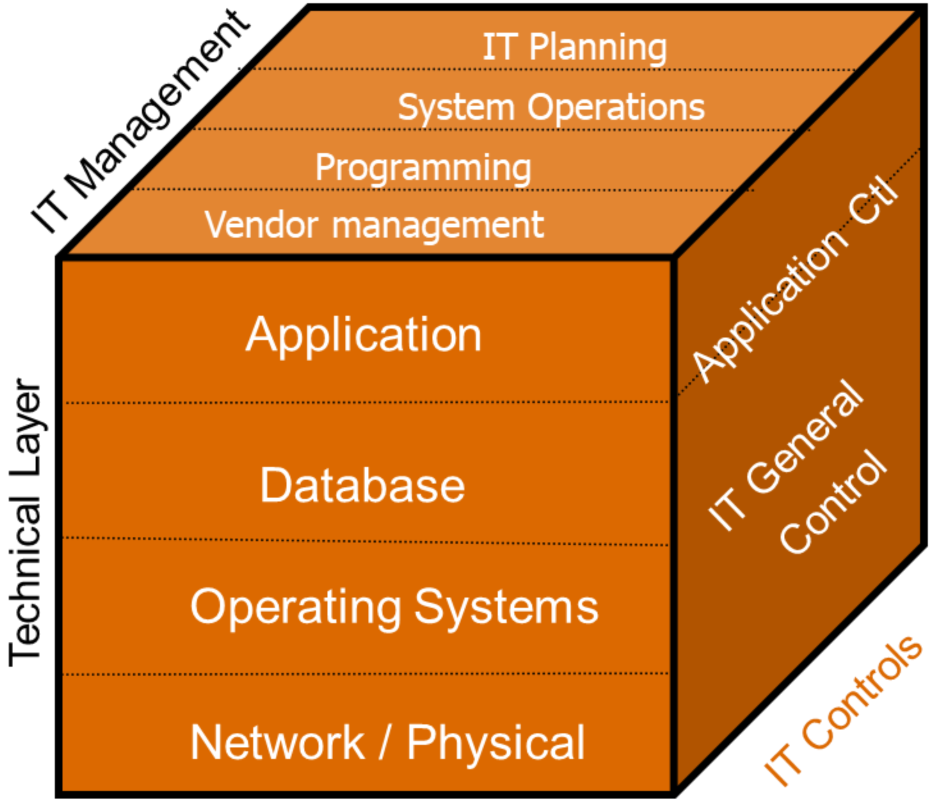
Layer 2 – IT Controls Layer

IT General Controls:

1. Systems development
2. Change management
3. Data center security
4. Backup & restore

Application Controls:

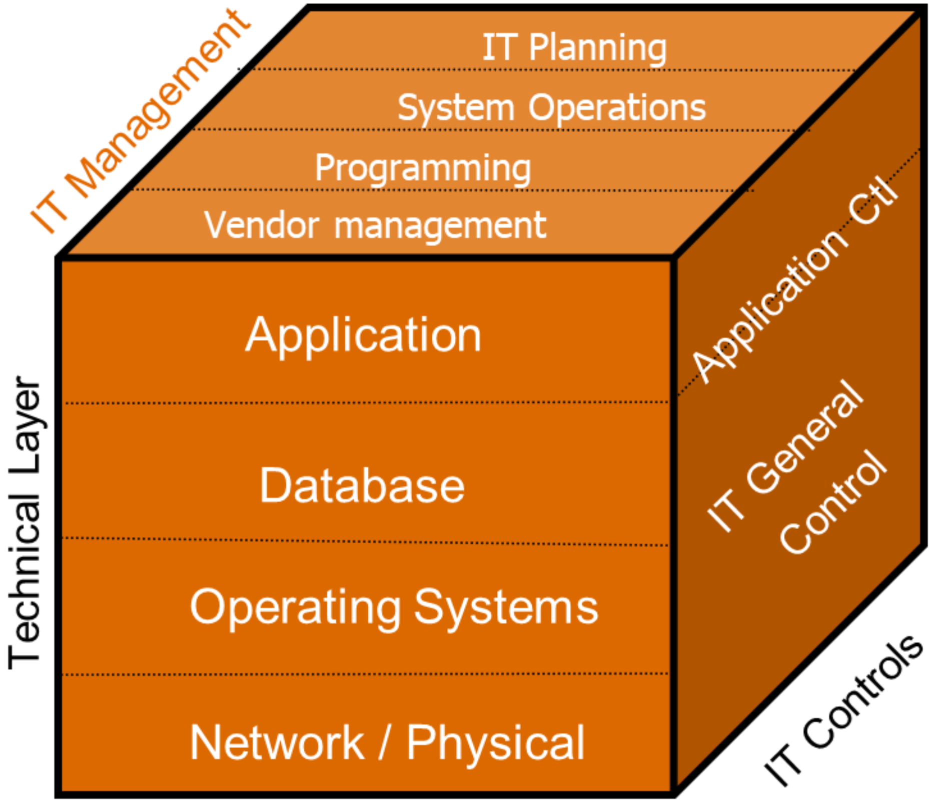
1. Authorization
2. Data integrity check
3. Segregation of duties



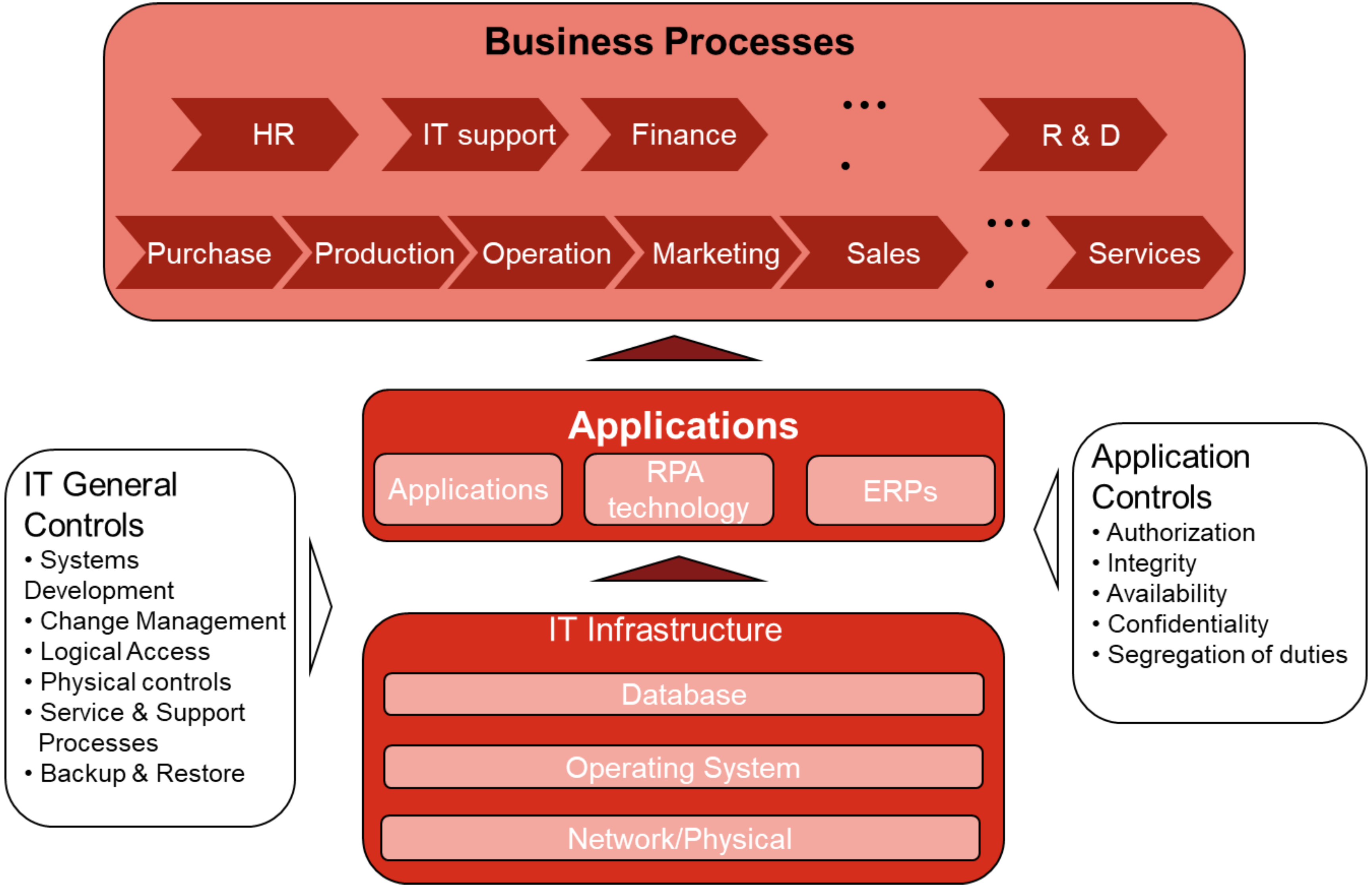
Layer 3 - IT Management

Comprises the set of people, policies, and procedures that manage the IT environment.

- IT Planning
- System operations
- Programming
- Vendor management



IT and the Business



Business Processes

HR

IT support

Finance

R & D

Purchase

Production

Operation

Marketing

Sales

Services

Applications

Applications

RPA technology

ERPs

IT Infrastructure

Database

Operating System

Network/Physical

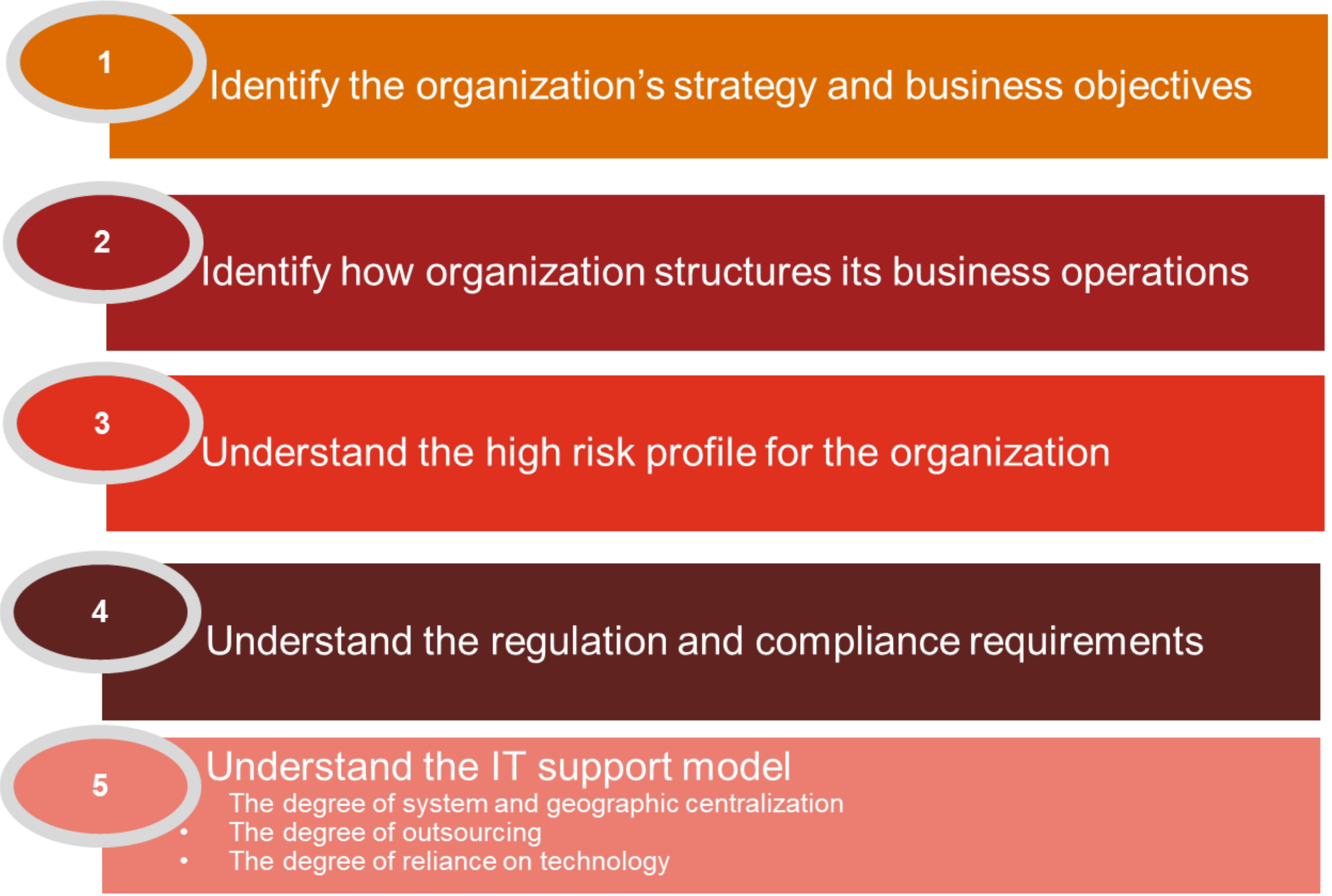
IT General Controls

- Systems Development
- Change Management
- Logical Access
- Physical controls
- Service & Support Processes
- Backup & Restore

Application Controls

- Authorization
- Integrity
- Availability
- Confidentiality
- Segregation of duties

Understand the Business



1 Identify the organization’s strategy and business objectives

2 Identify how organization structures its business operations

3 Understand the high risk profile for the organization

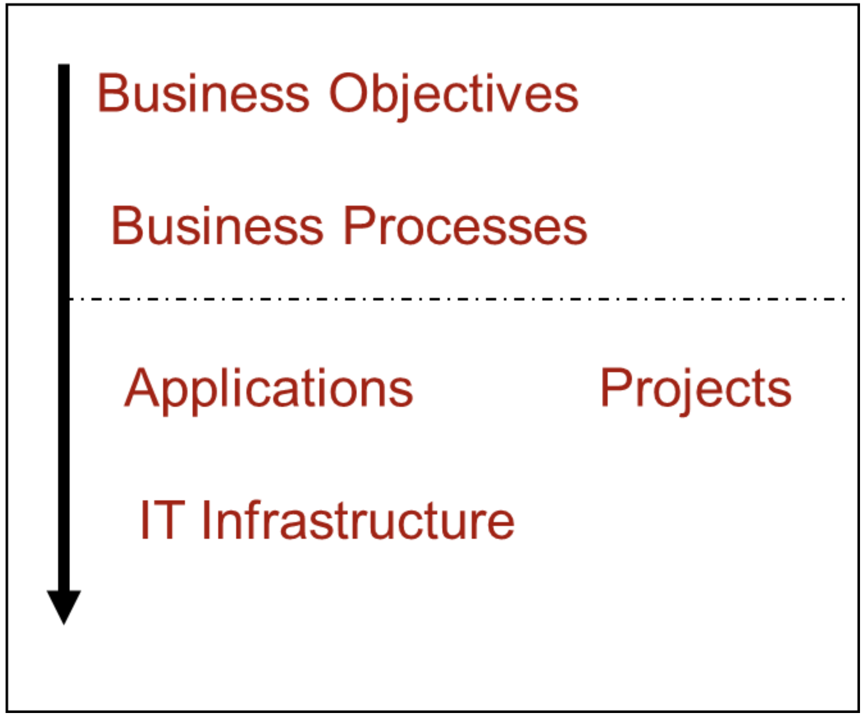
4 Understand the regulation and compliance requirements

5 Understand the IT support model

The degree of system and geographic centralization
- The degree of outsourcing
- The degree of reliance on technology

Define the IT Audit Universe

- Dissect the business fundamentals
- Identify key business areas
- Identify application systems that support the above business areas
- Identify critical infrastructure that supports the above applications
- Identify major projects and initiatives
- Determine realistic audit subjects



Business Objectives

Business Processes

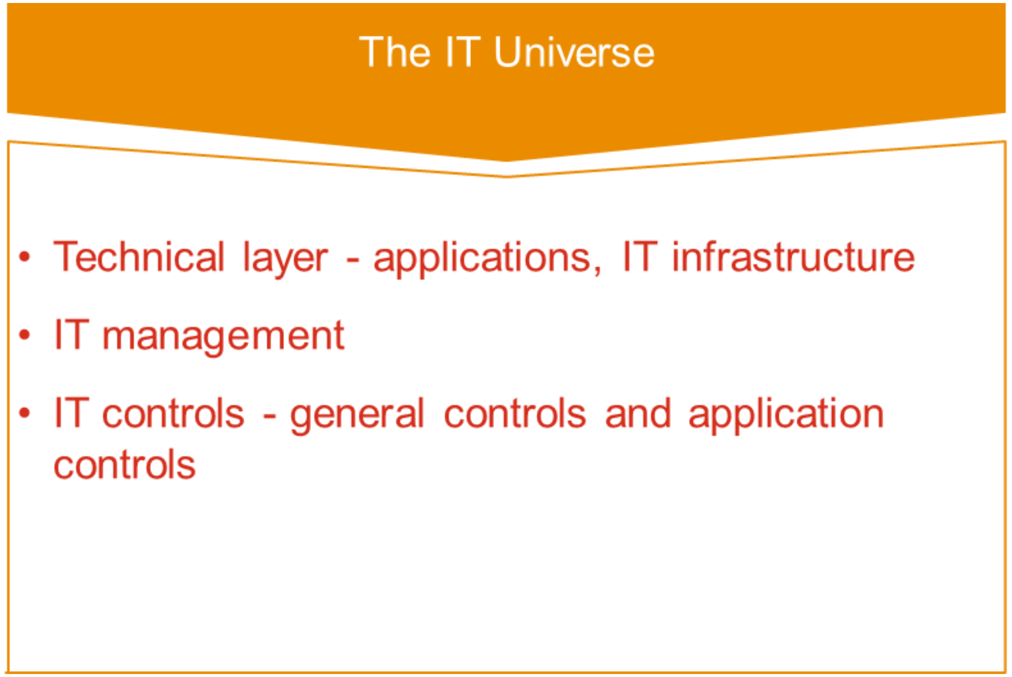
Applications

Projects

IT Infrastructure

Define the IT Audit Universe

Defining the IT audit universe should consider elements under all three IT layers



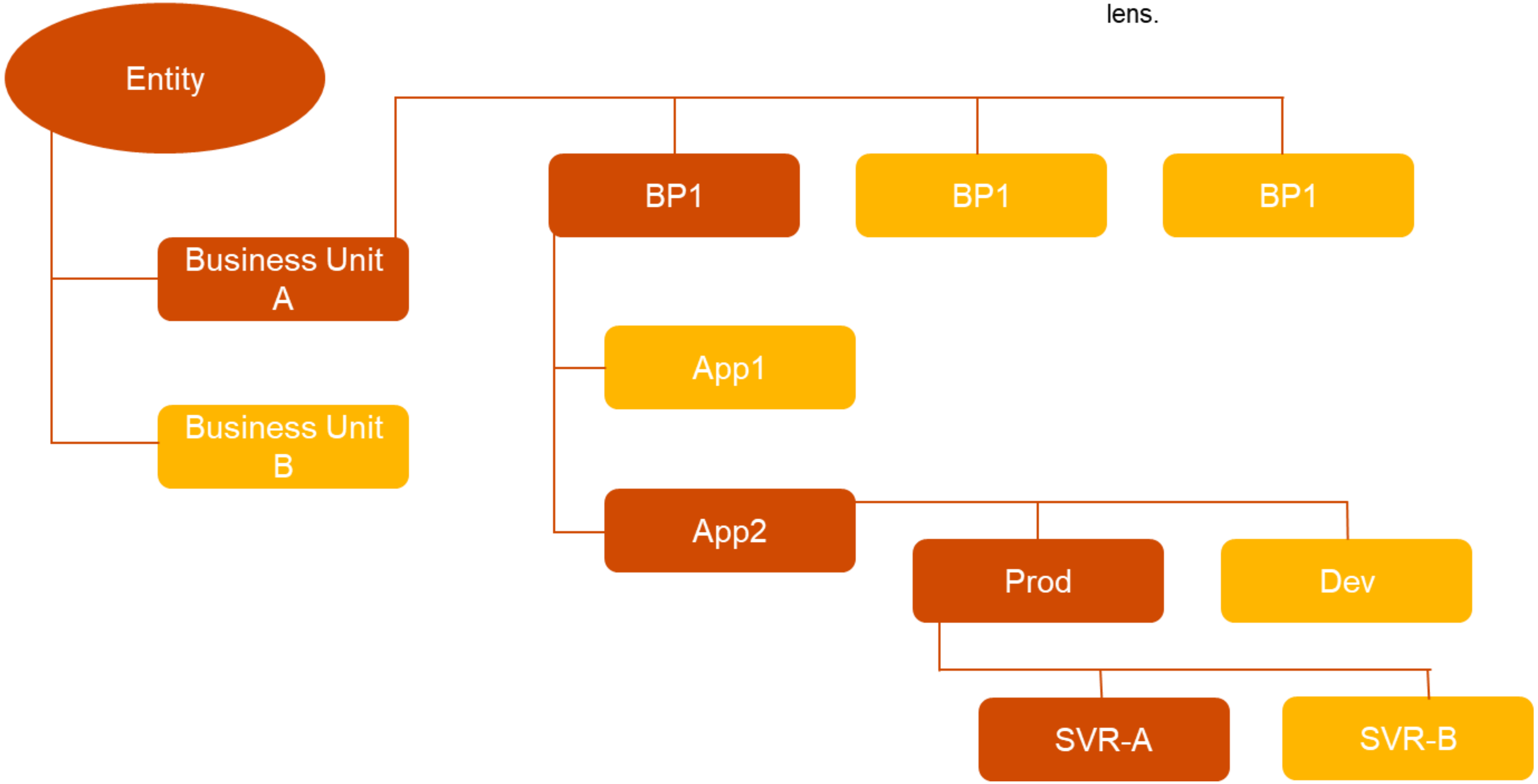
The IT Universe

- Technical layer - applications, IT infrastructure
- IT management
- IT controls - general controls and application controls

Technology Audit

Scoping is a risk based approach

Technology is risky because its use (or lack of use) has business consequences. Any consideration of technology risk should be viewed through this lens.



Develop the IT Audit Plan - Risk Assessment

The IIA Standard 2010 – Planning: The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals.

Examples of risks are

- Strategic
- Financial
- Reputation
- Legal and Regulatory
- Operational

Many risk ranking approaches. The IIA's IPPF states

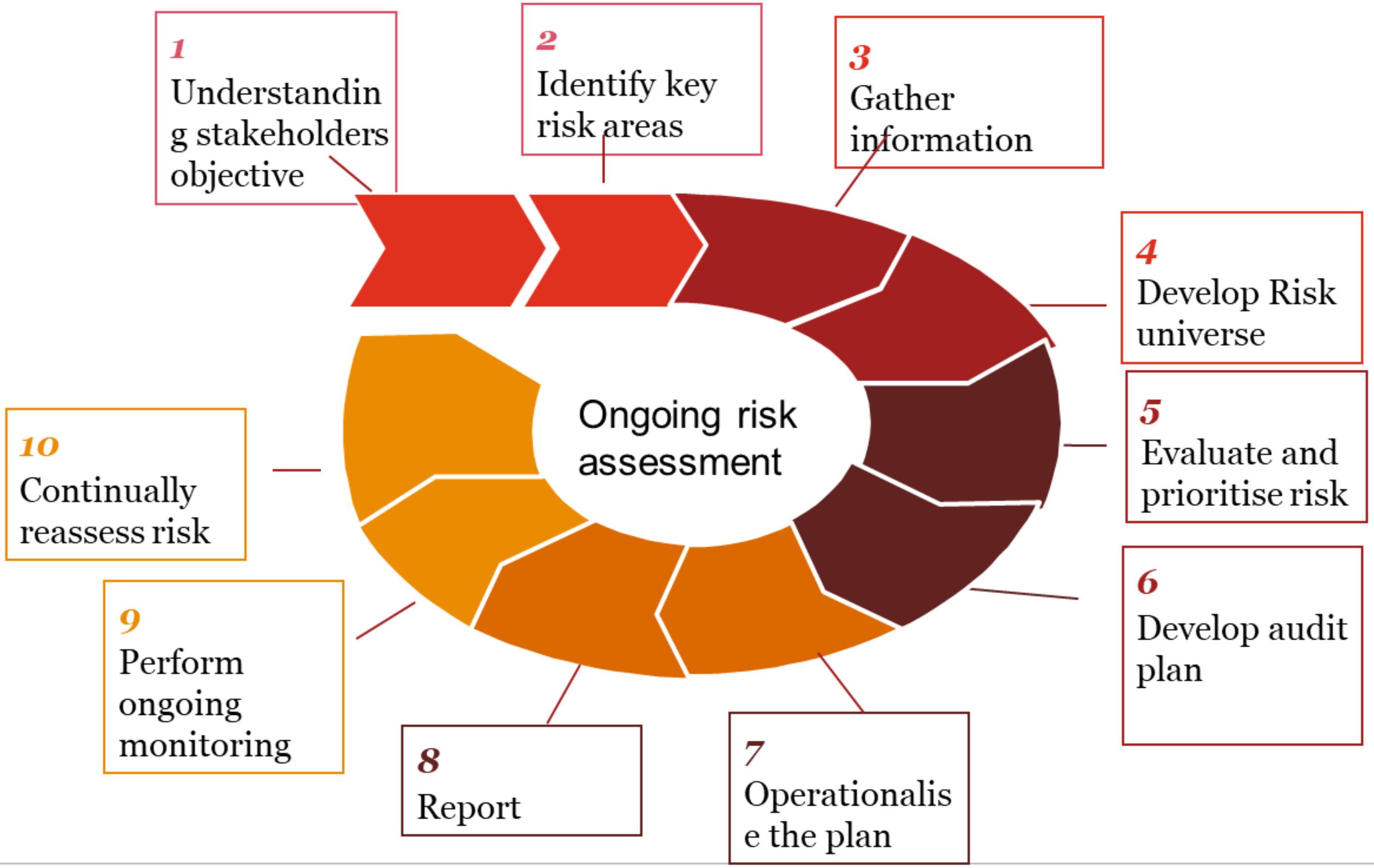
"Risk is measured in terms of impact and likelihood".

Prioritize audit subjects based on the risk ranking

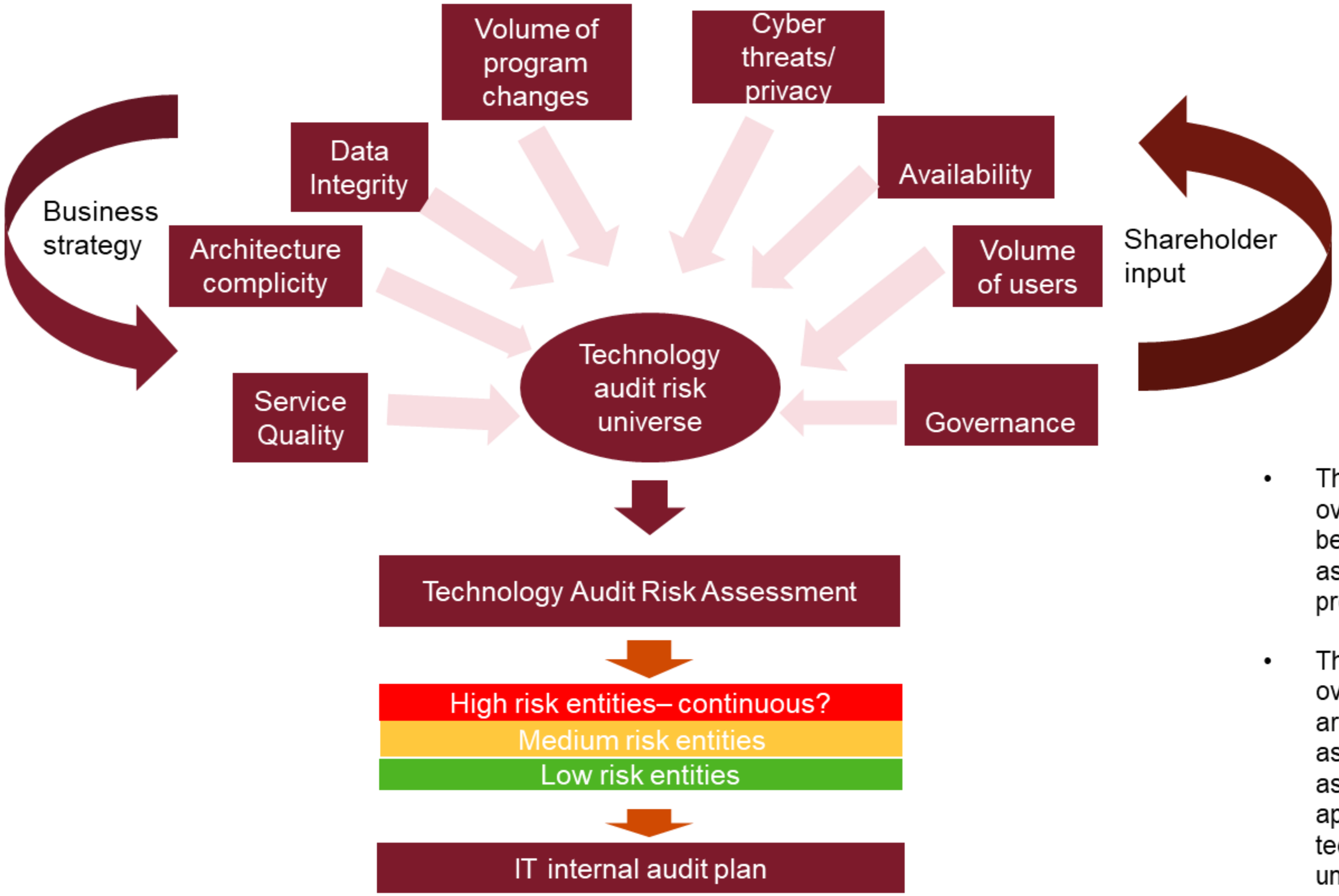
Technology Audit Risk Assessment

Risk is a natural part of Business landscape. If left unmanaged, the uncertainty can spread like weeds. If managed effectively, losses can be avoided and benefits obtained.

A Technology Audit Risk Assessments is a component of a larger enterprise risk management system.

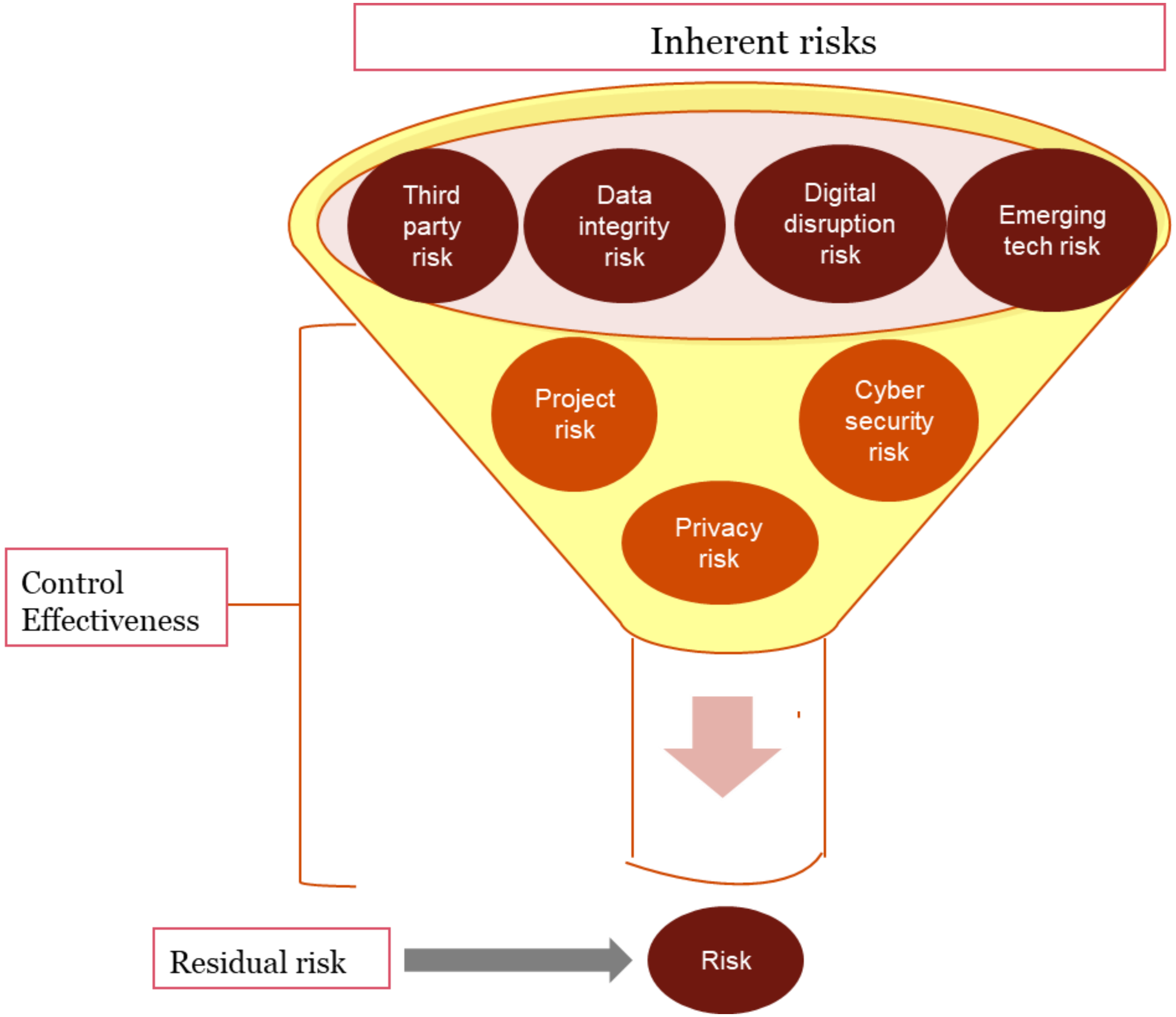


Technology Audit Risk Assessment - Strategy and profile



- This image provides an overview of the relationship between technology Audit risk assessment, Strategy and profile coverage.
- This image also provides an overview of some of inputs that are assessed in an IT risk assessment process. IT risk assessment requires application, infrastructure and technical knowledge and understanding of the organisation's IT environment.

Technology Audit Risk Assessment - Risk profiles



What are the risk assessment fundamentals?

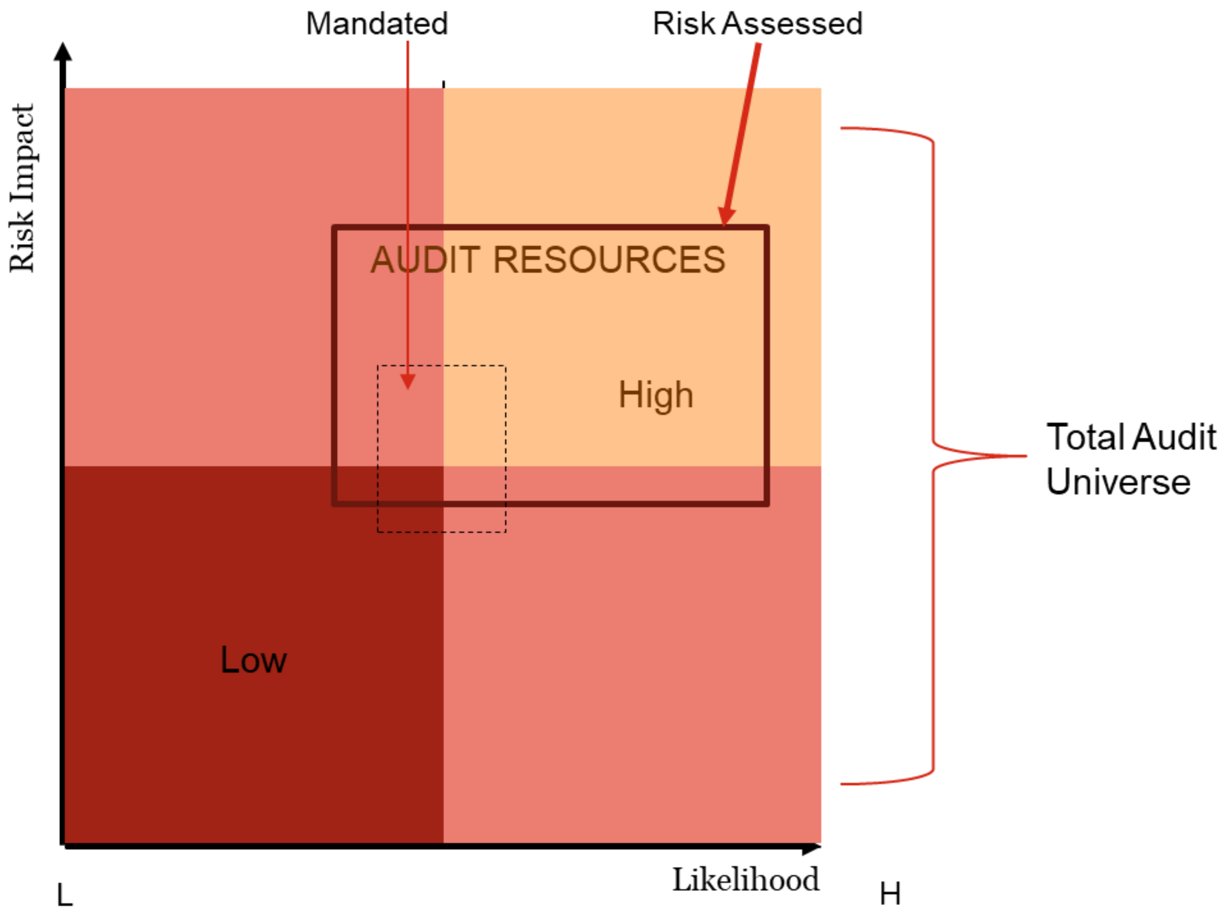
By considering both the inherent risk and control risks the likelihood of the occurrence, a **risk profile** of the organisation can be developed.

The **risk profile** is presented to management and the audit committee using a color-coded heat map that identifies high moderate and low risk areas.

This initial **risk assessment** identifies specific business units, processes or activities that present's the highest risks and forms the basis of the audit program.

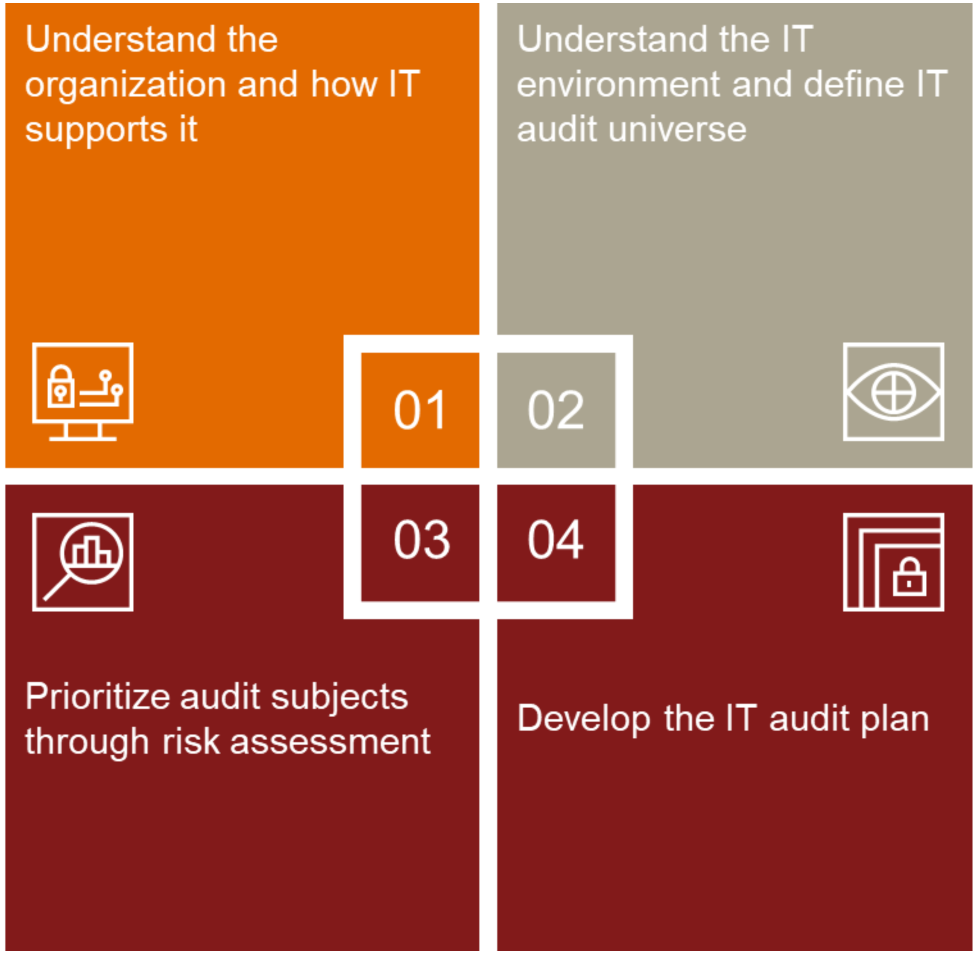
Validate the IT Audit Plan

Steps to develop the IT Audit Plan



Summary

Steps to develop the IT Audit Plan



01 Understand the organization and how IT supports it

02 Understand the IT environment and define IT audit universe

03 Prioritize audit subjects through risk assessment

04 Develop the IT audit plan

Conclusion

01 IT only exists to support and further business objectives.

02 To define the IT audit universe, understand the business first

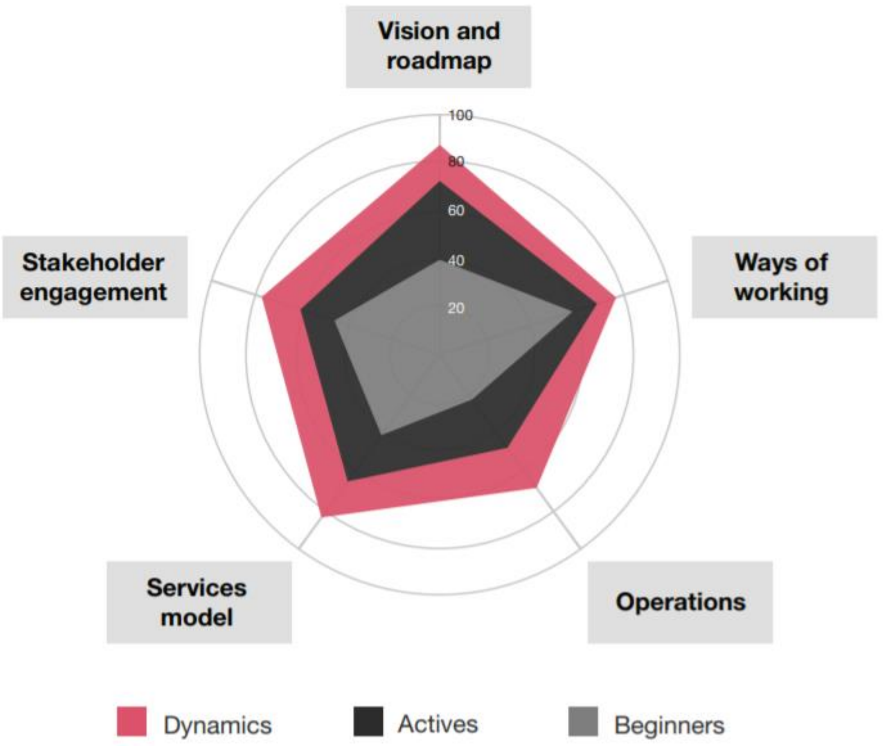
03 To develop the IT audit plan, assess business risk associated with IT

Elevating IA’s role to meet today’s emerging risks

In 2019, we measured the digital fitness of assurance functions.

Dynamics are the most digitally fit

Digital fitness in each dimension



Digital maturity score on a scale of 0 to 100 based on PwC analysis and index calculation.
Base: 252 Dynamics; 249 Actives; 500 Beginners

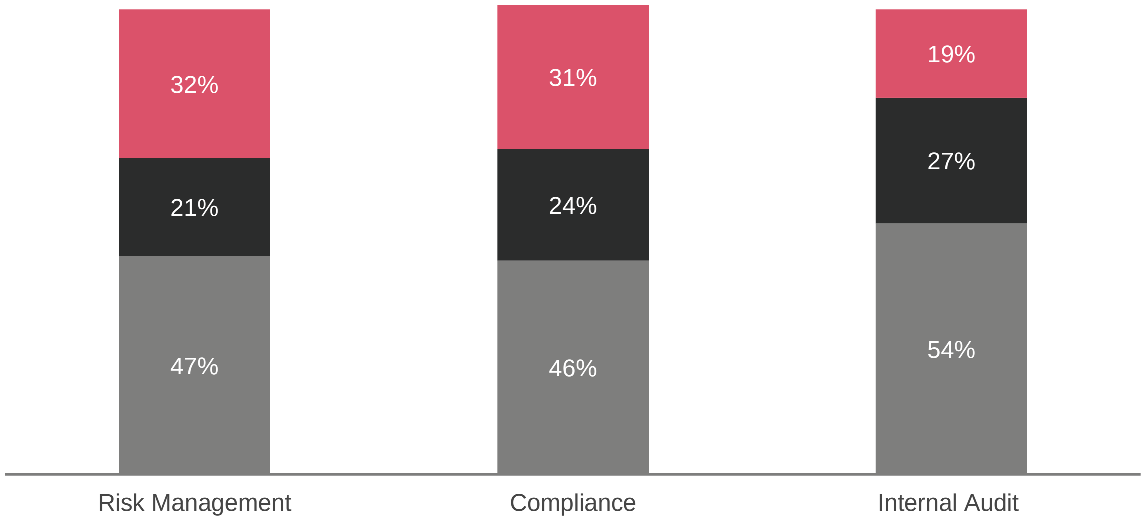
PwC’s 2019 state of the internal audit profession survey

Dynamics: the most digitally fit quartile of all risk, compliance and internal audit respondents

Actives: taking many of the steps necessary to become more digitally fit

Beginners: conducting or planning to conduct some of the activities we measured, though are at an early stage in their digital journey.

How does each function fare in digital fitness?

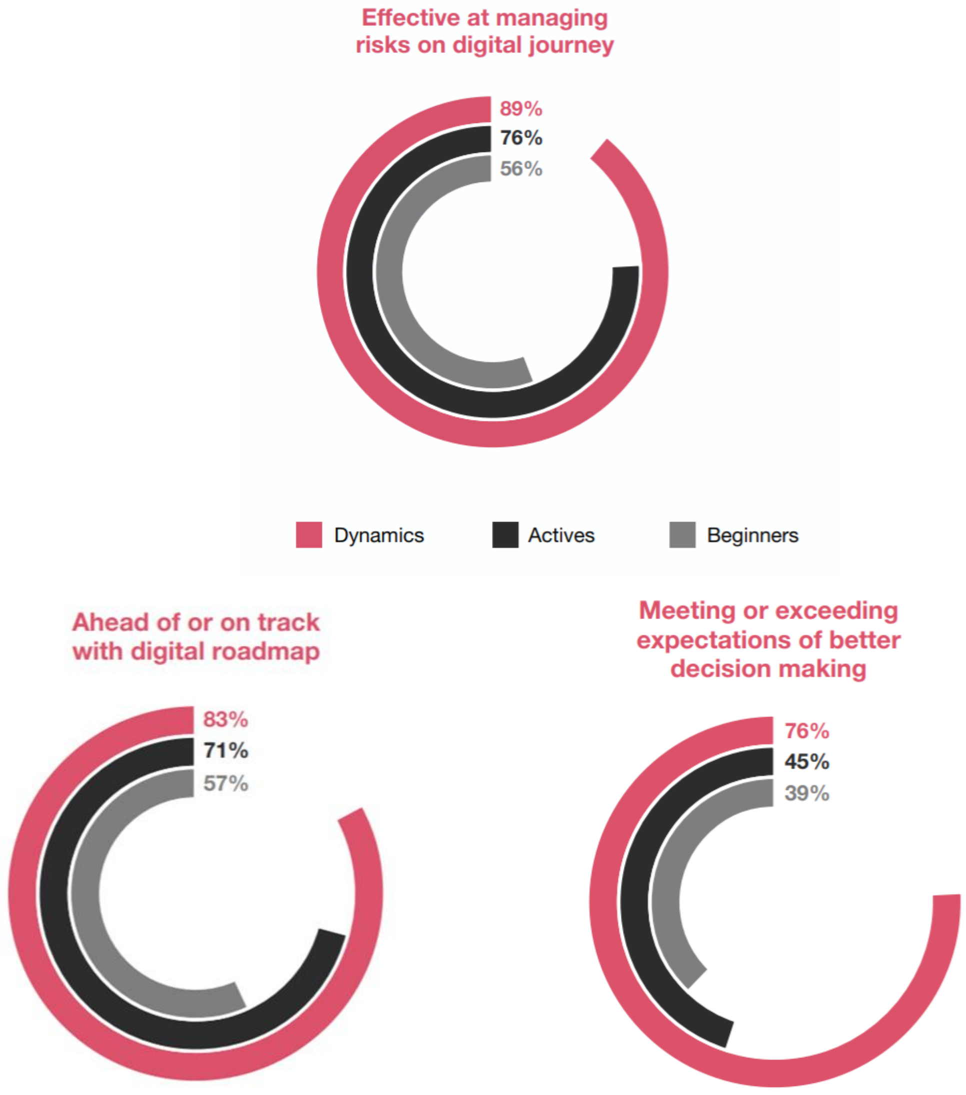


Elevating IA’s role to meet today’s emerging risks

We found that the payoffs of being a Dynamic are significant

Organizations with Dynamic risk functions receive many benefits:

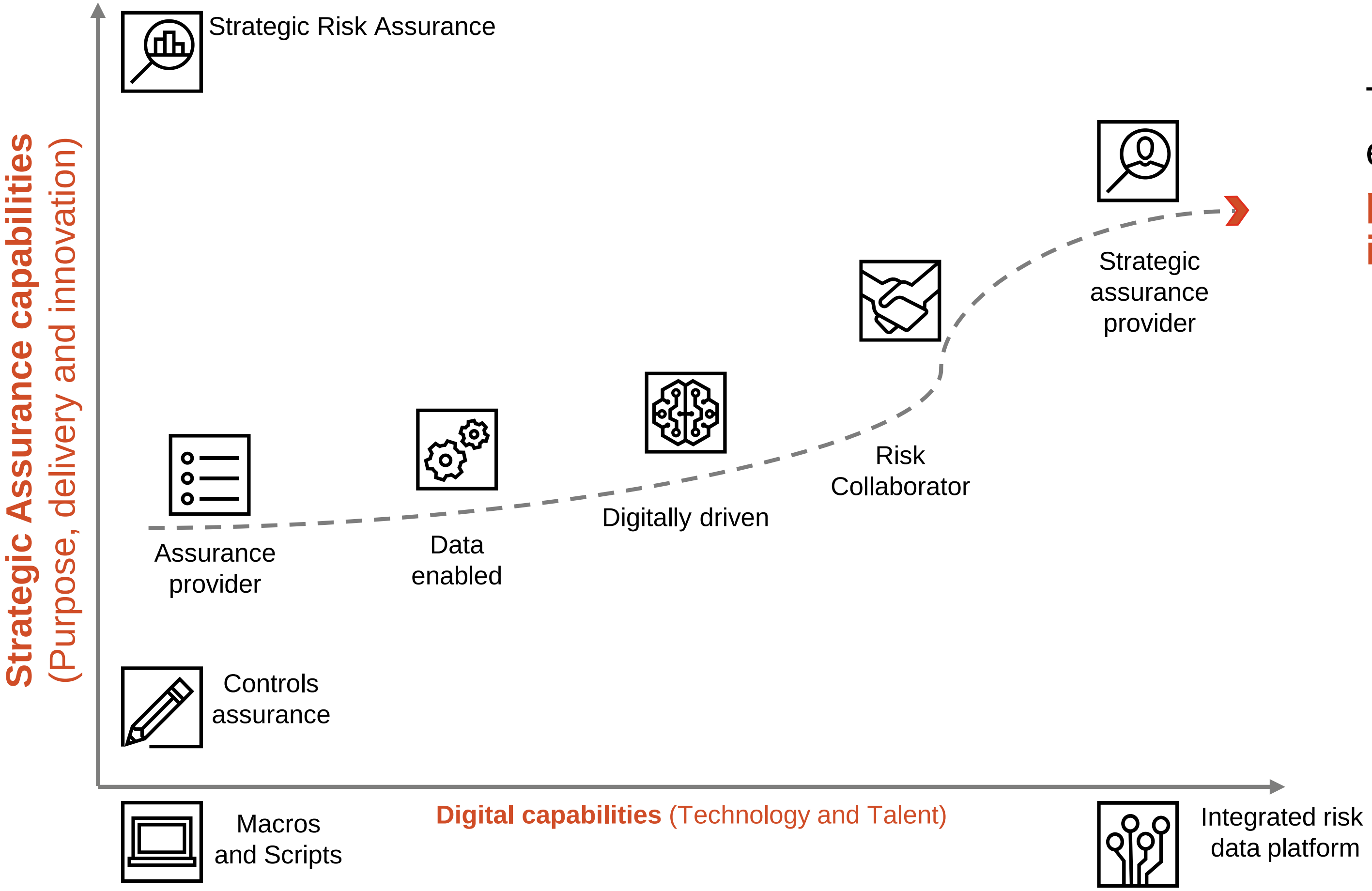
- Faster progress on their digital journey
- More confidence in taking risks consistent with their strategy
- More effective management of digital-related risks
- More value than anticipated from their digital investments



PwC’s 2019 state of the internal audit profession survey

Elevating IA's role to meet today's emerging risks

Historically the internal audit maturity curve has been from **"Assurance provider to Data enabled"**, which is the starting point of the new curve.


Strategic Assurance capabilities (Purpose, delivery and innovation)
Strategic Risk Assurance
Strategic assurance provider
Risk Collaborator
Digitally driven
Data enabled
Assurance provider
Controls assurance
Macros and Scripts
Digital capabilities (Technology and Talent)
Integrated risk data platform

The new internal audit maturity curve pushes the envelope further to create a **common assurance purpose** for the organization driven by an **integrated common data platform**

PwC's 2019 state of the internal audit profession survey

Digitization comes with its own unique risks

Cybersecurity

- Growing attack sophistication
- Expanding attack surface

Regulatory risk

- Unfavorable regulatory pronouncements

Data Governance

- Magnification of poor data quality
- Democratization of Data Analysis

Data Privacy

- GDPR/NDPR enforcement
- Consumer awareness

Third Party risks

- Proliferation of business ecosystems
- Nth-Party Risk

Ethics & Integrity

- Inattention to digital ethics
- Human bias in Artificial intelligence

Internal Audit Challenges as a result of digitization

01 How do we mitigate risks such as 3rd party IT integration with our environment

02 How can we reduce the cost and time spent on Audit and monitoring

03 Do we have the skills and training needed to manage the risks in emerging technologies

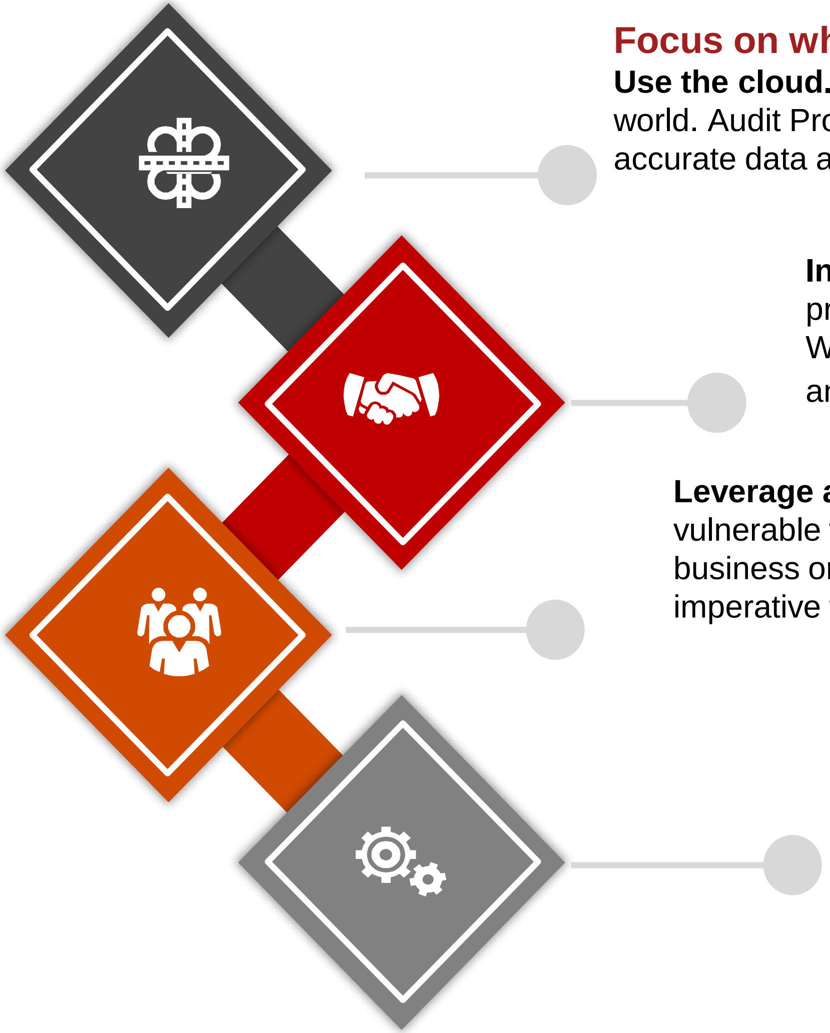
04 Do we have the right technologies to review controls in digitized processes

05 How can we adopt an integrated approach to providing assurance on risks of digitisation

IT Audit Considerations

Leveraging Technology For Remote Auditing

Moving with the trends in Remote Auditing



Focus on what matters;

Use the cloud. Cloud computing offers a virtual workspace for colleagues around the world. Audit Professionals can share ideas, track progress, and work on a single source of accurate data asynchronously at their own schedule or in real time, together.

Instill agile principles. Agile is a way of working that focuses on people over process, with emphasis on iterative planning and incremental delivery of work. With roots in software development, agile aims to meet business objectives and deliver value early and often. .

Leverage analytics and digital risk assessments. Internal audits tasks are vulnerable to challenges like cost overruns, missed deadlines, and failure to meet business or quality requirements. Remote work can easily amplify these risks, so it is imperative to make a point of projects and judgments through fact-based data analysis.

Emphasize digitization. Although some of the information required to complete an audit has been converted to digital format, organizations remain in various stages of their own digital journey. It may take a purposeful push to digitize in order to achieve the repeatability, scalability, and consistency necessary for operating effectively in a remote environment

IT Audit Considerations

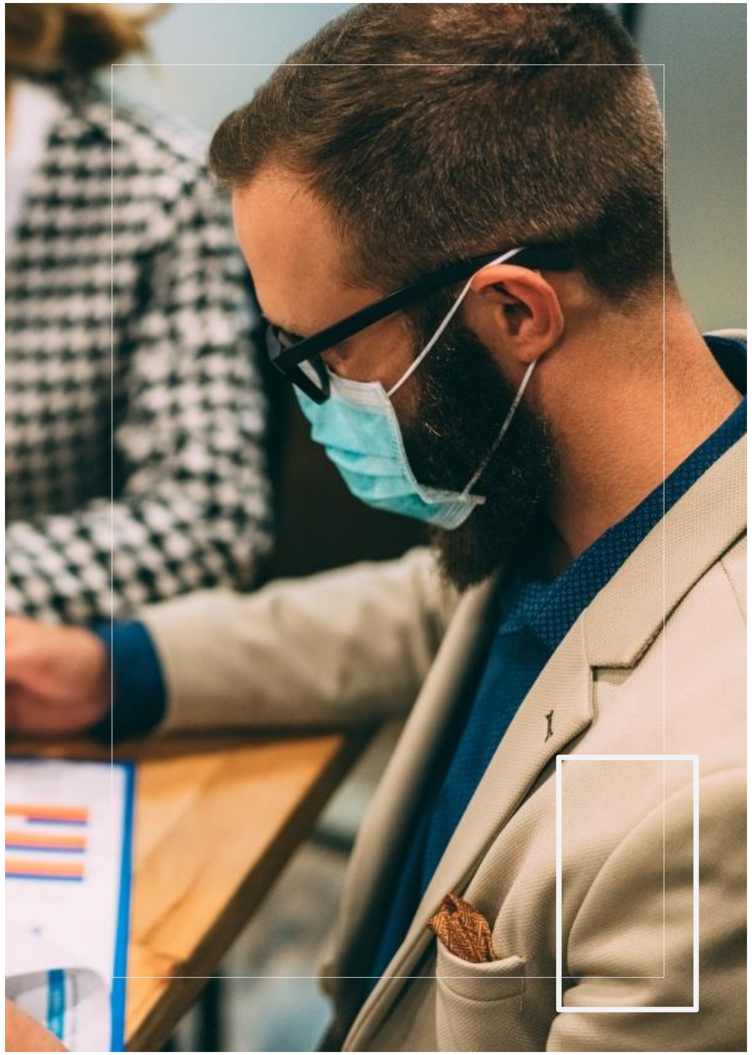
Leveraging Technology For Remote Auditing

Some Challenges

- Unsecure networks
- Phishing attacks
- Insecure mobile devices
- Computer Sharing and personal use
- Outdated companies policies

What to do:

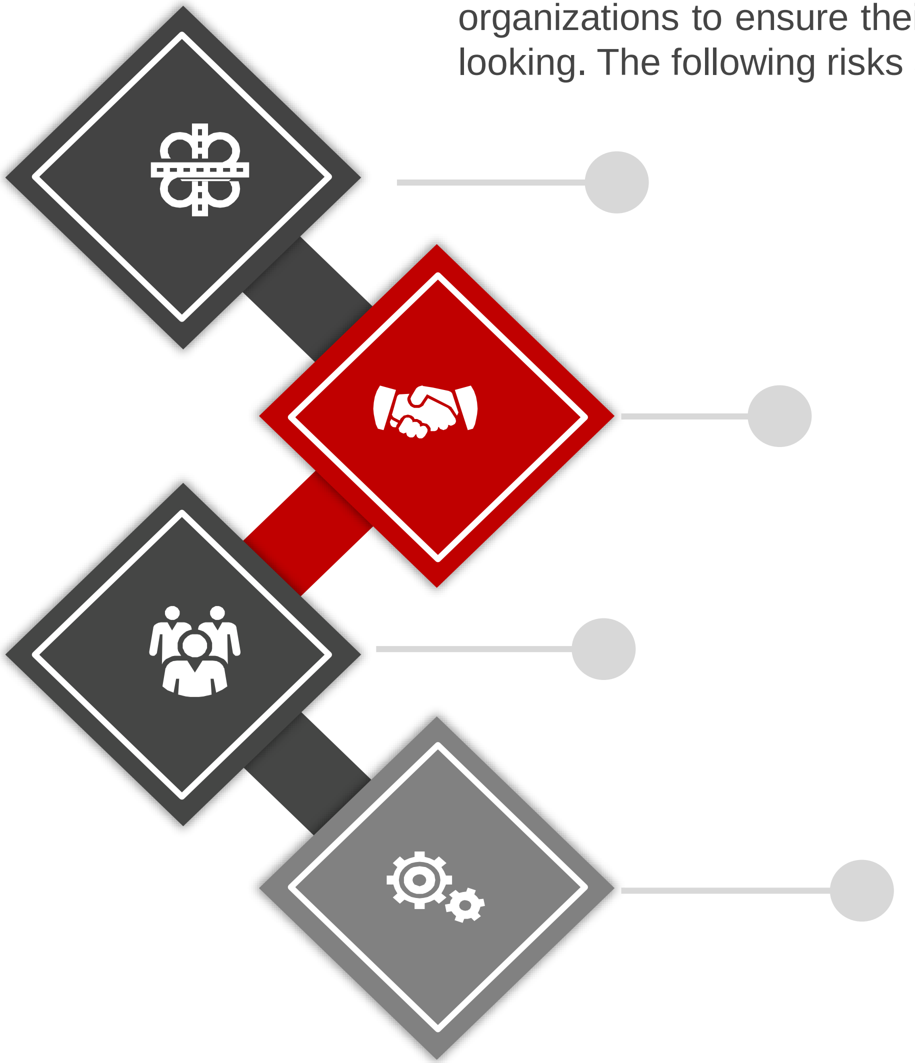
- Keep devices patched and up-to-date
- Boost security awareness with mandatory training
- Encourage good basic digital hygiene
- Give clear security guidance
- Update relevant policies to reflect current realities



IT Audit Considerations

Data Privacy and Governance Risks

Securing the Organization amid the pandemic



The global spread of COVID-19 has generated numerous privacy, data protection, security and compliance questions. These challenges are driving the need for companies and organizations to ensure their digital experience platform(s) are not only secure, but forward looking. The following risks are of major concern;

- Maintaining security of systems, software and Data outside the centralized, well controlled corporate network
- Employees using a separate connection link to access corporate network
- Rapid and unplanned scale up in current technology infrastructure
- New and untested features, along with suboptimal controls being used to ensure business operations

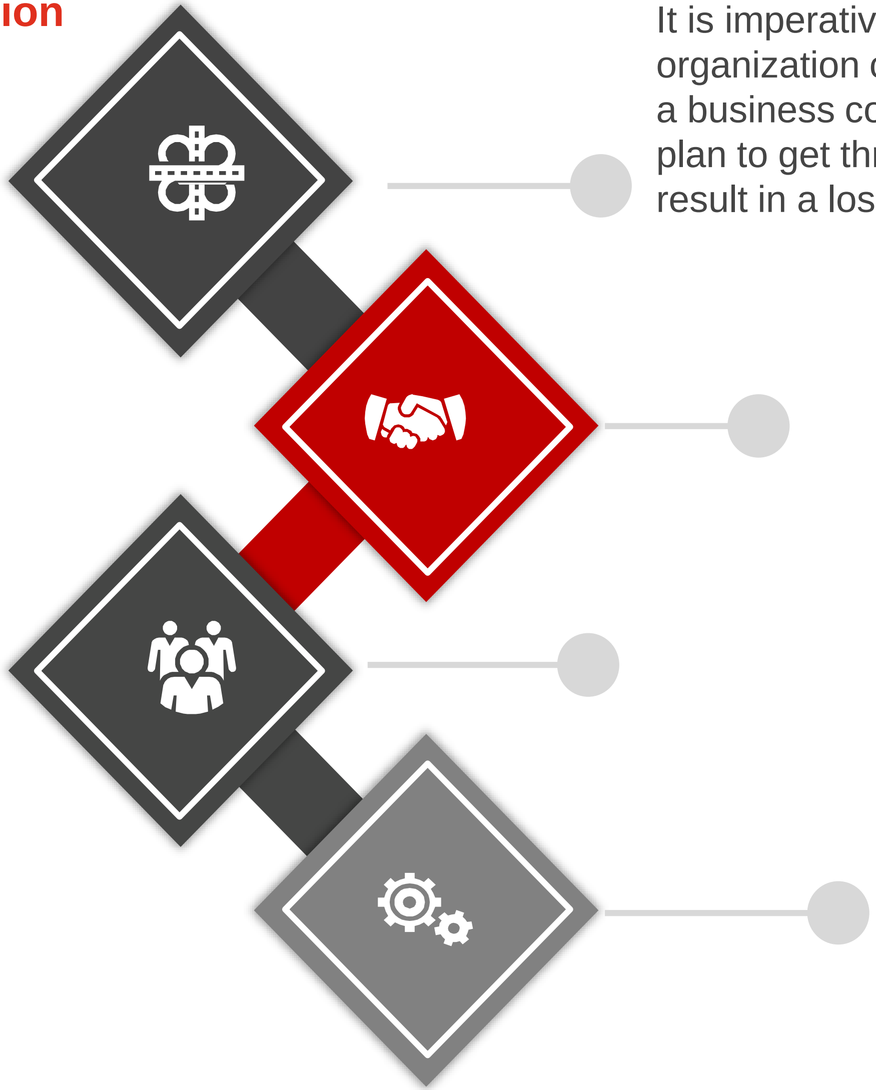
How to mitigate the risks;

- Fortify organization’s corporate network and data to ensure secure connection during remote working period
- Companies must provide employees with laptops, mobile phones, and other necessary equipment to secure virtual-private-network (VPN) connections so that they may work securely remotely
- Build agile administrative and technical controls around rapid infrastructure upgrades required to scale up operations

IT Audit Considerations

Third Parties Integration

Third-party risks can include operational risk, transaction, risk, and compliance/regulatory risk.



It is imperative that third party vendors are scrutinized to ensure the needs of the organization can be met. This should include ensuring the third-party vendor has a business continuity and disaster recovery plan. Ensuring a third-party has a plan to get through the COVID-19 pandemic is vital since their own failure may result in a loss to your organization as well.

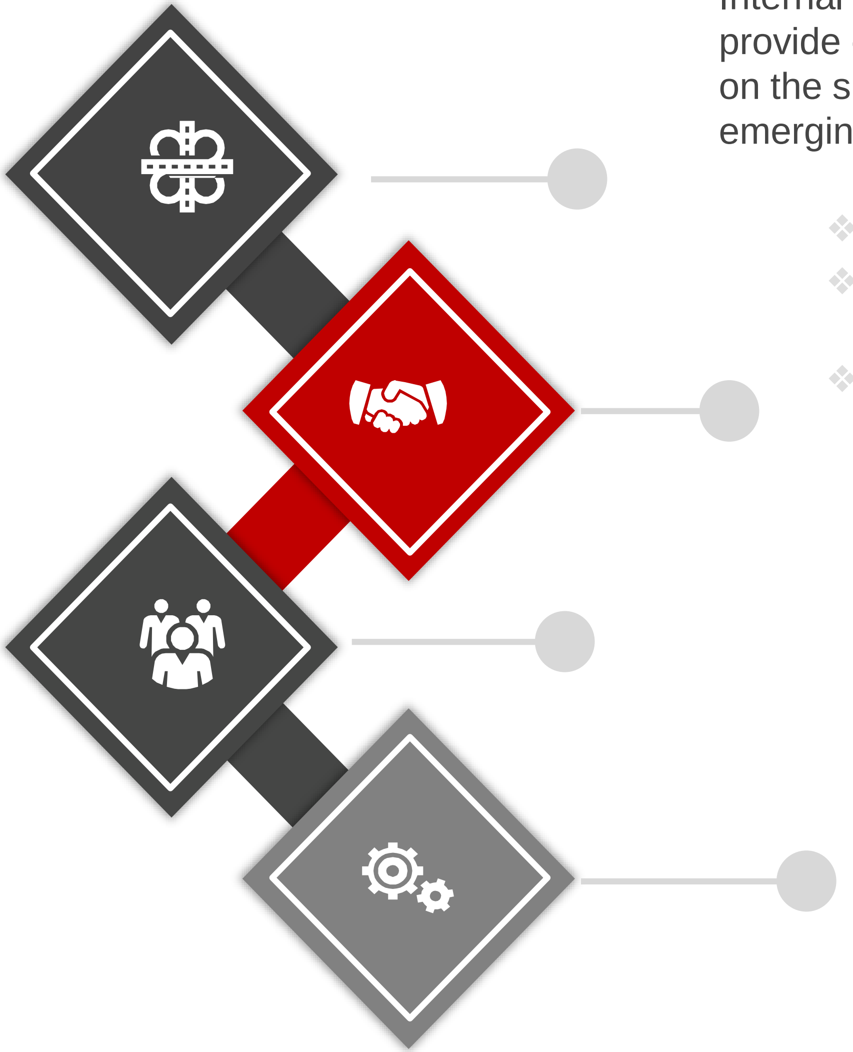
- Unvetted third Parties providers doing business with the organization
- Lack of insight into Vendors’ Business Continuity and Disaster Recovery Plans
- Third Parties application integration protocols and gateways.

How to mitigate the risks;

- It is important that third parties vendors are scrutinized to ensure that the need of the organization are met.
- Continuous monitoring of third parties incidents and issue logs
- The organization must review third parties business continuity and disaster recovery plans since their failure may impact the organization considerably.
- Ensure that all necessary controls in third parties protocols are tested inline with applicable standards before promoting to production environment

IT Audit Considerations

Business Continuity Management



Business continuity emerging risk areas

Internal audit team has an important role to play to continue to provide critical Assurance, help advise management and the board on the shifting risks and controls landscape and help anticipate emerging risks.

- Organization’s Single Point of Failure Points
- Inadequate Internal business continuity metrics and assumptions
- Business assumptions on outsource service providers

Internal audit considerations should include;

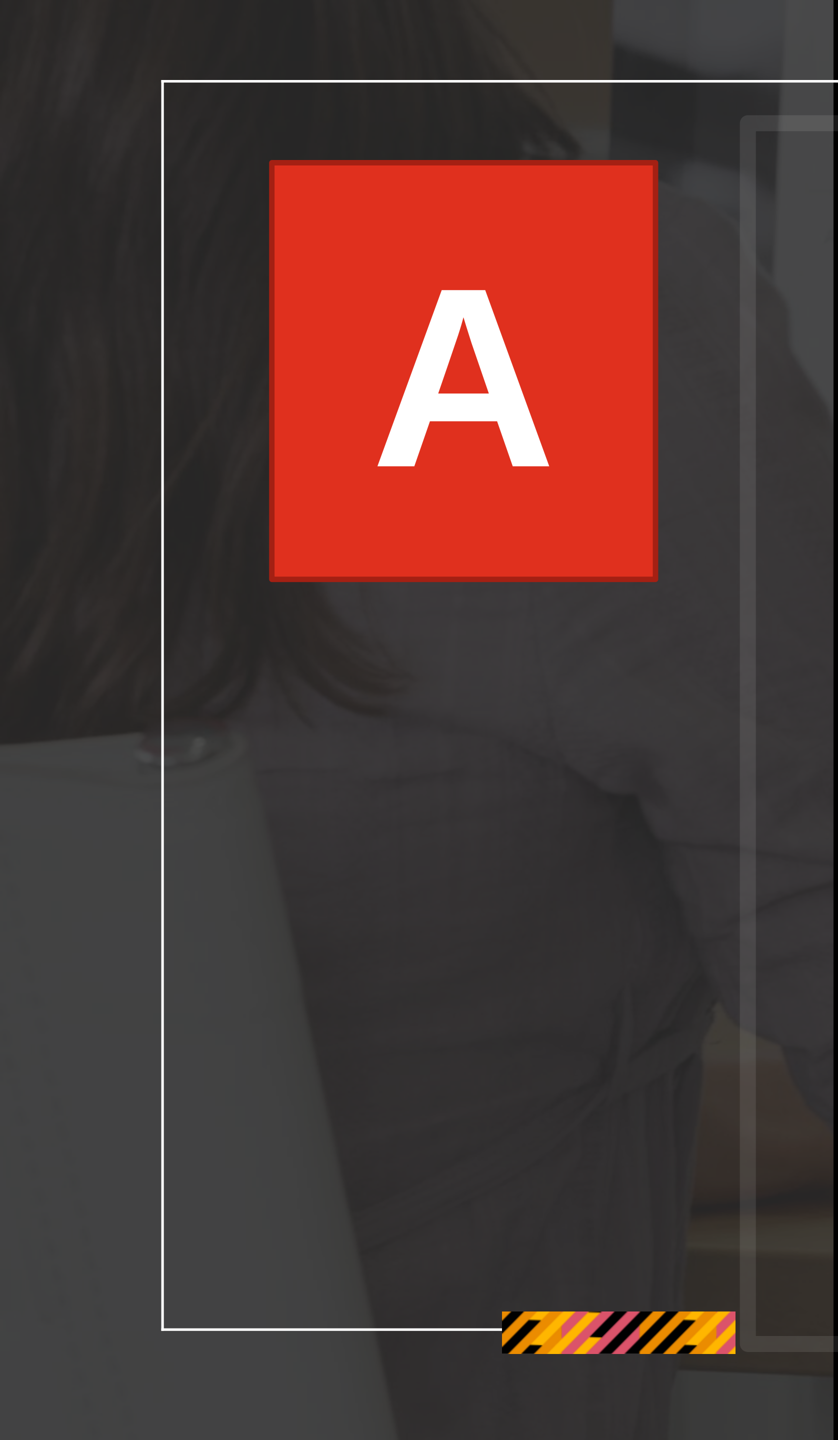
- Reviewing organization’s single point of failure points across different processes in line with the business continuity plans and risk assessment priorities
- Validating and channeling key metric used by management to make decisions on mission-critical activity and challenging and benchmarking management’s assumptions regarding the nature, extent and duration of situations
- Validating management’s assessment, monitoring and contingency plans of key outsource service providers
- Developing and/ or testing appropriate scenarios, plans or measures to restore business operations (disaster recovery plans)

Auditing Cloud Security and Challenges with VPN Infrastructure

05

Content

- What is Auditing?
- Cloud Computing
- Cloud security: Security measures and auditing framework
- Cloud Security Threat and environment attack Vectors
- Types of Audit Report
- Shadow IT, API deployment in your organisation
- Cloud Security Risks, Compliance, Data Privacy and Protection
- Role of Internal Auditor in Cloud Security
- Basic understanding of VPN Infrastructure
- Challenges associated with VPN implementation
- Cloud based protection technologies against VPN



A

What is Auditing?

What is Auditing?

Auditing in the traditional sense involves the ensuring of compliance with policy, guidelines, and regulations.

Within a cloud environment, auditing presents additional challenges and complexities over a traditional data centre

B

Cloud Computing

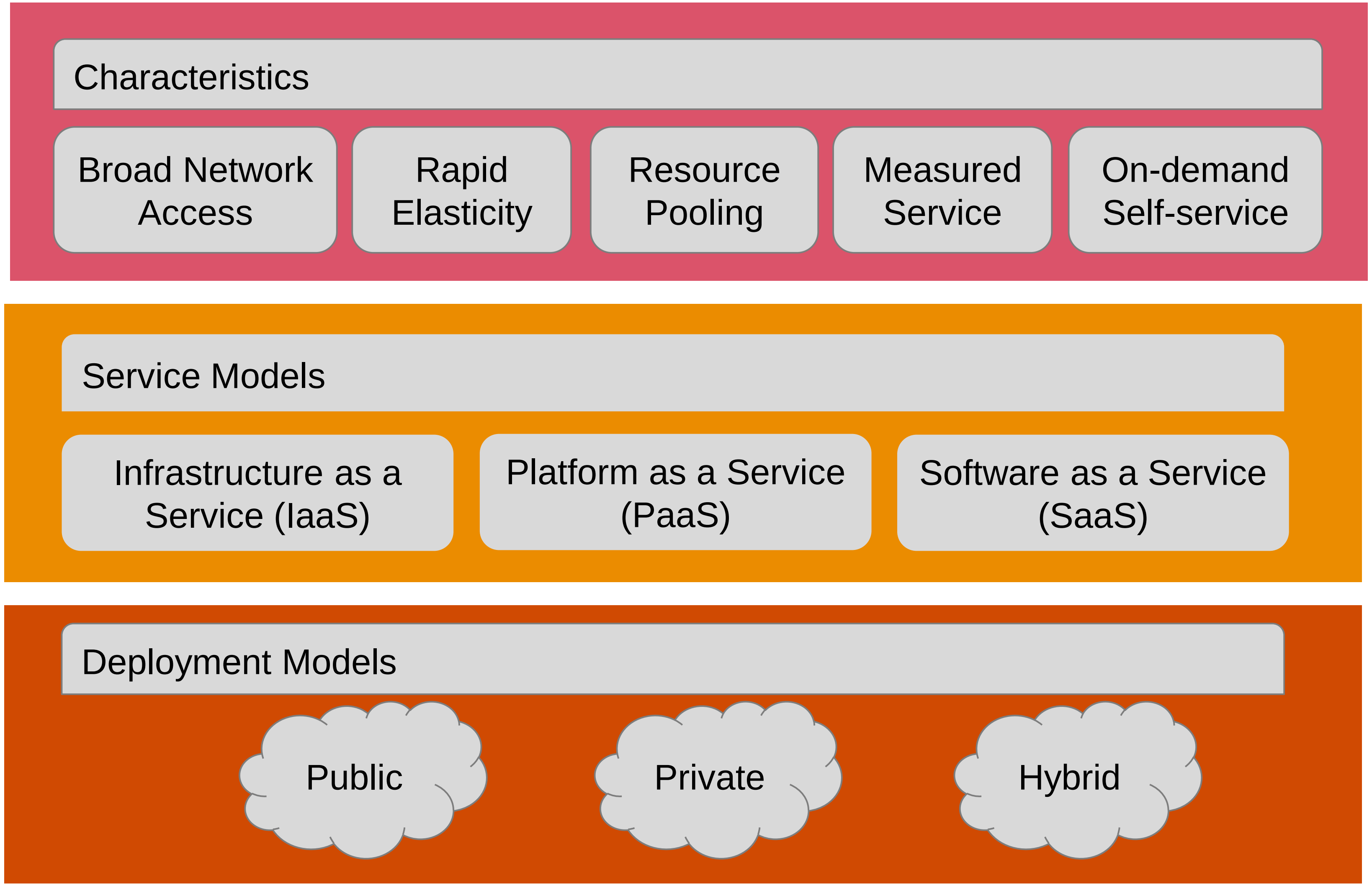
Cloud Computing

Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet)

~~Wikipedia

A style of computing where scalable and elastic IT-enabled capabilities are provided 'as a service' to external customers using Internet Technologies.

~~Gartner



Characteristics

Broad Network Access

Rapid Elasticity

Resource Pooling

Measured Service

On-demand Self-service

Service Models

Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

Software as a Service (SaaS)

Deployment Models

Public

Private

Hybrid

Cloud Computing

Microsoft Security

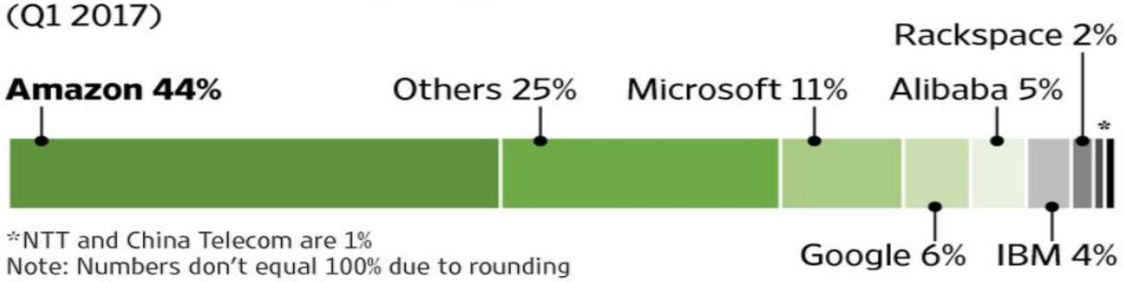
The mass migration to remote work and growing pressure to control costs are accelerating the transition to cloud-based computing and cybersecurity solutions.

Cloud computing proves worth as pandemic pressure-tests security, productivity

Cloud Competition

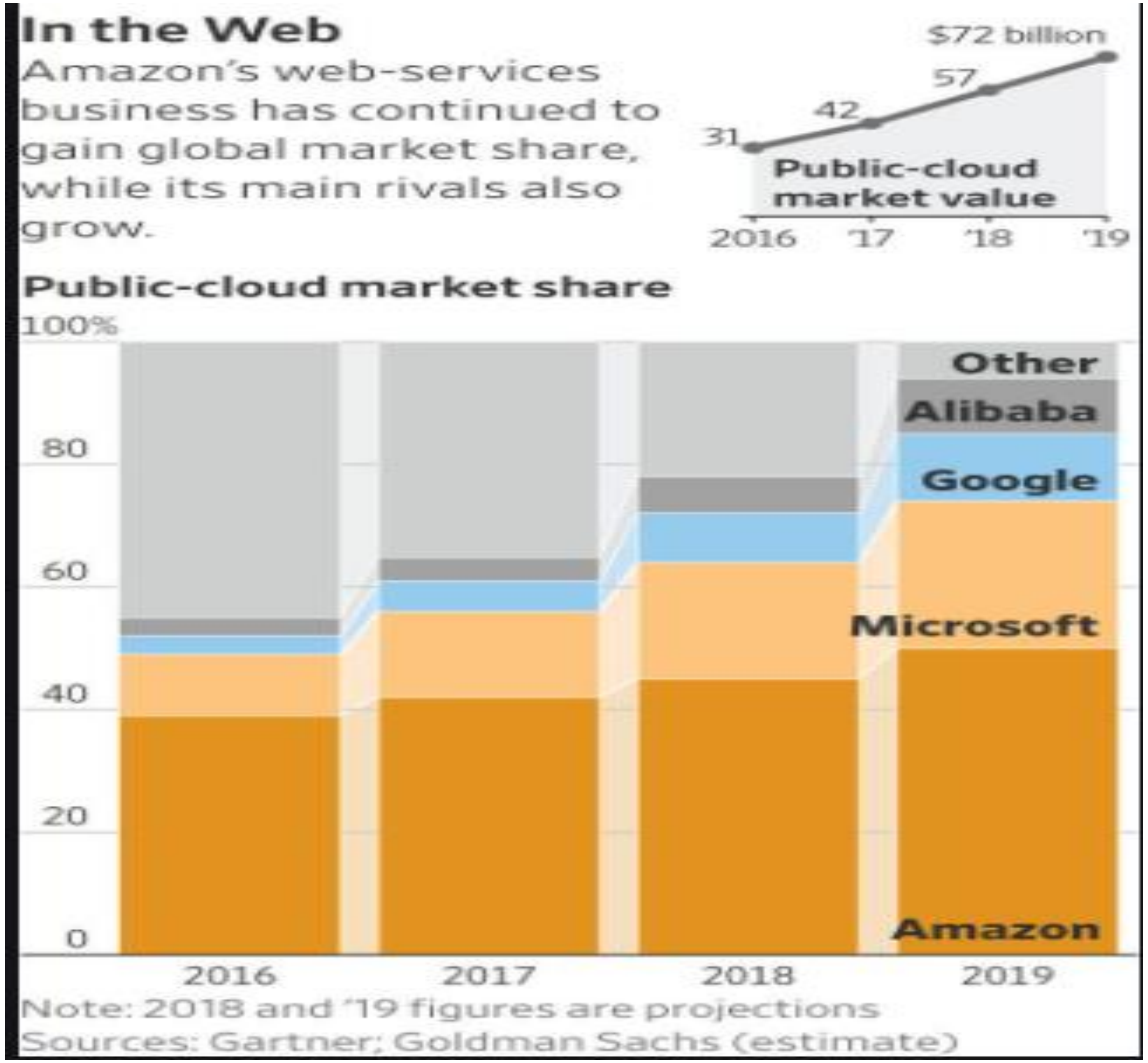
Amazon dominates the business of providing cloud-computing infrastructure, though Microsoft may gain some ground with the retailer's rivals.

World-wide cloud-computing infrastructure market share (Q1 2017)



*NTT and China Telecom are 1%
Note: Numbers don't equal 100% due to rounding
Source: Synergy Research Group

THE WALL STREET JOURNAL.



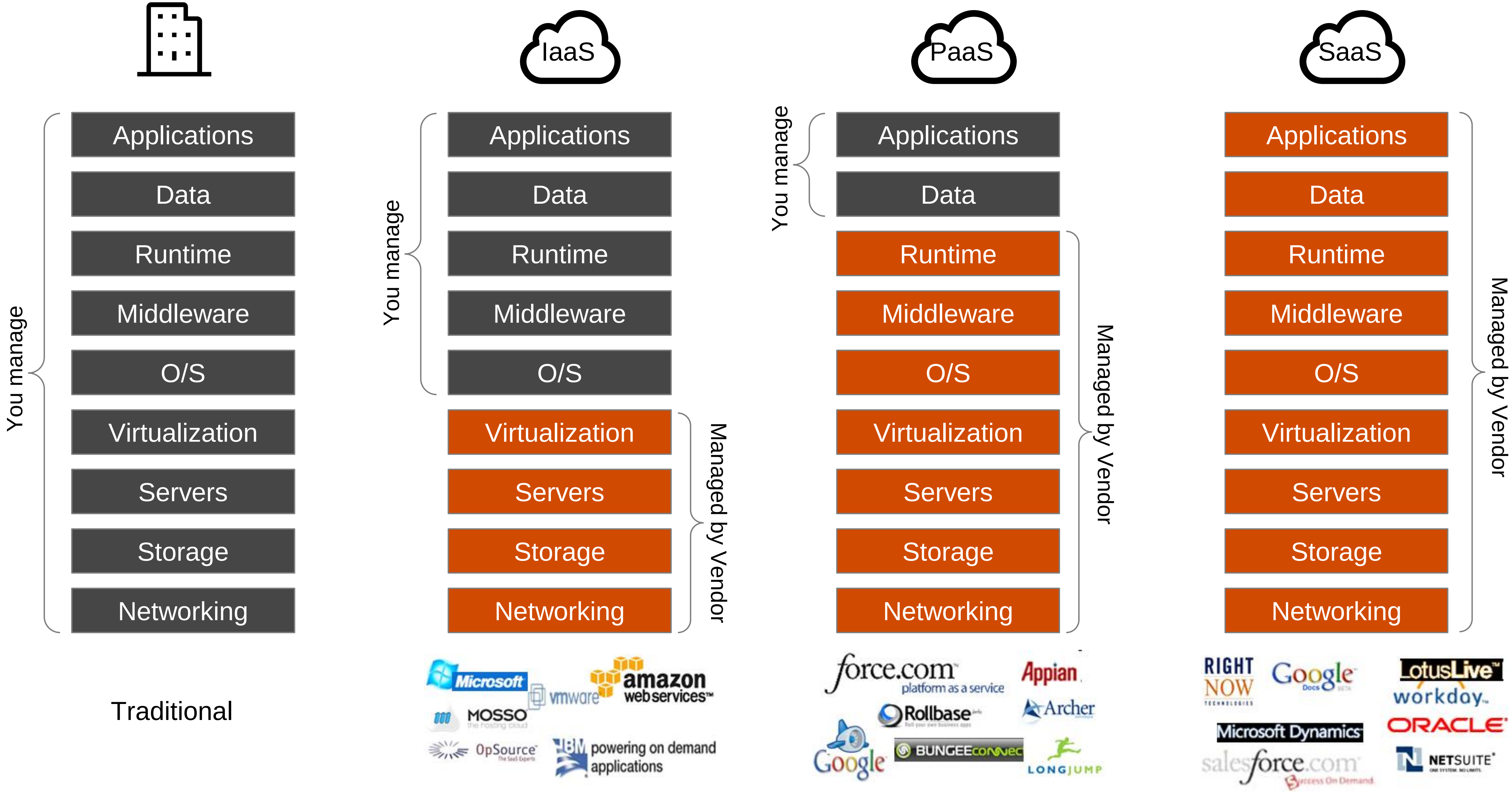
In the Web

Amazon's web-services business has continued to gain global market share, while its main rivals also grow.

Public-cloud market share

Note: 2018 and '19 figures are projections
Sources: Gartner; Goldman Sachs (estimate)

Cloud Computing: Service Models



Traditional

You manage: Applications, Data, Runtime, Middleware, O/S, Virtualization, Servers, Storage, Networking

IaaS

You manage: Applications, Data, Runtime, Middleware, O/S

Managed by Vendor: Virtualization, Servers, Storage, Networking

PaaS

You manage: Applications, Data

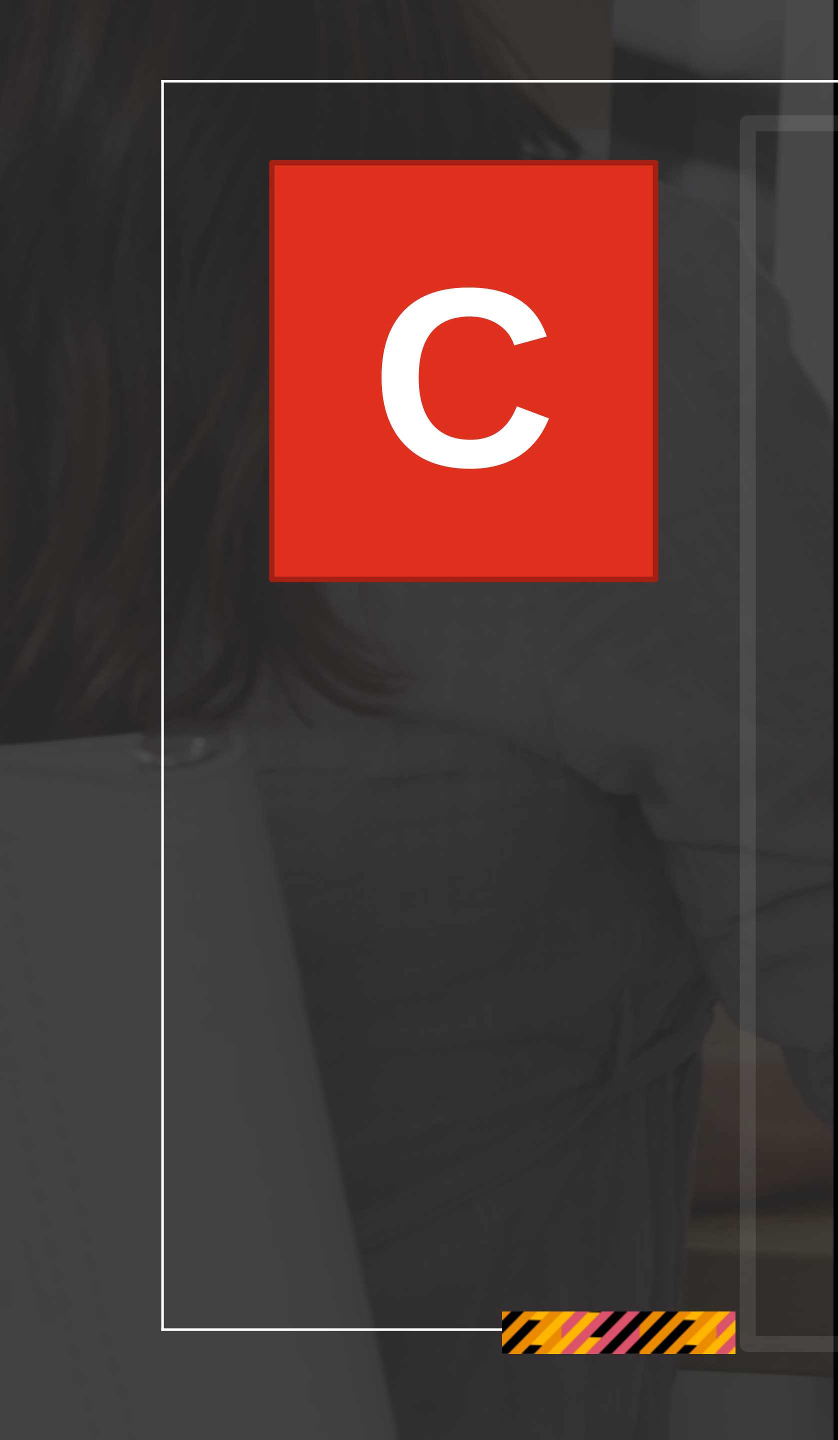
Managed by Vendor: Runtime, Middleware, O/S, Virtualization, Servers, Storage, Networking

SaaS

Managed by Vendor: Applications, Data, Runtime, Middleware, O/S, Virtualization, Servers, Storage, Networking

Cloud Computing: Deployment Models

	Definition	Advantage	Disadvantage
Public Model	● Available over the internet to the public. ● Accessible by a pay-as-you-use basis ● E.g AWS, Azure, Force.com	● Time Saving ● Cost effective ● Pay-as-you-Use	● Higher security risk ● Lack of customization
Private Model	● Internal to a single organization. ● Accessible to a limited number of users behind a firewall. ● E.g Openstack, Apache	● Higher privacy and security ● Customizable environment ● Improved reliability and server control	● High cost ● Opex is borne by the business
Hybrid Model	● Combination of both Public and private Model ● E.g AWS, VMware, Rackspace	● Cost-efficient ● Control and flexibility ● Improved organizations agility to build and test new software	● Might lead to higher operational cost ● High cost of initial assembling



C

Cloud Environment Attack Vectors

Cloud Security Threats

Cloud Security Alliance (CSA) recently released their Top Threats to Cloud Computing. This report released in September lists the top cloud threats that occurred in 2019. They used surveys and questionnaires as instruments of study.

S/N	Cloud Threat	Description	How to remediate/Recommendations
1	**Data Breaches**	Breaches can cause great reputational and financial damage. They could potentially result in loss of intellectual property (IP) and significant legal liabilities.	• Attackers want data, so businesses need to define the value of its data and the impact of its loss. • Who has access to data is a key question to resolve to protect it. • Internet-accessible data is the most vulnerable to misconfiguration or exploitation. • Encryption can protect data, but with a trade-off in performance and user experience. • Businesses need robust, tested incident response plans that take cloud service providers into account.
2	**Misconfiguration and inadequate change control**	Poor change control practices for most of the misconfiguration errors as well as complexity of cloud-based resources. CSA cites the Exactis incident where the provider left an Elasticsearch database containing personal data of 230 million US consumers publicly accessible due to misconfiguration.	• Use automation and technologies that scan continuously for misconfigured resources. • Implement change management control practices
3	**Lack of cloud security architecture and strategy**	The desire to minimize the time needed to migrate systems and data to the cloud usually takes precedence over security. As a result, the company becomes operational in the cloud using security infrastructure and strategies that were not designed for it.	• The security architecture needs to align with business goals and objectives. • Develop and implement a security architecture framework. • Keep threat models up to date. • Deploy continuous monitoring capability

Cloud Security Threats (cont'd)

S/N	Cloud Threat	Description	How to remediate/Recommendations
4	**Insufficient identity, credential, access and key management**	The report notes that the cloud requires organizations to change practices related to identity and access management (IAM). Consequences of not doing so, according to the report, could result in security incidences and breaches	• Secure accounts, including the use of two-factor authentication. • Use strict identity and access controls for cloud users and identities--in particular, limit the use of root accounts. • Segregate and segment accounts, virtual private clouds and identity groups based on business needs and the principle of least privilege. • Take a programmatic, centralized approach to key rotation. • Remove unused credentials and access privileges.
5	**Account hijacking**	Account hijacking remains the fifth biggest cloud threat this year. As phishing attempts become more effective and targeted, the risk of an attacker gaining access to highly privileged accounts is significant. Phishing is not the only way an attacker can gain credentials. They can also acquire them by compromising the cloud service itself or stealing them through other means.	• Don't just do a password reset when account credentials are stolen. Address the root causes. • A defense-in-depth approach and strong IAM controls are the best defense • Implement rigorous cybersecurity awareness training against social engineering
6	**Insider threats**	Threats from trusted insiders are just as serious in the cloud as they are with on-premise systems. Insiders can be current or former employees, contractors, or a trusted business partner—anyone who doesn't have to break through a company's defenses to access its systems. CSA cites the Ponemon Institute's 2018 Cost of Insider Threats study, which states that 64% of all reported insider incidents were due to employee or contractor negligence.	• Conduct employee training and education on proper practices to protect data and systems. • Make cybersecurity education an ongoing process. • Regularly audit and fix misconfigured cloud servers. • Restrict access to critical systems.

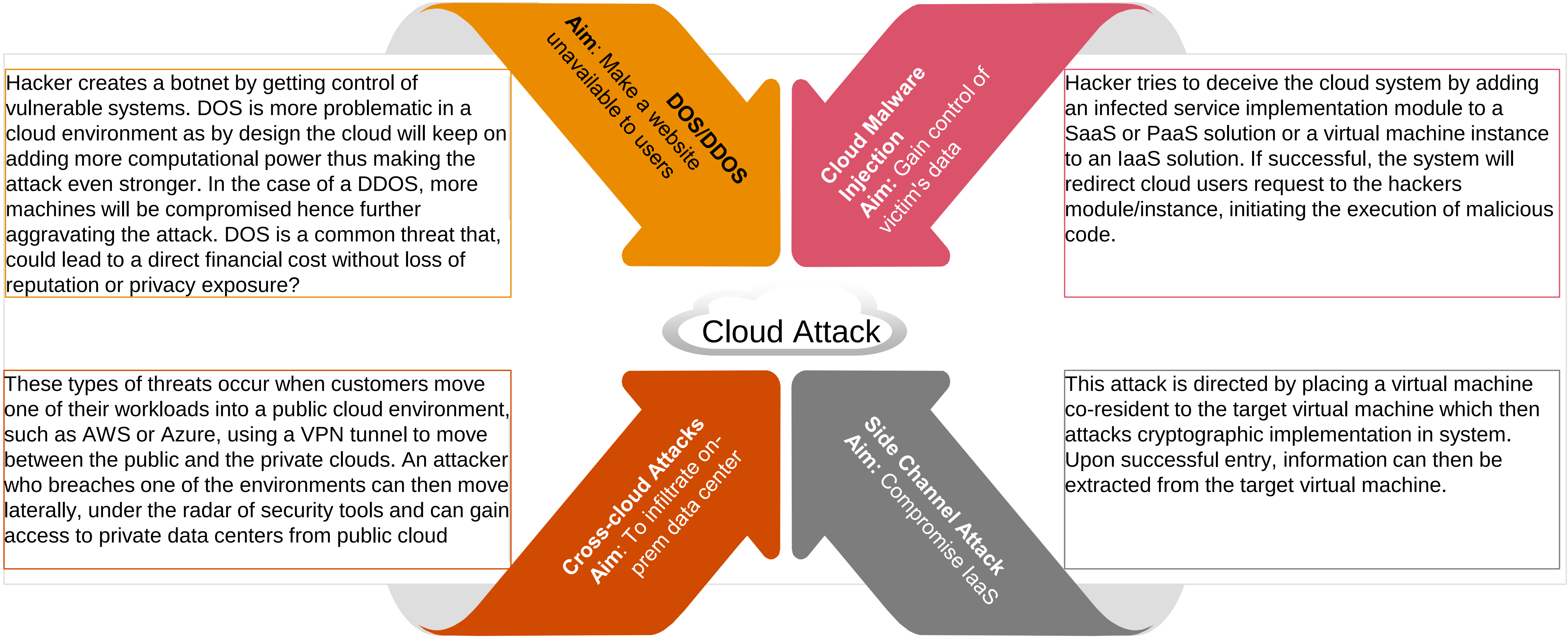
Cloud Security Threats (cont'd)

S/N	Cloud Threat	Description	How to remediate/Recommendations
7	**Insecure interfaces and APIs**	In 2018, Facebook experienced a breach that affected more than 50 million accounts that was the result of a vulnerability introduced in its View As feature. Especially when associated with user interfaces, API vulnerabilities can give attackers a clear path to stealing user or employee credentials.	• Employ good API practices such as oversight of items like inventory, testing, auditing and abnormal activity protections. • Protect API keys and avoid reuse. • Consider an open API framework such as the Open Cloud Computing Interface (OCCI) or Cloud Infrastructure Management Interface (CIMI).
8	**Weak control plane**	According to the CSA, The control plane is weak if the person in charge of these processes does not have full control over the data infrastructure's logic, security and verification. The administrators need to understand the security configuration, how data flows, and the architectural blinds spots or weaknesses. Failure to do so could result in data leakage, unavailability of data, or data corruption.	• Make sure the cloud service provider offers the security controls needed to fulfill legal and statutory obligations. • Perform due diligence to ensure the cloud service provider possesses an adequate control plane
9	**Metastructure and applistructure failures**	A CSP metastructure holds security information on how it protects its systems, and it discloses that information via API calls. CSA calls the metastructure the CSP/customer "line of demarcation" or "waterline." The APIs help customers detect unauthorized access, but also contain highly sensitive information such as logs or audit system data	• Make sure the CSP offers visibility and exposes mitigations. • Implement appropriate features and controls in cloud-native designs. • Make sure the CSP conducts penetration testing and provides findings to customers.

Cloud Security Threats (cont'd)

S/N	Cloud Threat	Description	How to remediate/Recommendations
10	**Limited cloud usage visibility**	A common complaint among security professionals is that a cloud environment makes them blind to much of the data they need to detect and prevent malicious activity. This is a result of shadow APIs (unsanctioned use) and sanctioned use misuse	• Develop a cloud visibility effort from the top down that ties into people, processes, and technology. • Conduct mandatory company-wide training on accepted cloud usage policies and enforcement. • Have the cloud security architect or third-party risk management personnel review all non-approved cloud services. • Invest in a cloud access security broker (CASB) or software-defined gateways (SDG) to analyze outbound activities. • Invest in a web application firewall to analyze inbound connections. • Implement a zero-trust model across the organization.
11	**Abuse and nefarious use of cloud services**	Attackers are increasingly using legitimate cloud services to support their activities. For example, they might use a cloud service to host disguised malware on sites like GitHub, launch DDoS attacks, distribute phishing email, mine digital currency, execute automated click fraud, or carry out a brute-force attack to steal credentials.	• Have mitigations in place to prevent and detect abuse such as payment instrument fraud or misuse of cloud services. • Monitor employees' cloud usage for abuse. • Employ cloud data loss prevention (DLP) solutions to monitor and stop data exfiltration

Cloud Attack Vectors



DOS/DDOS
Aim: Make a website unavailable to users

Hacker creates a botnet by getting control of vulnerable systems. DOS is more problematic in a cloud environment as by design the cloud will keep on adding more computational power thus making the attack even stronger. In the case of a DDOS, more machines will be compromised hence further aggravating the attack. DOS is a common threat that, could lead to a direct financial cost without loss of reputation or privacy exposure?

Cloud Malware Injection
Aim: Gain control of victim's data

Hacker tries to deceive the cloud system by adding an infected service implementation module to a SaaS or PaaS solution or a virtual machine instance to an IaaS solution. If successful, the system will redirect cloud users request to the hackers module/instance, initiating the execution of malicious code.

Cloud Attack

Cross-cloud Attacks
Aim: To infiltrate on-prem data center

These types of threats occur when customers move one of their workloads into a public cloud environment, such as AWS or Azure, using a VPN tunnel to move between the public and the private clouds. An attacker who breaches one of the environments can then move laterally, under the radar of security tools and can gain access to private data centers from public cloud

Side Channel Attack
Aim: Compromise IaaS

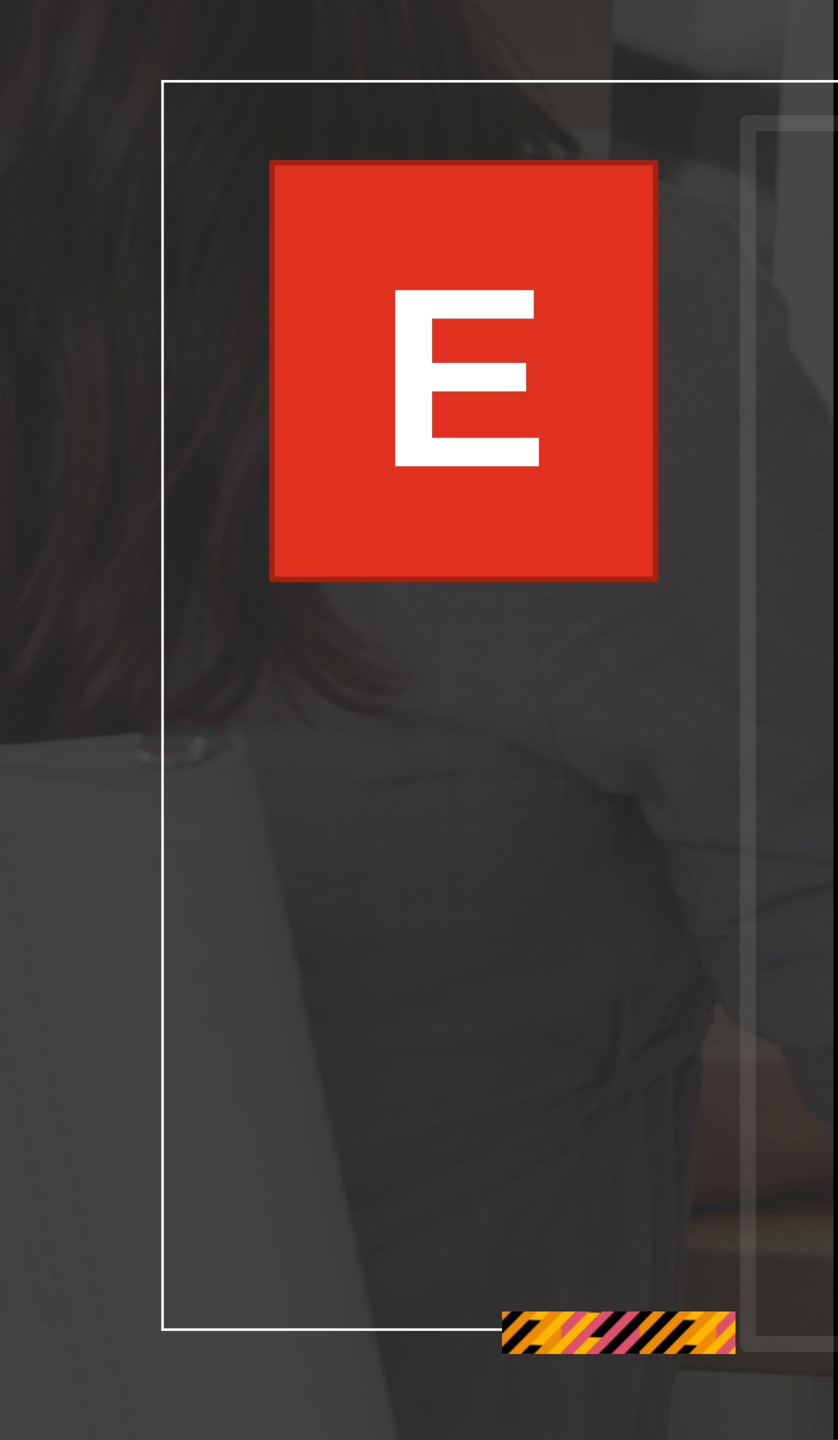
This attack is directed by placing a virtual machine co-resident to the target virtual machine which then attacks cryptographic implementation in system. Upon successful entry, information can then be extracted from the target virtual machine.

D

Cloud Security: Types of Audit Reports

Types of Cloud Audit Reports

Type	Definition	Sub Classes	Who uses it?
SOC 1 **Service Organization Control 1**	This type of reports is strictly for auditing the financial reporting instruments of a corporation. This definitely has nothing to do with Cloud Security	Type 1: Not relevant Type 2:Not relevant	Auditors, users
SOC 2 **Service Organization Control 2**	This report is specifically intended to report audits of any controls on an organization's security, availability, processing integrity, confidentiality, and privacy.	**Type 1**: SOC 2 Type 1 only reviews the design of controls, not how they are implemented and maintained, or their function. SOC 2 Type 1 is not extremely useful for determining the security and trust of an organization. **Type 2:** The SOC 2 Type 2 report is highly detailed and reviews the design of controls, how they are implemented or their functions. Type 2 is the kind of report that is extremely useful for getting a true assessment of an organization's security posture. However, cloud vendors will probably never share an SOC 2 Type 2 report with any customer.	Management, Regulators. Normally shared under NDA
SOC 3 **Service Organization Control 3**	This report contains no actual data about the security controls of the audit target and is instead just an assertion that the audit was conducted and that the target organization passed		Publicly available to anyone
CSA STAR * Cloud Security Alliance Security, Trust, and Assurance Registry (STAR) program	This is a third-party independent assessment of the security of a cloud service provider. The technology-neutral certification leverages the requirements of the ISO/IEC 27001:2013 management system standard together with the CSA Cloud Controls Matrix.	There are 3 levels - Level 1 (Self assessment), Level 2 (3rd Party audit, Level 3 (Continuous Auditing)	Publicly available



E

Cloud Security: Security Measures & Auditing Framework

Cloud Security Measures

Cloud security consists of a set of:

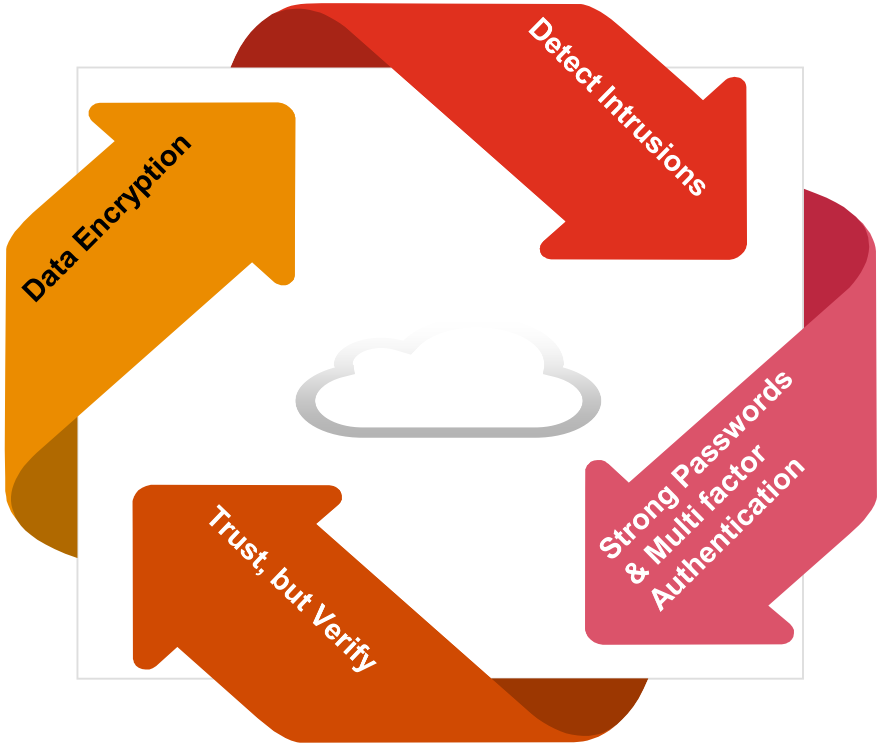
- Policies
- Controls
- Procedures
- Technologies

that works together to protect cloud-based systems, data and infrastructure.

Use a fully managed intrusion detection system that provides network monitoring and notifies about the abnormal behaviour of insiders and intruders.

Data in the cloud environment needs to be encrypted at all stages of its transfer and storage;

- At the source
- In transit
- At rest

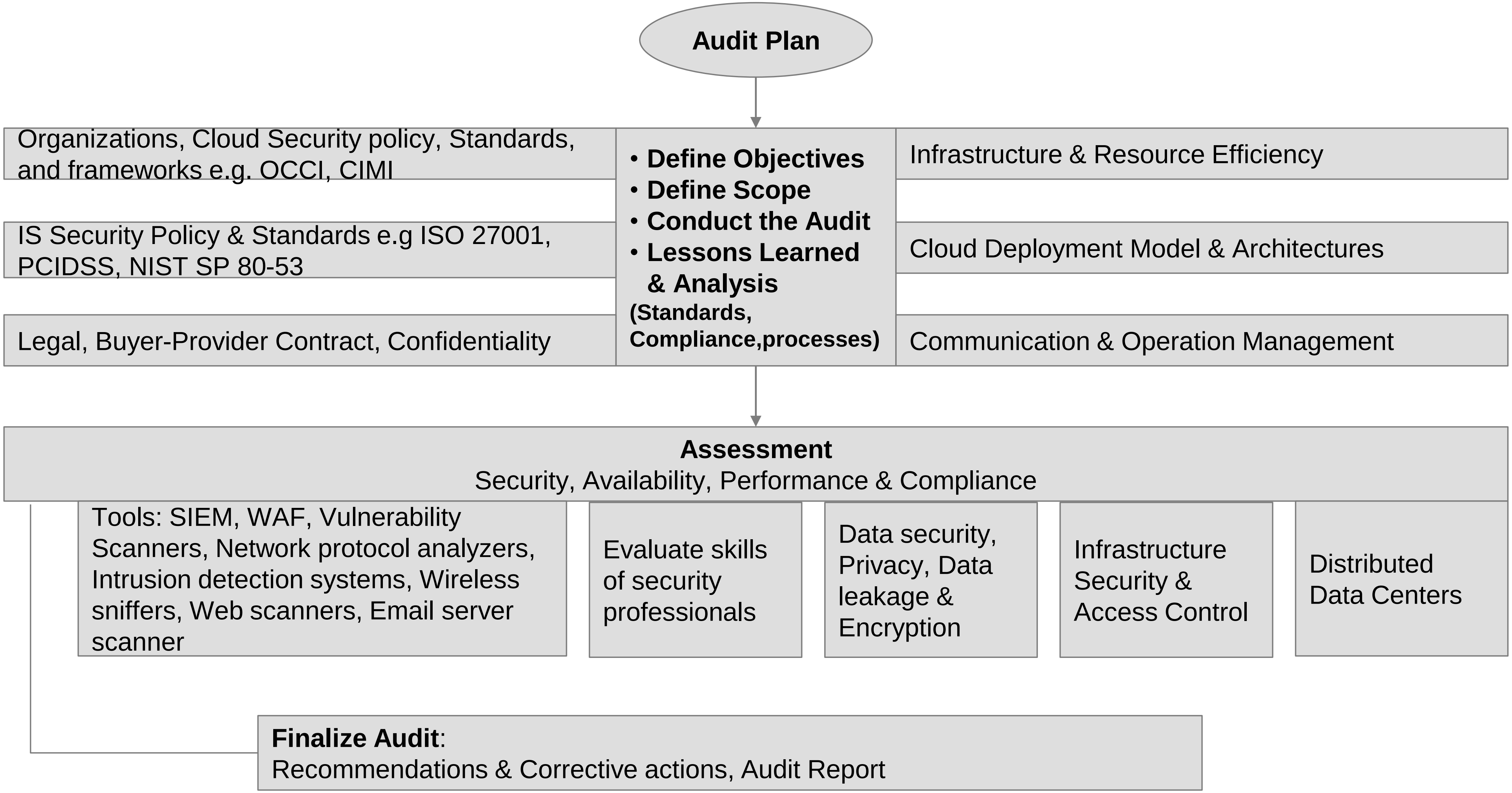


Strong password should include uppercase and lowercase letters, numbers and special symbols.

In addition, employ the use of multi factor authentications like OTP’s

Monitor and continuous audit the activities of your cloud service provider.

Cloud Security: Auditing Framework



Audit Plan

Organizations, Cloud Security policy, Standards, and frameworks e.g. OCCI, CIMI

IS Security Policy & Standards e.g ISO 27001, PCIDSS, NIST SP 80-53

Legal, Buyer-Provider Contract, Confidentiality

- **Define Objectives**
- **Define Scope**
- **Conduct the Audit**
- **Lessons Learned & Analysis**

(Standards, Compliance,processes)

Infrastructure & Resource Efficiency

Cloud Deployment Model & Architectures

Communication & Operation Management

Assessment
Security, Availability, Performance & Compliance

Tools: SIEM, WAF, Vulnerability Scanners, Network protocol analyzers, Intrusion detection systems, Wireless sniffers, Web scanners, Email server scanner

Evaluate skills of security professionals

Data security, Privacy, Data leakage & Encryption

Infrastructure Security & Access Control

Distributed Data Centers

Finalize Audit:
Recommendations & Corrective actions, Audit Report

Cloud Security: Auditing Framework

Governance

Review cloud usage using vendor provided dashboards or logging information

Data Management

- Review Data transit and storage capability of CSP to identify if it is vulnerable at any point
- Review how the CSP ensures data segregation, logical separation and security in a multi-tenancy environment.

Data Environment

- Review CSP Data privacy policy
- If applicable, review the applications & operating systems utilized
- Review frequency of infrastructure (software and hardware) update

Cyber Threat Response

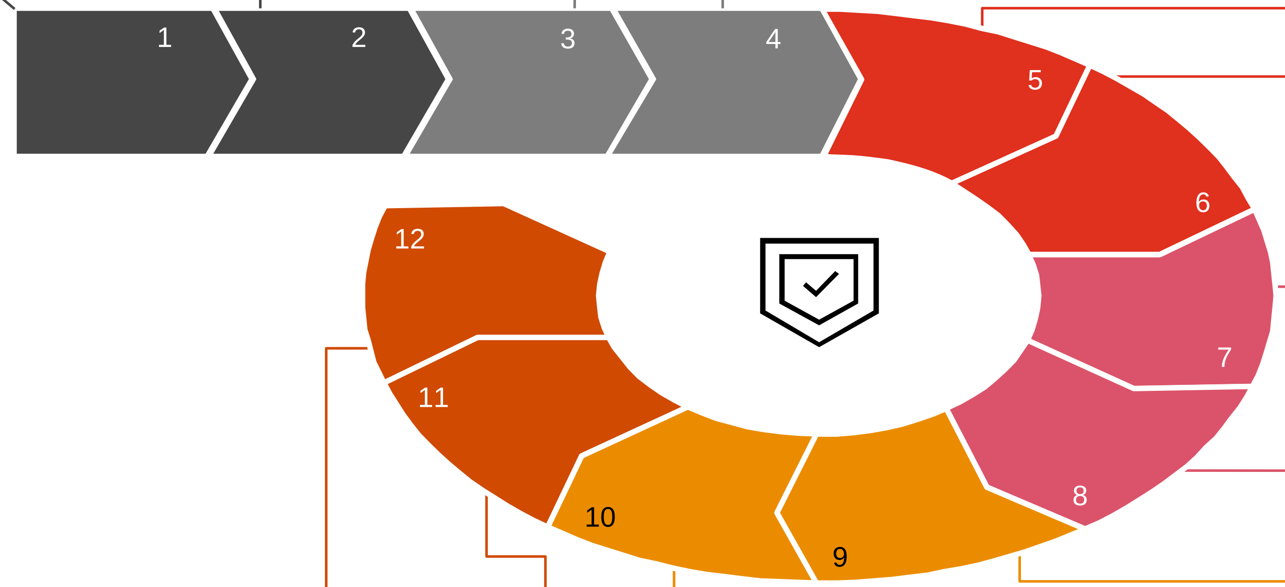
Review CSP's;

- Patch and Vulnerability management practice
- Vulnerability remediation process
- Employed guideline around web application security project

Infrastructure Management

Review CSP's

- Access right management process
- Data handling process
- Ability to troubleshoot performance issues due to continuous environment changes



Logs and Audit trails Management

Review audit trails and logs practice and policy: provision of dedicated storage, tamper proofing of logs and audit trail, and ability of CSP to provide timely forensic investigations

Service Availability

Review CSP's;

- Incident response plan
- Safety guards against Cyber threat vectors
- Capacity to handle peak period load

Identity and Access Management

Review CSP's;

- Physical security measures at its office and server site(s)

Legal

Review SLA for legal rights and obligations around;

- Notification for any data breach.
- Recourse action in the event of security incidents, failure to meet SLA, Disaster recovery or business continuity conditions
- Additional fees for termination of services, delivery or erasure of data

Regulatory Compliance

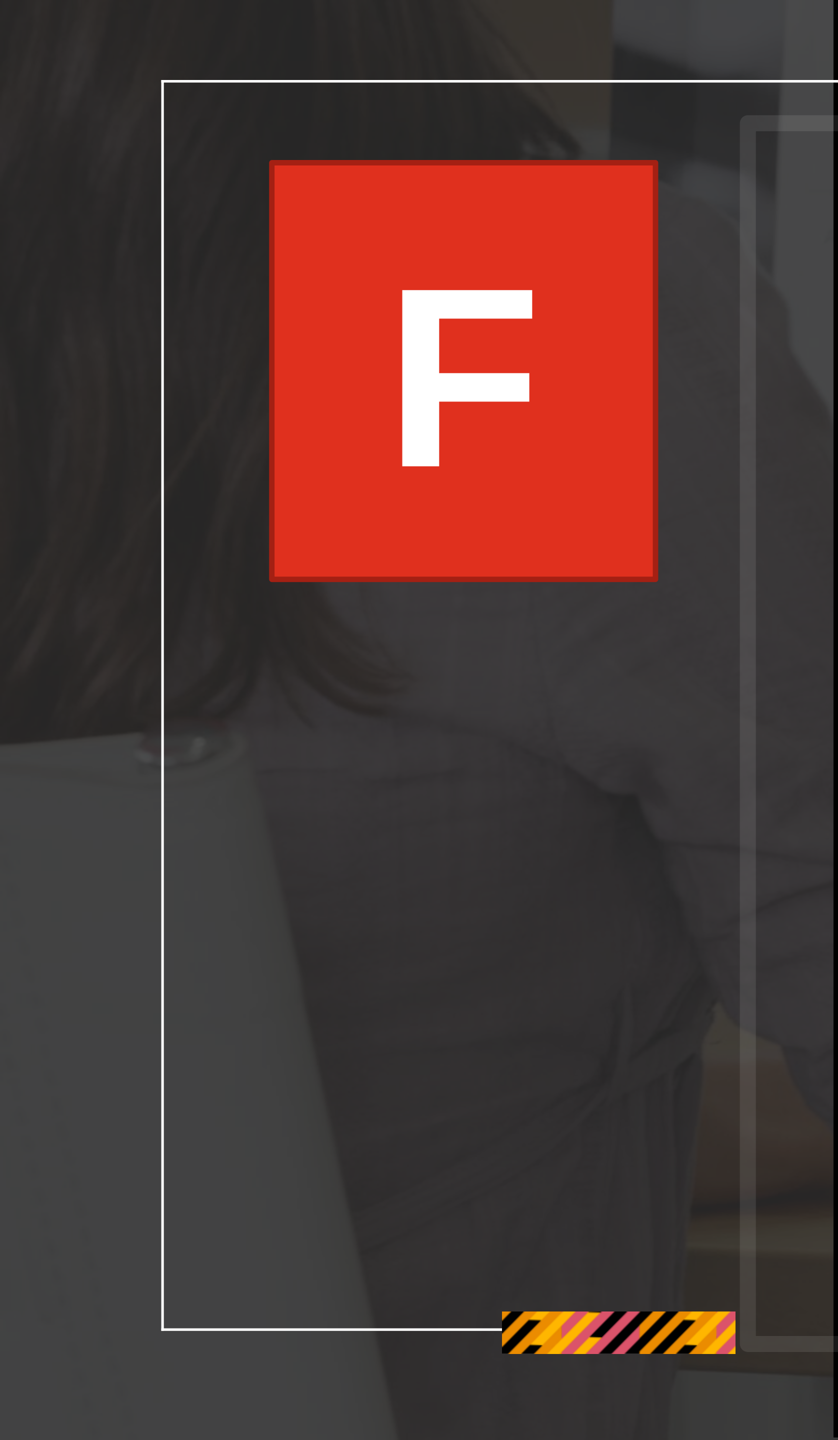
CSP should provide evidence to provide compliance with regulatory requirements and standards (e.g. SOC 2, ISO 27001 & 27002, Cloud security Alliance (CSA), and PCI-DSS)

Privacy

- What data is collated and stored by CSP and how are they managed?
- Under what conditions are regulators granted access to confidential data and to what extent

Encryption

- Is there any encryption utilized for data at rest?
- For data in storage, how are encryption keys stored?
- For data backups that are data encrypted in transit or at rest? How are keys managed?



F

Shadow IT, API deployment in your organisation

Shadow IT and API Deployment

What is Shadow IT?

Shadow IT occurs when a department or end user adopts an application for business purposes without involving the IT department.

Common Shadow IT Applications:

- Unauthorized USB Flash Drives
- Use of personal email addresses
- Unauthorized online file-sharing applications (WhatsApp, etc)
- Unauthorized VoIP (Voice over Internet Protocol) applications (WhatsApp, Instagram)
- OAuth authentication via Corporate Cloud Applications (G-Suite, Microsoft 365) into third party applications (Spotify, etc) using social media (Facebook, Twitter, etc) account.

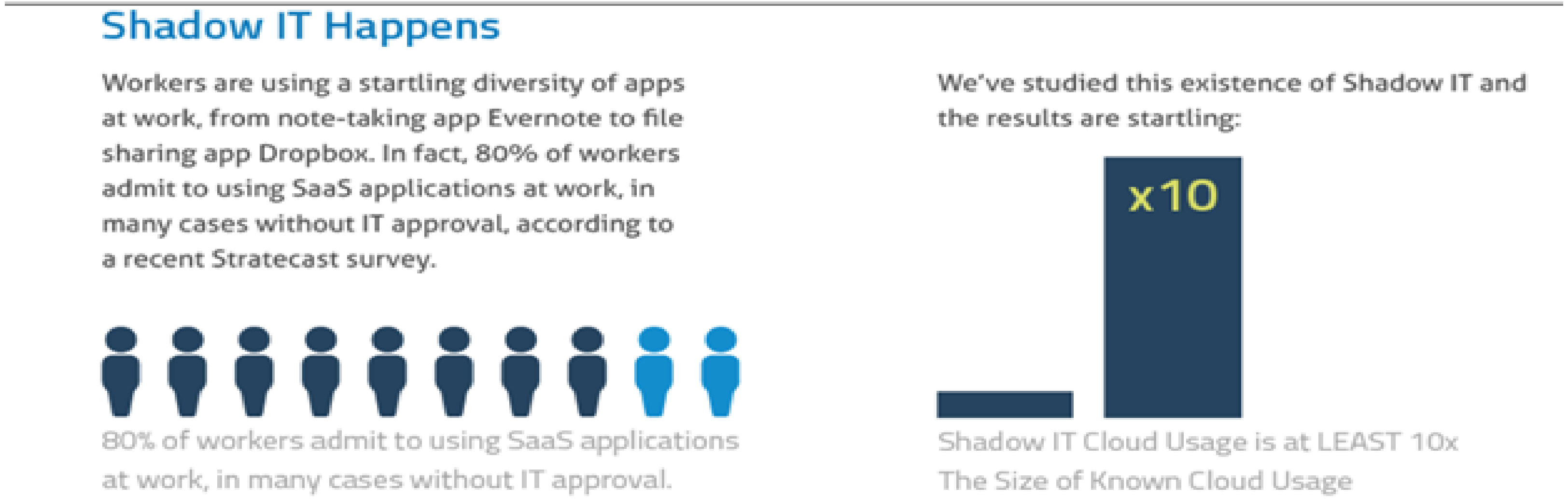
Shadow IT

Expected Shadow IT vs Actual Shadow IT

The average company currently uses **1,083 cloud services** in total.

Unfortunately, legacy management and security products just don't have the visibility to find, understand, or control cloud service usage and risk, leaving IT flying blind.

975
unknown services



Shadow IT Happens

Workers are using a startling diversity of apps at work, from note-taking app Evernote to file sharing app Dropbox. In fact, 80% of workers admit to using SaaS applications at work, in many cases without IT approval, according to a recent Stratecast survey.

80% of workers admit to using SaaS applications at work, in many cases without IT approval.

We've studied this existence of Shadow IT and the results are startling:

Shadow IT Cloud Usage is at LEAST 10x The Size of Known Cloud Usage

Source: McAfee

Drawbacks of Shadow IT

1 **Higher risk of data loss or leaks:** Shadow IT data backup procedures may not be provided or audited. Personnel and contractors in Shadow IT operations may not be put through normal education, procedures or vetting processes. Originators of Shadow IT systems may leave the organization often leaving with proprietary data or leaving behind complicated systems the remainder of staff cannot manage

2 **Wasted time:** Shadow IT adds hidden costs to organizations, consisting largely of non-IT workers in finance, marketing, HR, etc., who spend a significant amount of time discussing and re-checking the validity of certain data, setting up and managing systems and software without experience.

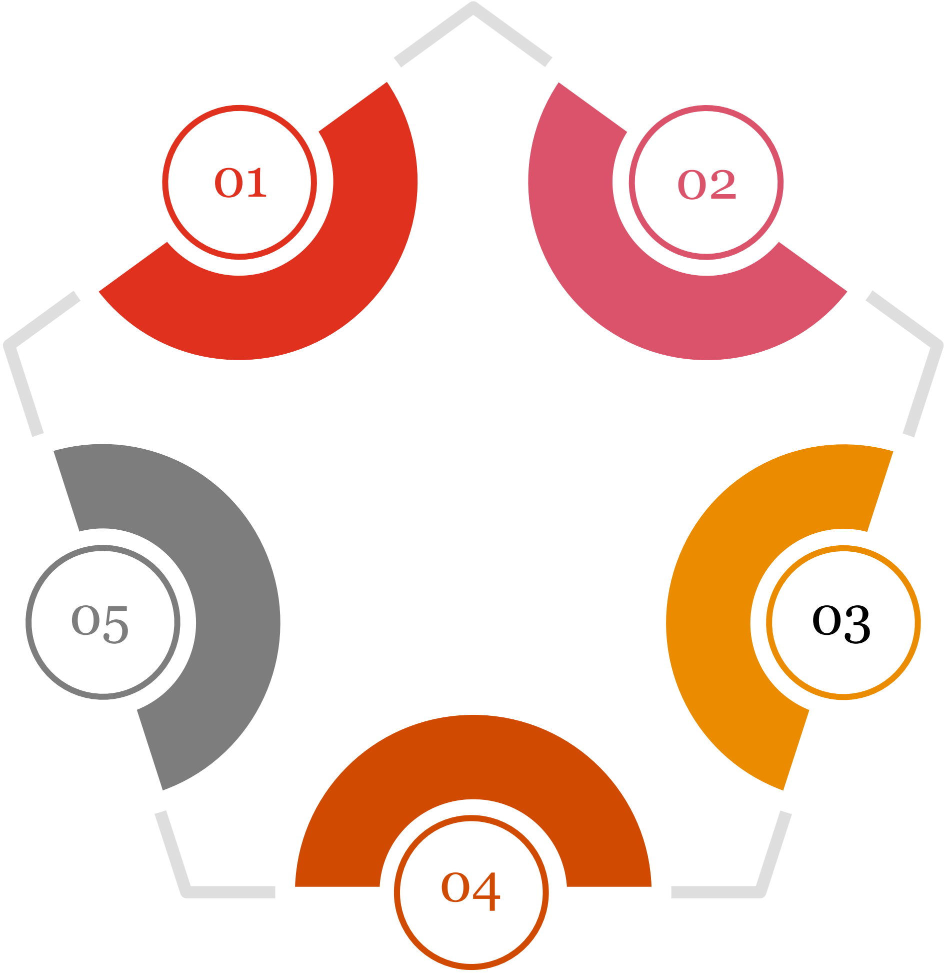
3 **Compliance issues:** Shadow IT increases the likelihood of uncontrolled data flows, making it more difficult to comply with the Sarbanes-Oxley Act (USA) and many other compliance-centric initiatives, such as: Basel II (International Standards for Banking), GLBA (Gramm-Leach-Bliley Act)[10], COBIT (Control Objectives for Information and related Technology)

4 **Inefficiencies:** Shadow IT can be a barrier to innovation by blocking the establishment of more efficient work processes. Additional performance bottlenecks and new single points of failure may be introduced when Shadow IT systems layer on top of existing systems. Data might be exported from a shared system to a spreadsheet to perform the critical tasks or analysis.

5 **Inconsistent business logic:** If a ‘shadow IT’ spreadsheet application encapsulates its own definitions and calculations, it is likely that over time inconsistencies will arise from the accumulation of small differences from one version to another and from one group to another, as spreadsheets are often copied and modified.

6 **Inconsistent approach:** Even when the definitions and formulas are correct, the methodology for doing analysis can be distorted by the arrangement and flow of linked spreadsheets, or the process itself can be wrong.

Shadow IT Security Control Measures



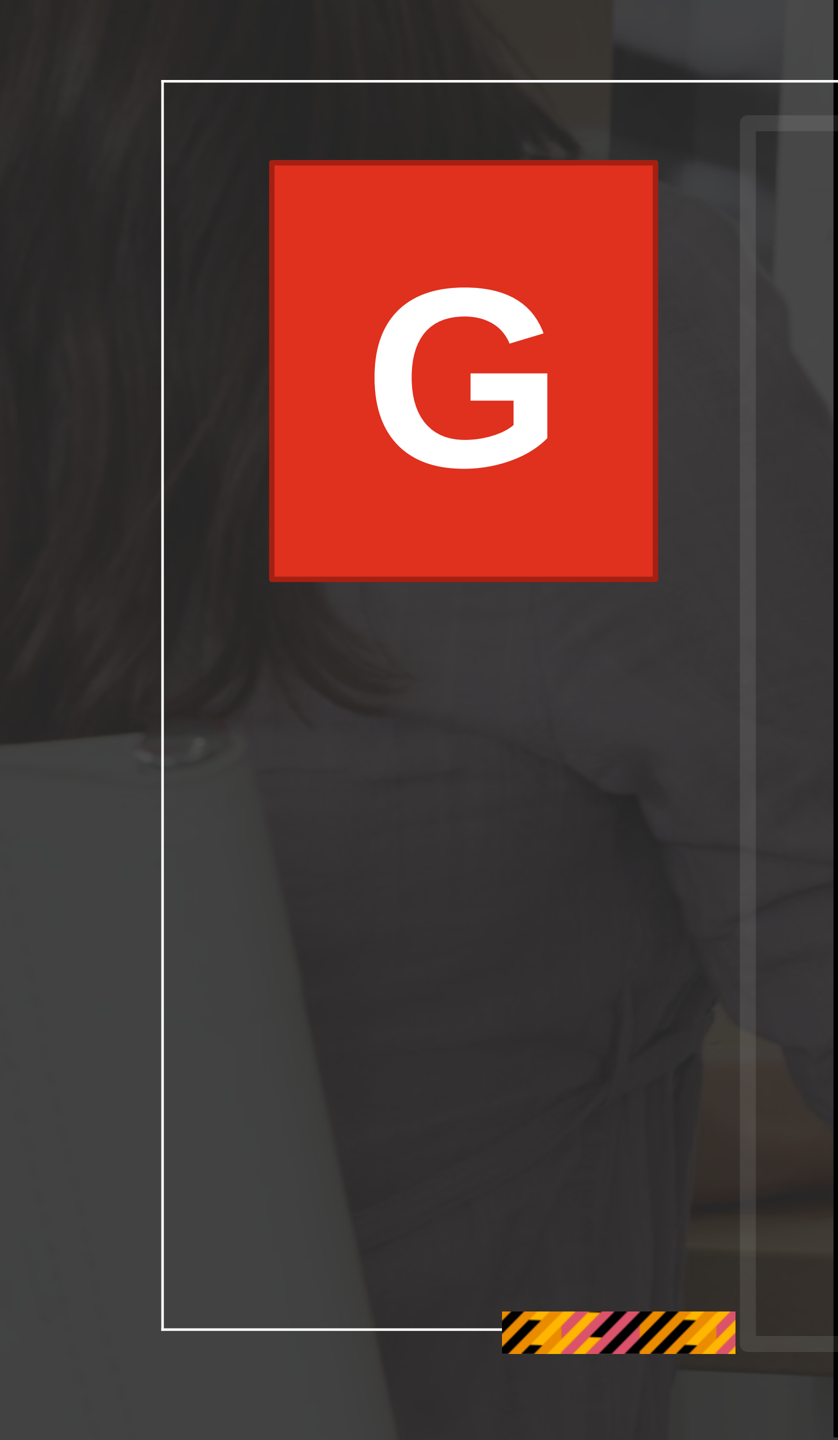
01 **Develop a strategy for resolving business needs**
Organizations should develop a strategy for meeting business needs. Business concerns from employees should be heard and acted upon for quick resolution. This prevents employees or non-IT units from turning to shadow IT to meet their needs.

02 **Leverage clear, easy-to-use tools**
Organizations should ensure that the tools provisioned to for business use are clear and easy-to-use. If such tools are difficult to use, employees or non-IT units will independently use non-approved tools to increase their productivity at work.

03 **Find out what applications are being used**
The internal audit function can be tasked to find out the unapproved applications being used across the organization. This can be achieved through discussions with unit heads, monitoring outbound proxy and web traffic.

04 **Focus on controls**
For unapproved application, organizations should determine how they are being controlled? Are the units/individuals leveraging real-time monitoring? Who has access? What types of external threats exist? Who’s accountable?

05 **Develop a monitoring strategy**
A monitoring strategy can help ensure that any software, extensions, add-ons and/or plugins are clear of malware, viruses, or bots that can pose a significant internal threat to your data and applications.



Cloud Security Risks, Compliance, Data Privacy and Protection

Cloud Security Risks, Compliance, Data Privacy and Protection

Loss of Visibility

Most companies will access a range of cloud services through multiple devices, departments, and geographies. This kind of complexity in a cloud computing setup can cause you to lose visibility of access to your infrastructure.

Lack of Cloud Security Strategy and Architecture

This a cloud security risk that you can easily avoid, but many don’t. In their haste to migrate systems and data to the cloud, many organizations become operational long before the security systems and strategies are in place to protect their infrastructure.

Contractual Breaches

Any contractual partnerships you have will include restrictions on how any shared data is used, how it is stored, and who is authorized to access it. Your employees unwittingly moving restricted data into a cloud service without authorization could create a breach of contract.

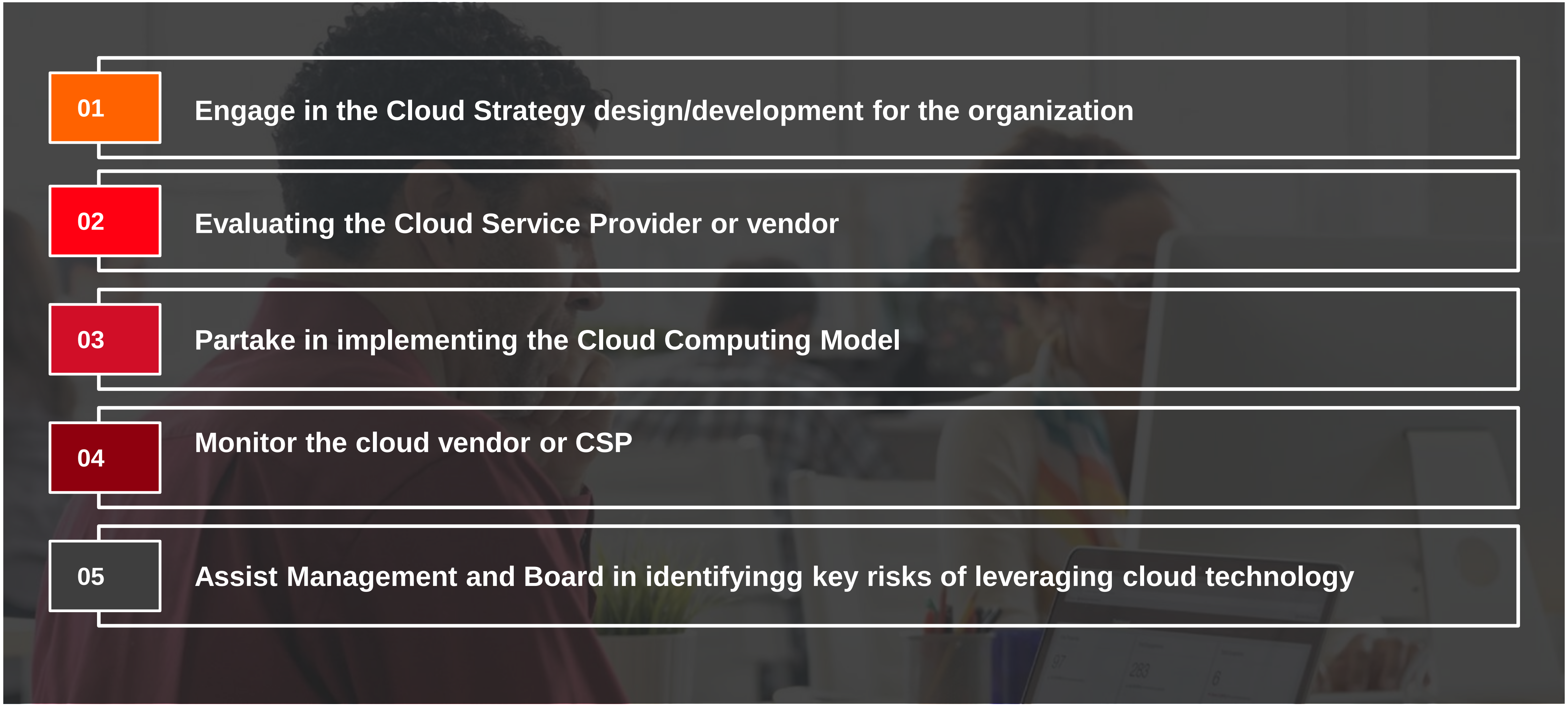
Insecure Application Programming Interface (API)

External-facing APIs can introduce a cloud security risk. Any insecure external API is a gateway offering unauthorized access by cybercriminals looking to steal data and manipulate services.

Misconfiguration of Cloud Services

Misconfiguration of cloud services is another potential cloud security risk. With the increased range and complexity of services, this is a growing issue. Misconfiguration of cloud services can cause data to be publicly exposed, manipulated, or even deleted.

Internal Auditor’s Role in Cloud Security in an organization



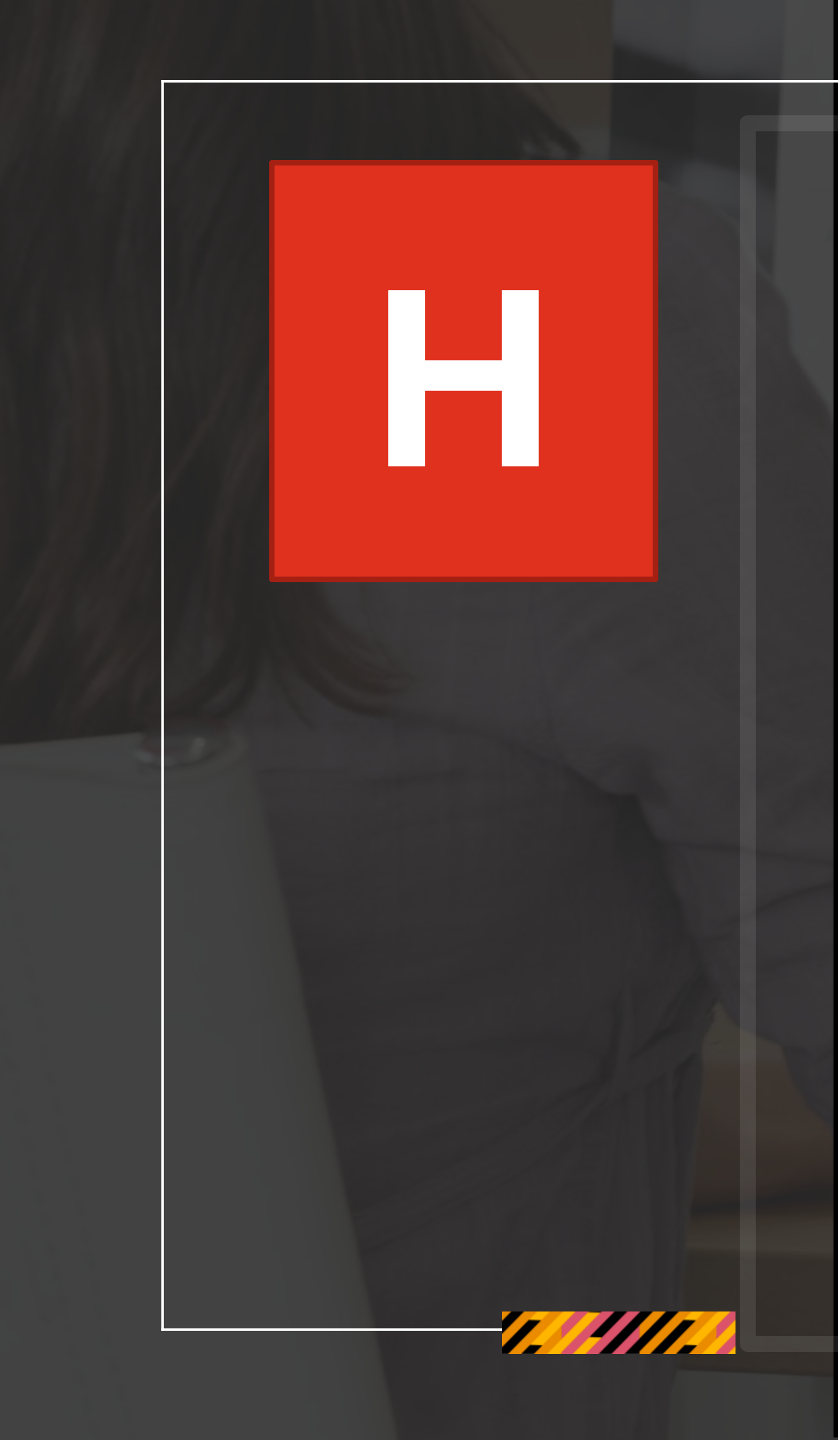
01 Engage in the Cloud Strategy design/development for the organization

02 Evaluating the Cloud Service Provider or vendor

03 Partake in implementing the Cloud Computing Model

04 Monitor the cloud vendor or CSP

05 Assist Management and Board in identifyingg key risks of leveraging cloud technology



H

Basic understanding of VPN Infrastructure

VPN Infrastructure

What is a Virtual Private Network (VPN)

According to Wikipedia, a virtual private network (VPN) extends a private network (enterprise network) across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

How VPN works - A Case Study

Alice works for XYZ Corp as the Chief Internal Auditor. Due to Covid-19, employees of XYZ Corp. are working from home but Alice is unable to access the software needed to carry out her duties via her home WiFi. To solve this problem, the Chief Technology Officer for XYZ Corp. sets up an intermediary network that employees can connect to which in turn connects them to the private network in the office.

Challenges with VPN Implementation

01

Authentication Risks
Key to any VPN strategy is providing extremely strong authentication of users and their devices attempting to connect. In a simple deployment at least, anyone able to connect and authenticate to a VPN endpoint is the same as someone walking into your headquarters and plugging in their computer.

02

VPN Server Risks
Companies need to monitor the VPN servers closely, both for CPU and memory usage as well as configuration changes and evidence of denial-of-service attacks.

03

Remote Worker Bandwidth and Network Concerns
Not all workers have high-speed Internet at home. VPNs are not cheap in terms of bandwidth and can be quite sensitive to network quality when it comes to performance.

04

Endpoint Risks
Remote workers may have to use computers they have at home. These may be unpatched computers with several vulnerabilities and may already be infected with malware Such vulnerabilities and malware can take advantage of the connection opportunity to a VPN to infect other machines, including critical systems within the enterprise.

Solutions

01 Organizations can authenticate VPN users in a variety of ways, ranging from authenticating the username and password against Microsoft’s Active Directory and also encouraging multi-factor authentication. Companies should also monitor authentication systems closely for evidence of brute force and credential stuffing attacks.

02 Companies must watch, protect, and provision their VPN servers to withstand attack, as the alternative is turning them off. it’s important to use robust encryption with the VPN. VPNs are, at their root, devices designed to prevent malicious actors from inspecting traffic on an unsecured link. To do this, they use encryption—and this encryption must be resistant to attack and free of known vulnerabilities.

03 Companies need to limit remote workers to only those systems necessary to do their jobs and to encourage them to avoid heavy movement of data with those systems to preserve network bandwidth for others.

04 Organizations should ensure that the devices allowed to connect to the VPNs are corporate-managed, fully patched systems, with certificates for authentication, strong passwords, and endpoint protection software installed. These can be managed remotely just as when they are on the LAN, and many VPNs offer facilities for detecting if the machines connecting to them meet specific security policies in terms of patch level or installed software.

Thank you!

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 155 countries with over 284,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com