ROBOTIC PROCESS AUTOMATION (RPA) & AUDIT

DAVID GRAFF, MANAGING DIRECTOR INTEGRATED RISK MANAGEMENT PRACTICE, FOCAL POINT DATA RISK

CHRISTOPHER JURS, VP, CYBERSECURITY AND DATA PRIVACY

WEBINAR INFORMATION & QUICK TIPS

- The Presentation Deck can be downloaded from the **MATERIALS** window.
- Windows can be hidden or expanded to fit your preference.
- Submit questions in the **Q&A** window.
- Use the **HELP** icon at the bottom for FAQ’s and system requirements.
- Please click on the **ISACA Customer Experience Center** image to be redirected to ISACA’s customer support page.

ISACA

CPE CERTIFICATE & CREDIT

LIVE EVENT & ON DEMAND RECORDING

- You must view the **Live** or **On-demand** recorded webinar for at least the required amount of time (100 minutes). We encourage you to stay on and watch the entire webinar.

- Check the **CPE Credit and Certificate** window to see the timer.

- Once the required amount of time has been completed – the CPE Certificate will automatically appear in the **ISACA CPE RECORDS** tab on the **MyISACA** page in your ISACA account.

- Please be patient. Your CPE Certificate will appear in your account approximately **1-2 hours** after the webinar concludes.

ISACA

TODAY'S SPEAKER

David Graff

Managing Director, Integrated Risk Management
Focal Point Data Risk

David is a Managing Director in Focal Point's Advisory practice. He has approximately 20 years of experience with ERM/GRC, audit, risk management, internal control frameworks, strategic governance, and financial and operational processes within both industry and professional services roles.

He served as Chief Audit Executive for a large publicly traded water utility, responsible for leadership of all aspects of the internal audit function and SOX compliance, ERM, and providing support to internal ethics investigations.

David also served in executive leadership roles in industry having responsibility for business process transformation in areas of payroll, HR, and accounts payable. David is a Certified Public Accountant and Certified Internal Auditor.

TODAY'S SPEAKER

Christopher Jurs

VP, Cybersecurity and Data Privacy
Focal Point Data Risk

Chris manages a large team of risk management professionals, oversees the delivery of engagements for Focal Point clients, and innovates market-leading solutions in the security, privacy, and compliance space.

Chris has extensive experience in conducting privacy and cybersecurity assessments such as GDPR, CCPA, HIPAA, NIST CSF, Privacy Program Maturity, and has assisted clients with their transition from assessments to programmatic remediation projects.

Chris is well versed in cybersecurity and data privacy strategy and governance, having deep knowledge in evaluating controls related to identity and access management, incident response, logging and monitoring, and the integration between data protection and compliance, operations, and sales functions.

AGENDA

What are we talking about today?

- Digital Transformation and Internal Audit – David Graff – 60 minutes
- Data Privacy Landscape and Audit – Christopher Jurs - 60 minutes

LEARNING OBJECTIVES

Digital Transformation and Internal Audit

At the end of this module attendees should be able to:

- Describe what digital transformation is
- Understand how RPA can fit into their company processes
- Understand RPA – what it is, what it isn't, and how it can be leveraged in business processes
- Understand use case examples for RPA and the benefits derived
- Understand and explain Internal Audit's various roles related to digital transformation and RPA

DIGITAL TRANSFORMATION

WHAT IS DIGITAL TRANSFORMATION?

ISACA

WHAT IS DIGITAL TRANSFORMATION?

Digital transformation is a **foundational change** in how an organization delivers value to its customers.

Digital transformation create new — or modifies existing — business processes, culture, and customer experiences and creates new risks....

Done well, traditional roles like sales, marketing, financial reporting and customer service, **will be more integrated** and will start and end with how you think about, and engage with, customers.

McKinsey interview with Tom Friedman, March 2019….**connectivity has gotten even more intense**….the ability to abstract complexity away has gotten even more rich. And we're taking them both deeper into the economy, so more people, companies, and places can participate in it…..

John Marcante, CIO of Vanguard, points: "Just look at the S&P 500. In 1958, U.S. corporations remained on that index for an average of 61 years, according to the American Enterprise Foundation. By 2011, it was 18 years. Today, companies are being replaced on the S&P approximately every two weeks. Technology has driven this shift, and companies that want to succeed must understand how to merge technology with strategy."

WHERE DOES RPA FIT IN YOUR FIRM'S DIGITAL TRANSFORMATION?

RESPONDING HOLISTICALLY IS CRITICAL

1

Everyone is affected

If you think you won't be affected, you just don't know how yet

2

It's easy to underestimate the pace of change

Time is not on your side

3

Strategy and execution are not enough

The strategy that got you here may not be the one you'll need tomorrow

ISACA

DIGITAL TRANSFORMATION IS ACTIONED BY

Robotics process automation (RPA):

A software solution that runs unattended, working like a virtual employee with legacy applications performing repetitive tasks reliably at the UI level

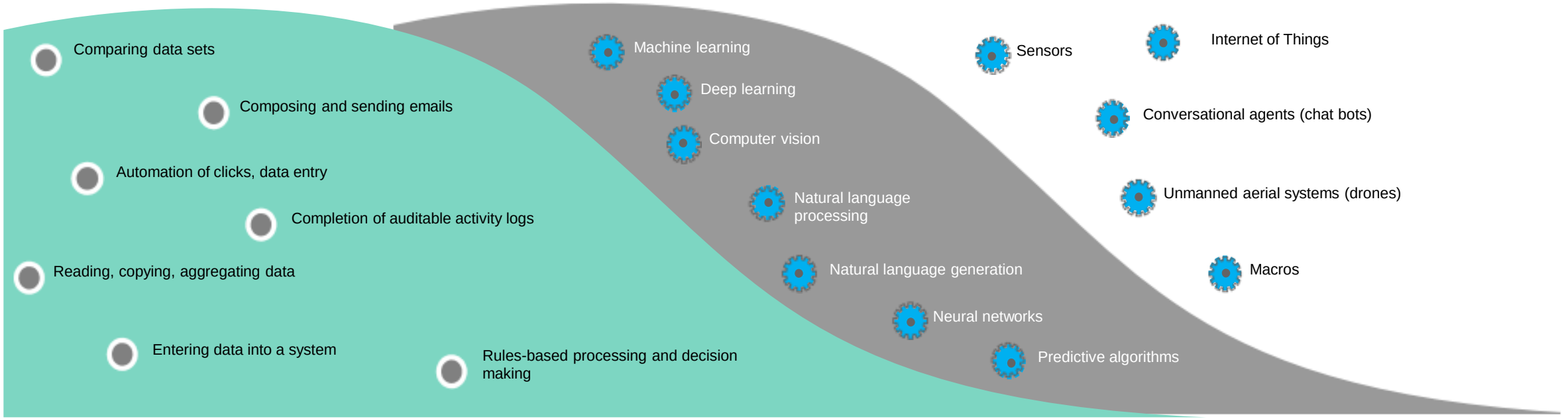
Artificial intelligence (AI):

Software-driven intelligence that mimics human cognition, behavior, and thought processing to

replicate more complex tasks that include professional judgment and historical knowledge

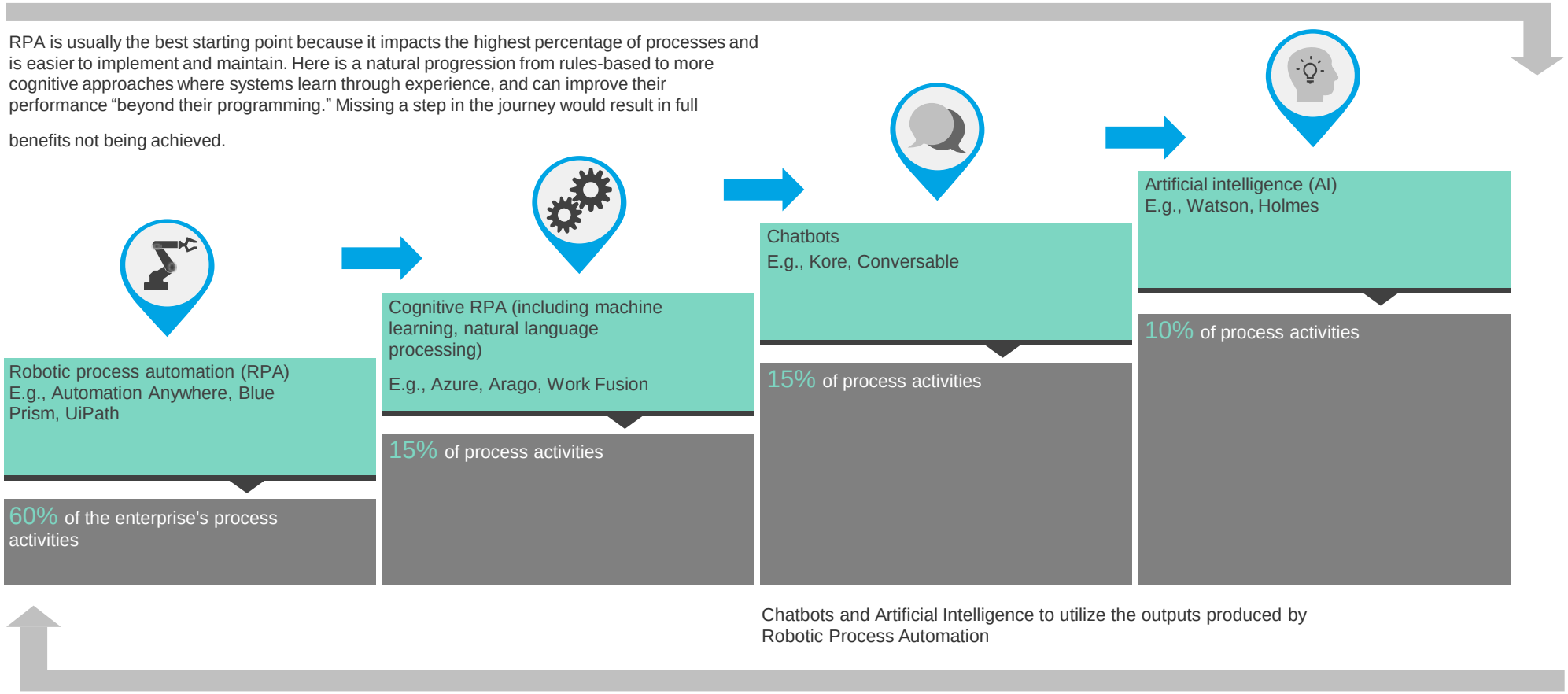
Other:

Complementary technologies, tools and architectures that can be combined with other layers on the spectrum to automate a business process or human experience



THE INTELLIGENT AUTOMATION JOURNEY

The ‘intelligent automation journey’ will most likely progress in stages.



DIGITAL TRANSFORMATION & INTERNAL AUDIT

Every company is a technology company

Emerging risks around business model and digital transformation continue to evolve

IA adds most value by focusing on risks and controls over:

- **DATA**
- **GROWTH**
- **OPTIMIZATION**

GROWTH, DATA & RPA ADOPTION

UiPath + Sumitomo Mitsui = Optimize Data to… Manage Data Growth & Eliminate Inefficiencies

UiPath = Data-Driven Process Automation

…[Robotic Process Automation's (RPA)] benefits compound as employees are freed from the burden of routine, monotonous manual work, enabling them to focus on high-value tasks such as improving customer service, enabling front-line staff to retrieve more data at a faster rate & enhancing every aspect, from the booking experience to customer service support.

This leads to greater employee satisfaction & more productive staff who deliver better customer service experience & positive feedback from customers.

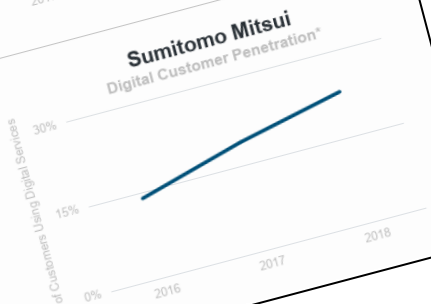
Daniel Dines – UiPath, Founder / CEO, 4/18

Sumitomo Mitsui = Increase Support Capacity

Our key areas of RPA implementation include – information gathering processes used to enhance sales & planning capabilities (customer transaction / industry data) & supporting branch operations (customer performance reports / mortgage loan brochures).

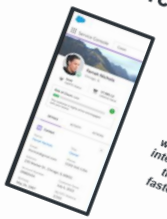
The anticipated 3MM person-hours of productivity to be generated over the next 3 years [by using RPA] will be used to expand value-add operations, like enhancement of sales capacity through improved customer proposals.

Sumitomo Mitsui Financial Group



Salesforce + Adidas = Collect Data to… Increase Customer Input / Improve Products

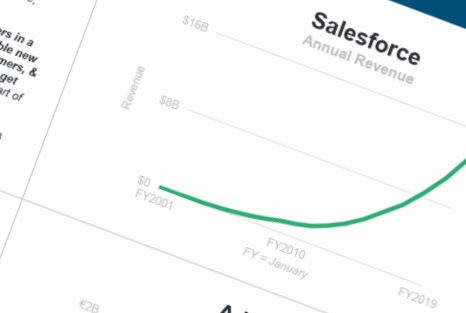
Salesforce = Customer Engagement



…as every company transforms their relationships with their customers…they're fundamentally changing how they sell & how they service, how they market & innovate.

They're connecting with their customers in a whole new way. They're building incredible new intelligent 360-degree views of their customers, & they're using extraordinary new tools to get faster, more informed decisions & at the heart of all this transformation is Salesforce.

Marc Benioff – Salesforce, Co-Founder / Co-CEO, 8/18

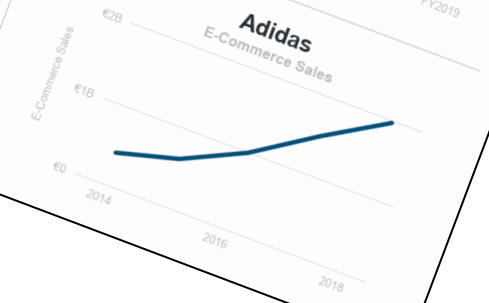


Adidas = Customer Co-Creation

We need to be able to respond to consumer expectations immediately. **The relationship between Adidas & Salesforce allows us to be proactive in our designs** – our ability to roll out new products & influence trends is amazing…

Our direct connection with customers through Salesforce basically makes it happen overnight.

Kasper Rorsted – Adidas, CEO, 6/18



ISACA

ROBOTIC PROCESSING AUTOMATION

WHAT IS ROBOTIC PROCESS AUTOMATION (RPA)?

Robotic process automation (RPA) is the rules-based automation of human activity using specific software applications. RPA 'bots' act as virtual workers through the use of software to manipulate existing application software to process a transaction or complete a process.*

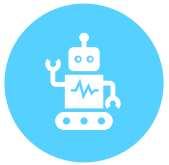
Robots are..

Software applications

Human substitutes for processing for performing repetitive rules-based tasks

Multi-functional, cross-application

Robots are not..



Physical, walking, talking machines

Physical paper processors

Learning machines with two-way voice communication (yet)

ISACA

WHAT IS ROBOTIC PROCESS AUTOMATION IN BUSINESS?

Robotic Process Automation (RPA), is a software application (i.e. “bot”) that can incorporate artificial intelligence and operates assisted or unassisted to automate business process(es), often programmed to perform the same tasks that human beings perform. Benefits of automating internal processes include:

RPA can be used to repeat or “copy” the actions of a human on a machine by performing the same keystrokes, more rapidly.

RPA can be scalable and provide efficiencies and compliance often with less oversight and manual interaction.

Can integrate with company infrastructure and can be highly configured for optimization of a business process.

RPA can reduce human error, increase throughput, and decrease overall costs.

CLEAR, TRACEABLE BENEFITS FROM RPA

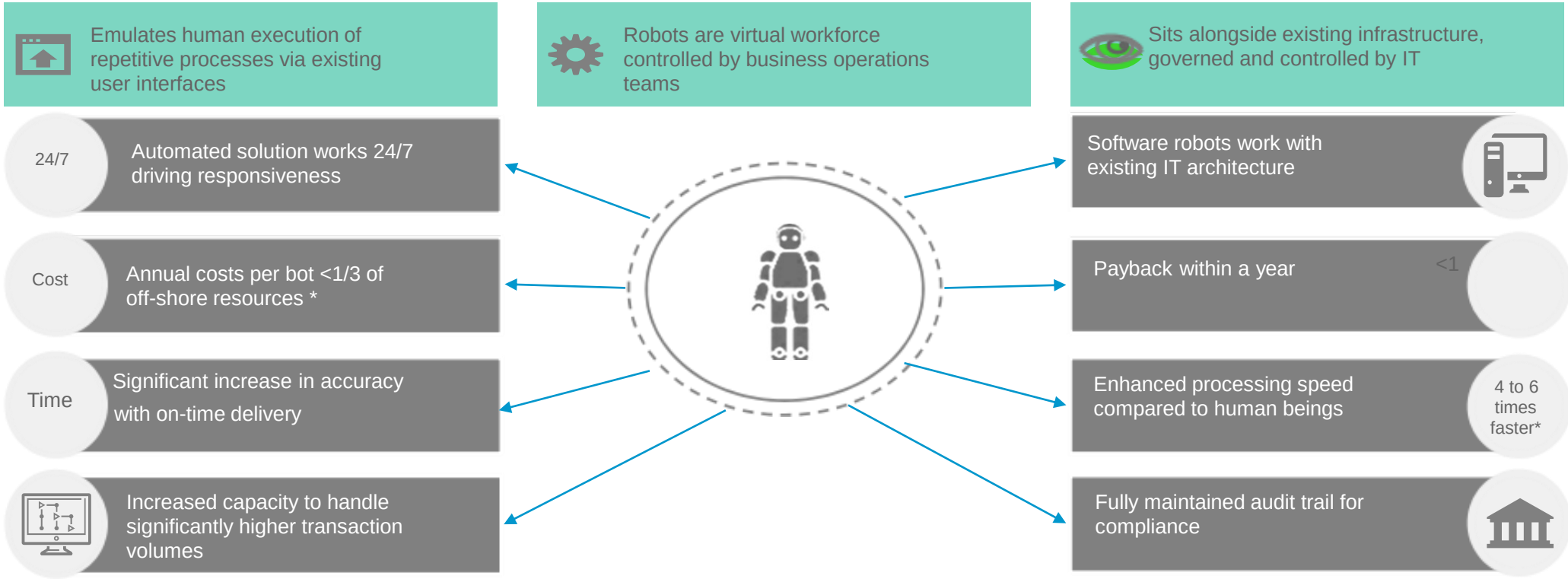
Benefits of RPA	Examples
Savings in human efforts	Reduce people expense by automating frequent manual repetitive tasks, improving exception handling and moving work to best location
Increased value-add talent	Improve knowledge worker value-add by increasing focus on highest return activities (e.g., focus on high value/core competencies – Innovation; Customer analytics; Competitor analysis; Product origination) and improve their satisfaction/retention by eliminating dull routines
Increased agility for transformation	Enable quick wins and rapid value realization to expand margins or generate funding for existing or new initiatives (e.g., Lean, BPR, implementations, process improvement)
Reduced errors (for automated process steps)	Improve auditability (every step could be logged), consistency, and control over error-prone manual activities that elevate risk, non-compliance, financial or reputational harm
Increase in speed of delivery	Reduce end-to-end time to handle peak periods, meet deadlines, and smooth post-M&A integration by virtually connecting disparate systems and data sources
Customer satisfaction/ advocacy	Delighting the customer with differentiated and enhanced servicing and journey experiences, therefore improving retention and satisfaction

Robotics improves data security, reduces impact of labor regulations, and strengthens control and governance

ISACA

IN ADDITION RPA DRIVES ENTERPRISE VALUE

With RPA, the software “bot” performs the activities its human predecessor used to by moving through and across the relevant applications with its own user name and passwords.



EVOLUTION OF RPA & COGNITIVE AUTOMATION

Skill: execution

Assistance

Assisting staff with process execution at their workstations

Replacement

Removing staff from process execution in the database

Skill: cognition

Assistance

Assisting staff with decision making by filtering and providing quality data

Replacement

Removing staff with cognitive learning in the data center

Desktop automation

- Scripting of individual tasks
- Assists human staff with their activities
- Runs on each agent's desktop
- Increases efficiency of workers
- Helps to consolidate information and provide consistent customer experience
- Assists in streamlining work and optimising processes

Robotic process automation

- Large scale unattended processing
- Must respond to fluctuation in system response, unknown events, unanticipated business scenarios without interruption
- Considers security, scheduling, audit, exception management
- Secure, centralized collection of management information, audit records, process logs
- 1:Many support requirement: 2 humans can supervise 200+ robots

Cognitive automation

- Aids or replaces subjective decision making based on large data samples
- Interprets contextual information and provides consistent reasoning
- Assists in the streamlining of processes and routing of enquiries
- Allows human-like reasoning to be applied in larger volumes, e.g., transaction monitoring, fraud identification, call filtering

ISACA

CHANGES TO THE OPERATING MODEL

The operating model will need to shift to support the workforce of the future.

Humans and robots teaming together, creating a powerful virtual workforce

- Easily and quickly scale up and down potentially eliminating the need for contingent labor during peak periods

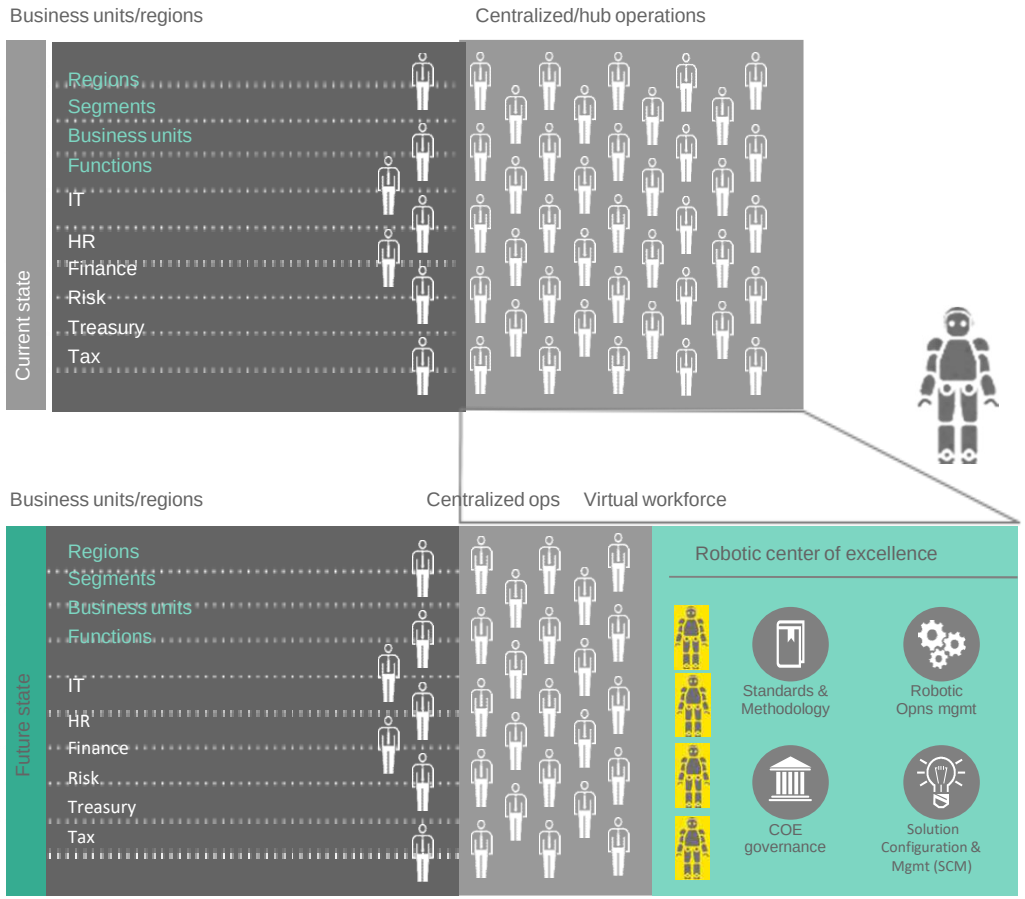
- Consider insourcing tasks previously outsourced
- Reduce cost without moving more jobs offshore
- Top grade onshore workforce to provide:

  - Advanced analytics and insights
  - Process improvements
  - Decision support

Robots do the “what”, freeing up humans to focus on the “why”

THE VIRTUAL WORKFORCE

Moving towards a new operating model enabled by a virtual workforce.



Moving towards “workforce of the future”

- Emergence of “virtual workforce” capable of rapid scale up or down
- Clear separation of tasks between physical and virtual workforce
- Enablement of current teams to take on more or new tasks
- Change in org structure and metrics in line with new operating model
- Robotic COE will add cognitive capabilities to virtual workforce

EXAMPLES OF RPA USED WITHIN BUSINESS FUNCTIONS

TABLE 2

Automation Potential of Various Functions and Sub-Processes

Function	Sub-Process	Automation Potential (Percent)	Savings Potential
Order to Cash	1. Customer Master Data Management	25–30%	40%–60%
	2. Credit Management	25–30%	
	3. Customer Service Support	25–30%	
	4. Account Receivables Management	25–30%	
	5. Incoming Payments	0–5%	
	6. Deductions and Disputes Management	25–30%	
Human Resources	1. HR General Services	25–30%	60%–80%
	2. Expat Management	10–15%	
Source to Pay	1. Source-to-Purchase	25–30%	50%–70%
	2. Purchase-to-Pay	25–30%	
	3. Projects Support	10–15%	
Supply Chain	1. Supply Chain Planning	10–15%	10%–15%
	2. Transport Planning	10–15%	
	3. Supply Planning	10–15%	
	4. Project Management	10–15%	
	5. General Supply Chain Services	10–15%	
General Accounting	1. Fixed Assets/FMM/Closing and Reporting	25–30%	10%–15%
	2. Local Tax Accounting	10–15%	
Controlling	1. Product Costing	5–10%	15%–20%
	2. CO Operation/Reporting	10–15%	
	3. Business Controlling Support	5–10%	
	4. BI and Systems	10–15%	
	5. Group Financial Controlling	5–10%	
Finance Other	1. Intercompany	25–30%	30%–50%
	2. Account and Bank Reconciliations	15–20%	
	3. Financial Planning and Analysis	25–50%	
	4. Tax	40–60%	

Table 2 shows one Big 4 firm's estimates of the amount of processes that can be automated in each sub-process of each function and the potential financial savings associated with the amount of automation.

Where to Automate?

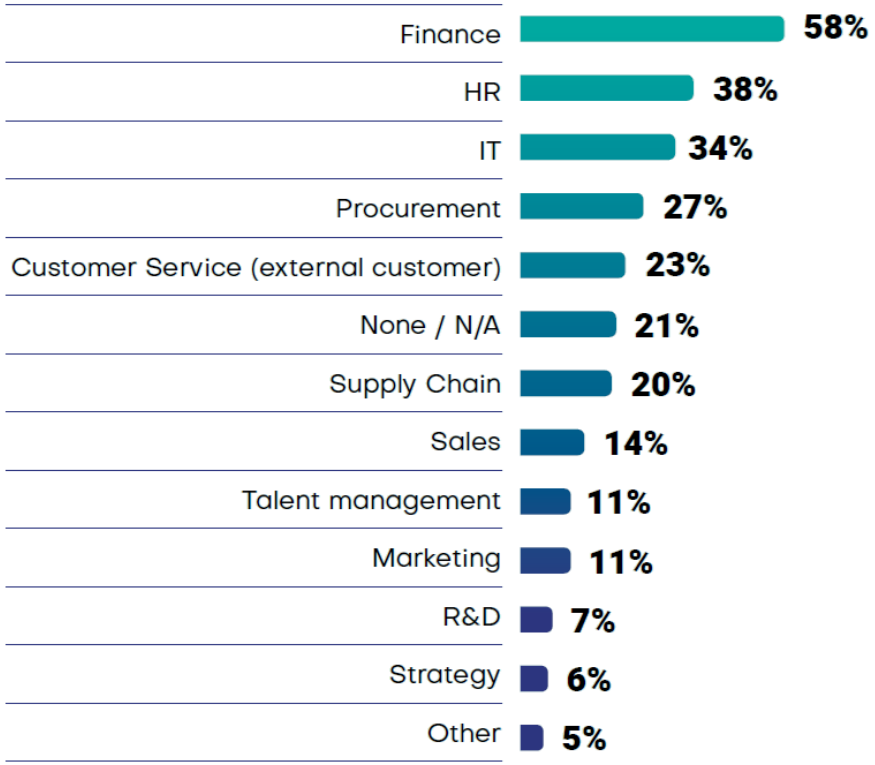
Why is Internal Audit not on the List?

ISACA

IN WHAT FUNCTIONS IS RPA BEING TYPICALLY APPLIED?

Essentially, any high-volume, business-rules-driven, repeatable process qualifies for automation. However, Finance & Accounting is the function with the highest level of RPA adoption, followed by HR and IT.

In which functional areas has IA been implemented?



Common process candidates include:

- **Purchase To Pay**
  - Purchase Order Processing
  - Invoice Coding & Processing
  - 3-Way Match
  - Payment Proposal Presentation
  - Vendor Reconciliations, Statement Preparation & Distribution
  - Vendor Master Maintenance
- **Order To Cash**
  - Customer Quotes Creation
  - Customer Order Processing
  - Cash Application
  - Sales To Cash Reconciliation
  - Collections Support
  - Aging Reporting Preparation
  - Customer Master Maintenance
- **Record To Report**
  - Journal Entry Processing
  - Intercompany
  - Accounting Close
  - Fixed Assets
  - Sales & Use Tax Calculation
  - Inventory Management
- **Decision Support/FP&A**
  - Other Operational Reporting
  - Variance Data Compilation
- **Hire To Retire**
  - Employee Hires & Onboarding Administration
  - Employee Terminations & Systems Provisioning
  - HR Employee Self-Service
  - Payroll

Each industry will also have sector-specific processes that can be automated. For example, in healthcare, the use cases tend to be around claims processing, insurance verification, compliance, etc. In banking, use cases include loan application review and processing and many others that are very specific to their industry.

ISACA

PUT ROBOTICS TO WORK INSIDE BUSINESS PROCESSES

Process characteristics to consider for RPA

- High volume repetitive transactions
- High levels of manual data capture and entry
- Interaction with multiple applications or systems
- Multiple tasks to perform a process
- Definable business rules and exceptions

- Data entry, validation and manipulation
- Data transfer between applications
- Automated formatting
- Copy and paste operations
- Login and logout of applications and emailing

Activities typically performed by RPA

The application scope is broad – penetrating for example finance and accounting, human resources, IT and Supply Chain

F&A

- Sales order
- Order to cash
- Collection
- Procure to pay
- Incentive claim
- Record to report
- Vendor setup
- Trend tracking

60%
Reduction in cost to process invoice

Supply chain

- Master data mgmt.
- Work order mgmt.
- Demand and supply planning
- Quote, invoice and contract management
- Returns processing
- Freight management

9–20%
of the cost to companies arise from supply chian problems

HR

- Payroll
- Benefits administration
- Pay slip management
- Time and attendance management
- Recruiting process
- Education and training
- Compliance reporting

80%
Reduction in payroll processing cost

IT

- Installation
- File transfer protocol download, upload and backup
- Server application and monitoring
- Synchronizing, deleting and emptying folders
- File and email mgmt.

30%
of the time spent by IT is almost on low level taks

ISACA

AUTOMATION “HOT SPOTS” FOR FINANCE

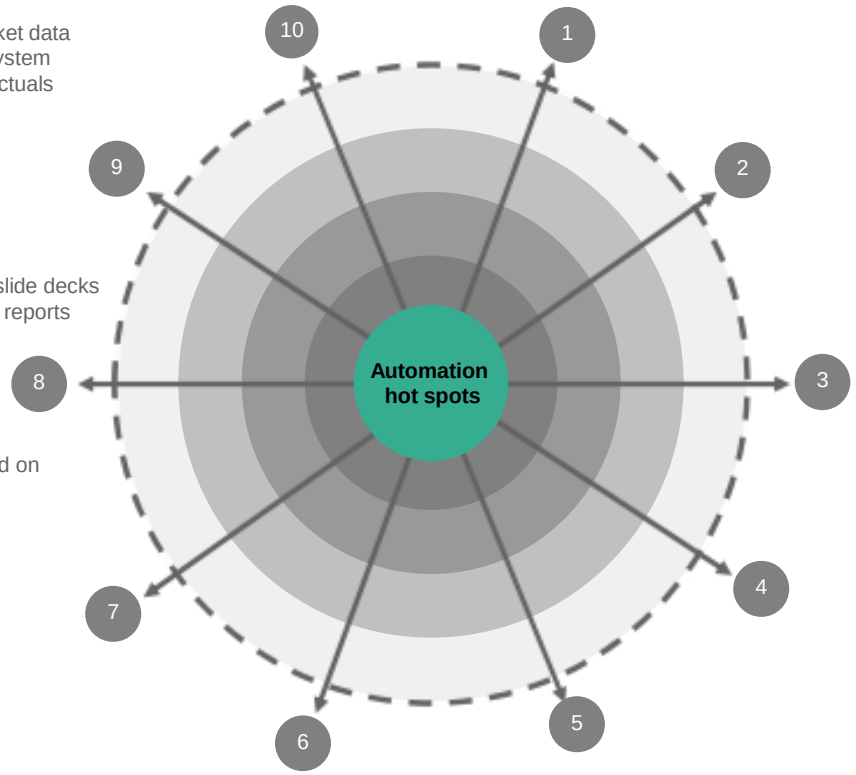
Financial planning & analysis (FP&A)
- Pre-population of forecasts using historical and market data
- Loading pre-populated balances into the planning system
- Creating variance reports to pre-population and to actuals

Regulatory and management reporting
- Data capture and cleansing to support automated generation of regulatory reports
- Pre-populating complex annual reporting
- Automating the preparation of management review slide decks by collecting data from multiple finance systems and reports

Accounting change
- Automating the collection of data for leases or revenue transactions
- Categorizing, summarizing and analysing data based on history and pre-established parameters
- Producing reports for internal analysis

Expense reimbursement
- Automating policy compliance reviews
- Calculation of purchase discounts
- Compliance and management reporting
- P Card or expense program maintenance

Intercompany reconciliation
- Automated checking and reconciliation of intercompany balances
- Basic research and reporting for exceptions
- Creating exception file and email report for finance review and approval



Accounts receivable processing
- Credit approvals and customer master file maintenance
- Order processing
- A/R – cash receipts processing and sending late notices via email

Accounts payable processing
- Vendor set up and maintenance
- Automating the workflow processes and approvals
- Data entry and payments preparation
- Automating processing of payments and bulk payment files for journal entries to sub system

Operational finance and accounting
- Automating pricing reviews based on customer contracts and pre-approved price lists
- Calculation and processing of rebates
- Downloading of detailed monthly sales data and calculation of commissions
- Creating files and emails to gain approvals
- Posting to detailed sub systems and General Ledger

Standard journal entries
- Creation of standard monthly journal entries using pre-populated templates provided by different business users
- Performing validation analytics
- Posting to ERP

Account and bank reconciliations
- Automating the download of subaccount balances and bank statements
- Uploading detailed transaction data from various sub systems
- Reconciling balances and transactions to core finance sub systems
- Creating balancing journal entries to handle discrepancies

Finance functions face regular peaks in demand that could be supported through the use of robotic assistants. Automation of a range of core finance activities has the potential to improve quality and allow great focus on analysis.

ISACA

AUTOMATION “HOT SPOTS” FOR IT

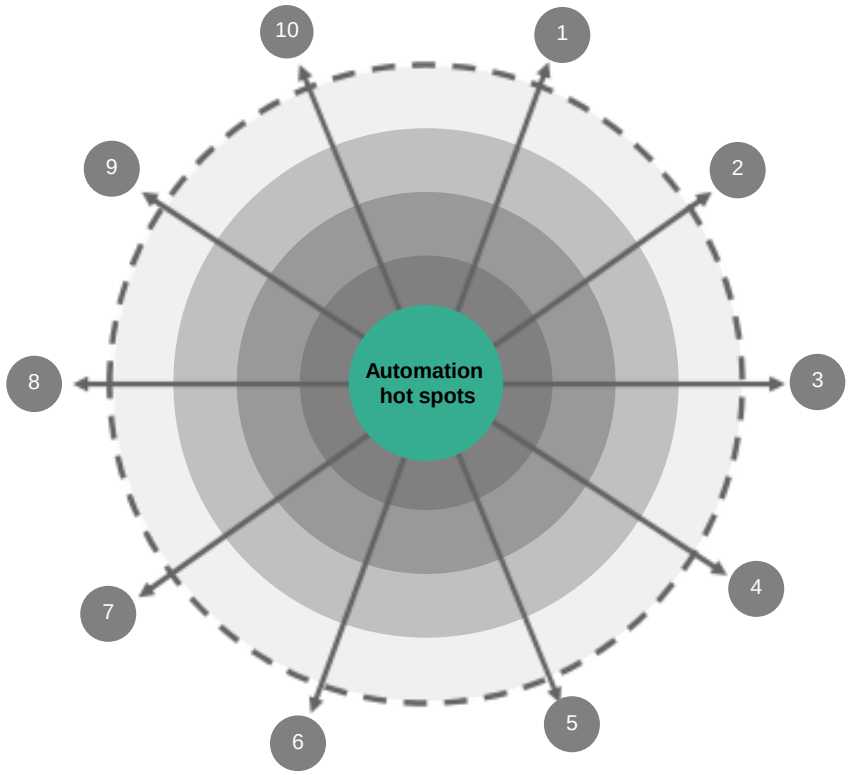
IT Policy and Training
- Automation of policy distribution
- Tracking of IT training completion and scores

Automated Reporting
- Creation of standard management reports
- Distribution of selected reports to various user groups
- Variance calculations and reporting vs. plan data,
- including basic explanation information

Help Desk Management
- Request processing and logging
- Automated responses to frequently asked questions
- Automated execution of pre-approved tasks

Event Management
- Event monitoring
- Event reporting
- First level incident resolution

Security Monitoring
- Technical threat and vulnerability management
- Incident registration and reporting
- First level incident resolution



Software Installation
- Automating the software request and approval process
- Downloading licensed software
- Installing approved software on designated servers and user machines

Application Testing
- Initial application performance testing
- Collection of user feedback ratings
- Reporting

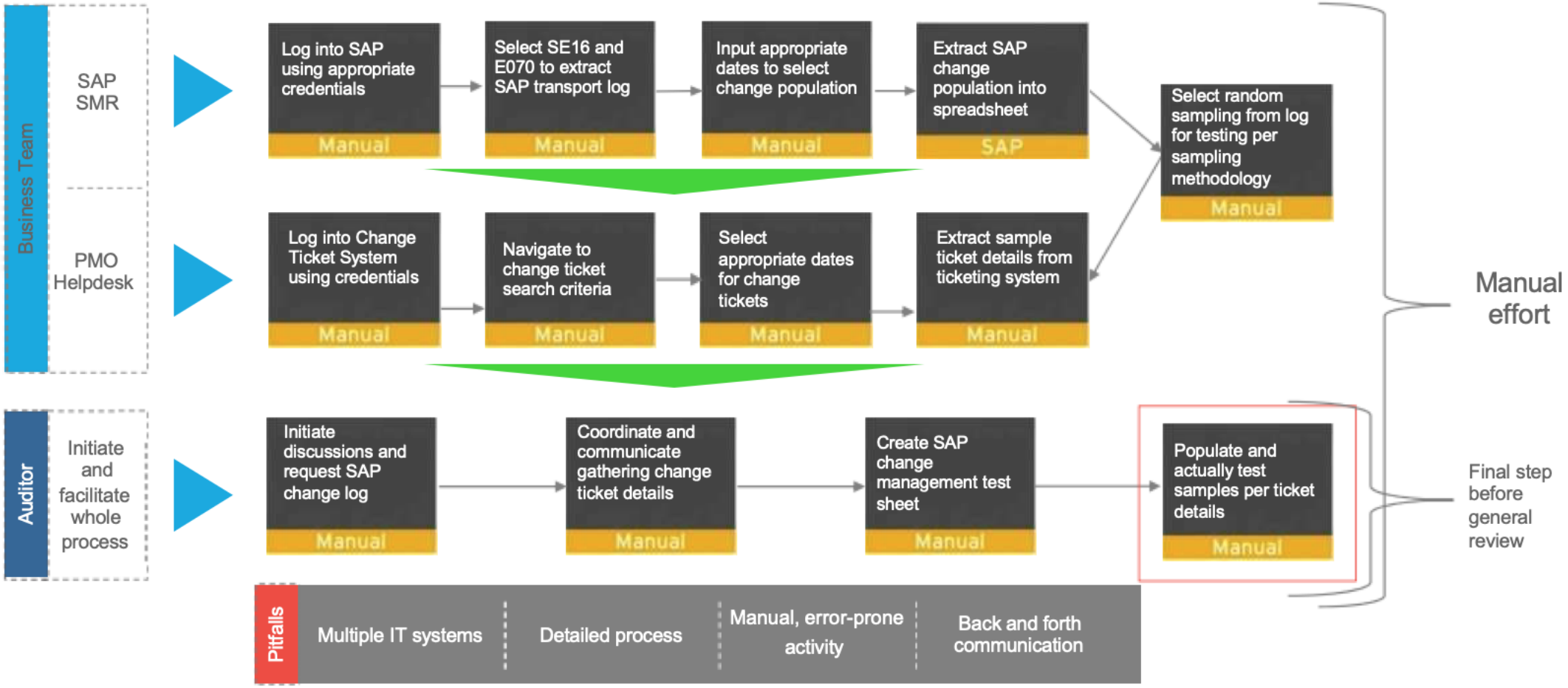
Ongoing Server Application Monitoring
- Daily monitoring of server performance
- Automating email notifications of server issues outside of pre-established parameters
- Reporting of server performance

File Management
- Batch processing
- Synchronizing, deleting, and emptying folders

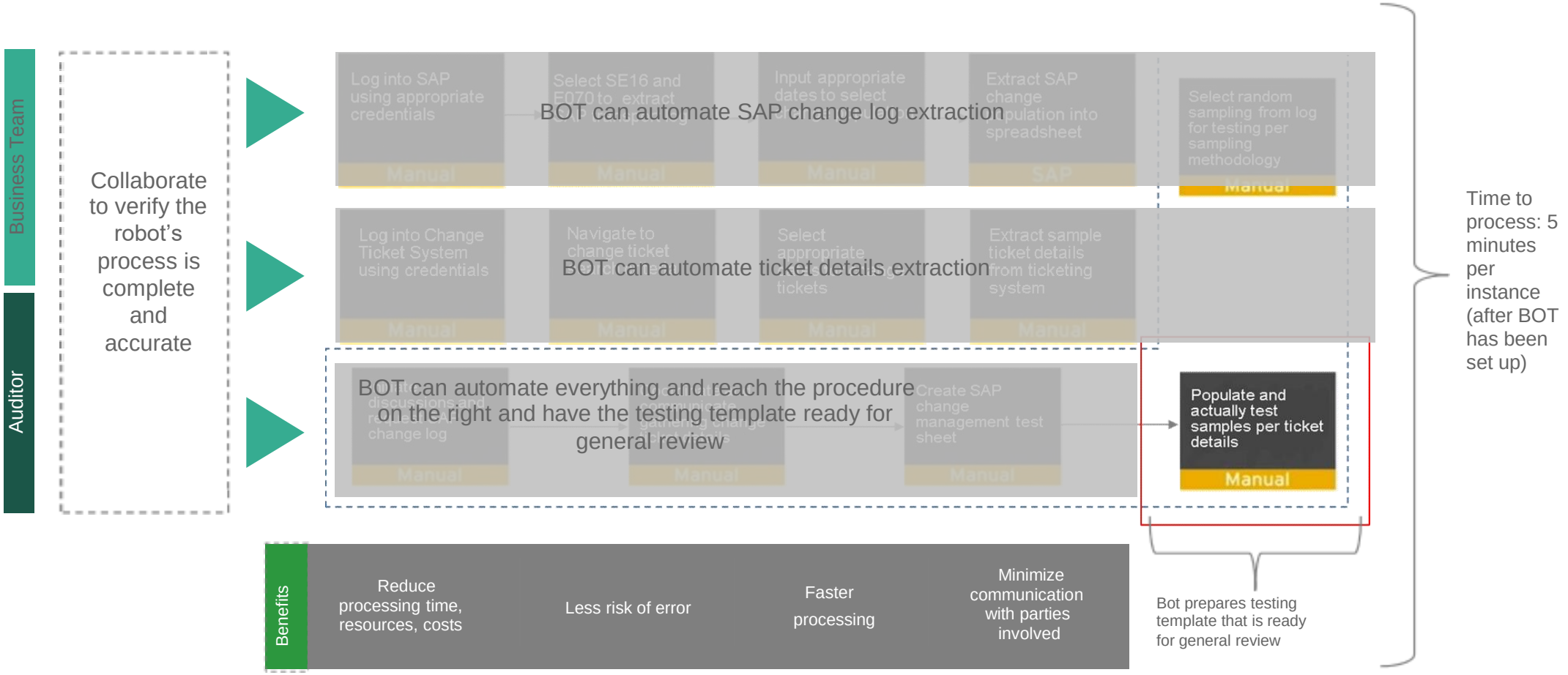
Identity and Access Management
- Automating user profiles and setup, including network, operating Systems, applications, databases, remote access
- Processing new and emergency user requests
- Managing password reset process
- Termination processing

ISACA

USE CASE: CHANGE MGMT. CONTROL TESTING (BEFORE)



USE CASE: CHANGE MGMT. CONTROL TESTING (AFTER)



ISACA

AUTOMATION “HOT SPOTS”: BUSINESS TAX COMPLIANCE

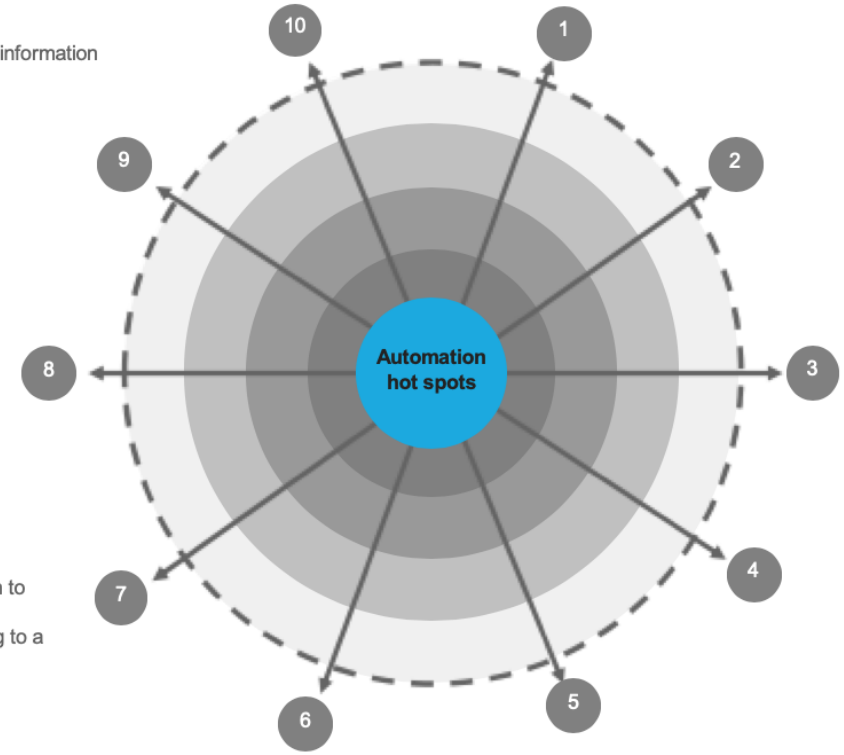
Saving workpapers and tax returns
- Utilizing a standard naming convention to save required information
- Maintaining historic tax data for audit purposes

eFiling
- Clearing diagnostics for eFiling
- XML to return reconciliation
- Printing or emailing eFiling acceptance notification or rejections or emailing that to a person

Mailing and printing
- Certified mail – completing the 3 separate forms needed and save the receipts in the right place
- Creating the labels for mailing
- Printing the returns and filing and saving the returns in the right place

Disclosures and attachments
- Election statements are included and validating a Return to ensure proper attachments and elections are included
- Validating the right attachments are included by referring to a matrix

Reconciliations
- Provision to return reconciliation and identifying unreconciled items and sending alerts
- Automated checking and reconciliation of various tax balances to triage exception items for review
- Reconciliation of balance and transactions in the finance systems



Extracting information from systems
- Extract book trial balance and key balances such as accruals, fixed assets, M&E or other tax sensitive accounts

Formatting and work paper creation
- Formatting, cutting, pasting to get it ready to be entered into the tax computation system
- Manipulating trial balances before importing into tax tool
- Rollover balances and input into tool

Data validations and roll forwards
- Automating the process of validating information by referring to a checklist of items to ensure that the checklist is completed
- Self assuring data such as validating the book income on the M-3 equals the book income in the equity roll-forward
- Fixed asset or quarterly payable roll forwards

Inputting data into tax systems and forms
- Automating tax form data entry by “pushing” of tax specific data from a work paper into the tax application for federal, state, international, extensions and estimates
- Moving trial balance data from GL into tax reporting systems
- Tasks that require clicking through the system
- Automating the workflow processes associated with tax returns processing

Generating reports
- Automating the download of specific reports at specified times and emailing them to key stakeholders

Tax functions face regular peaks in demand that could be supported through the use of robotic assistants
Automation of a range of core tax activities has the potential to improve quality, allow great focus on analysis and tax planning

ISACA

AUTOMATION “HOT SPOTS” FOR RISK AND CONTROLS

Quality control

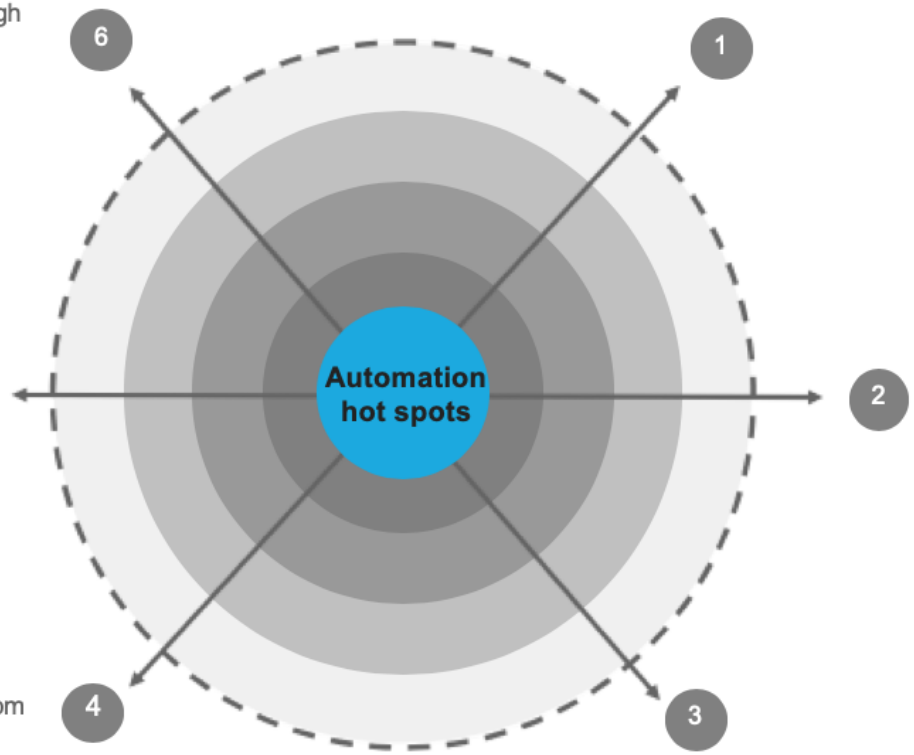
- Systematic controls to ensure quality through the testing process (cognitive)
- Identify exceptions in testing process (cognitive)

Report development

- Generate consolidate reports using predefined logic for various aggregated reporting required
- Generate reports based on trends and issues identified in Test Execution (cognitive)

GRC/tool reporting data collection

- Consolidate data for report development from disparate compliance, security or issue management platforms
- Distribute reports to owners, or publish on accessible location



Data collection and transformation

- Collect data from multiple disparate systems. Data may need to be extracted from mainframe screens, PDFs, images, or websites, preventing automation using common tools such as SQL
- Use alternate tools in addition to robotics for data extraction and interpretation
- Consolidate supporting information and documentation
- Transform data from complex structured information to standard templates required for testing

Control testing execution

- Conduct preliminary analysis, and initial test scripts execution for rules based, logical tests
- Integrate and execute scripts based on defined inputs and rules
- Tests requiring human judgments to interpret information could be pre-analyzed for an analysts to review based on set criteria and self-learning algorithms using structured information (cognitive)

Issue identification and upload

- Identify failures and report issues in issue management Platforms
- Consolidate issues and conduct bulk uploads of test issues

ISACA

IDENTIFYING RPA RISK OPPORTUNITIES

Audit execution and control automation

Audit process enhancement opportunities

- As expectations for audit and compliance functions increase, the ability to manage workload, increase efficiency and effectiveness, while meeting a changing regulatory landscape will be a differentiator
- Firms may look to technology to address new audit testing needs and increase efficiency. A number of technical approaches such as RPA can help achieve targeted automation of the audit process.

Where automation can make a difference

- Reduce cycle time for heavily manual data collection and preparation for testing
- Reduce cost associated with non-decision making manual process
- Increase traceability test steps performed
- Increase consistency of test supporting documentation and execution
- Ability to execute a variety of tests by using/modifying previously built test steps

Sponsor focus

- Internal Audit
- Compliance
- Privacy
- Attest services sponsors

Control efficiency/effectiveness opportunities

- Automation of highly time consuming, complex or repetitive manual control execution due to information gathering, desperate systems, or spreadsheet manipulation
- Frequent failures of manual controls where highly predictable outcome of controls to support key compliance requirements (SOX, Privacy, other regulatory requirements)

Where automation can make a difference

- Increase predictability of effectiveness related to control execution
- Increase in traceability through logging of RPA functions and outcome (completeness and accuracy of execution)
- Reduce effort related to heavily manual data collection and review for control execution
- Timeliness of control execution

Sponsor focus

- CFO/Controller
- Compliance
- Privacy
- CIO

RPA VENDORS

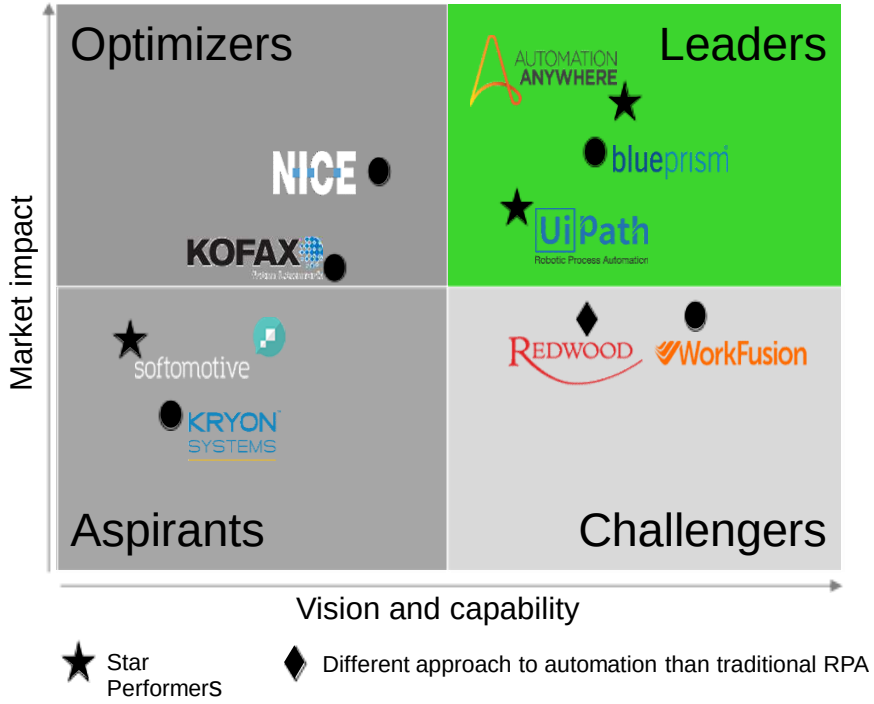
RPA SOFTWARE TOOLS ARE A DIVERSE & CONTINUOUSLY EVOLVING MARKET

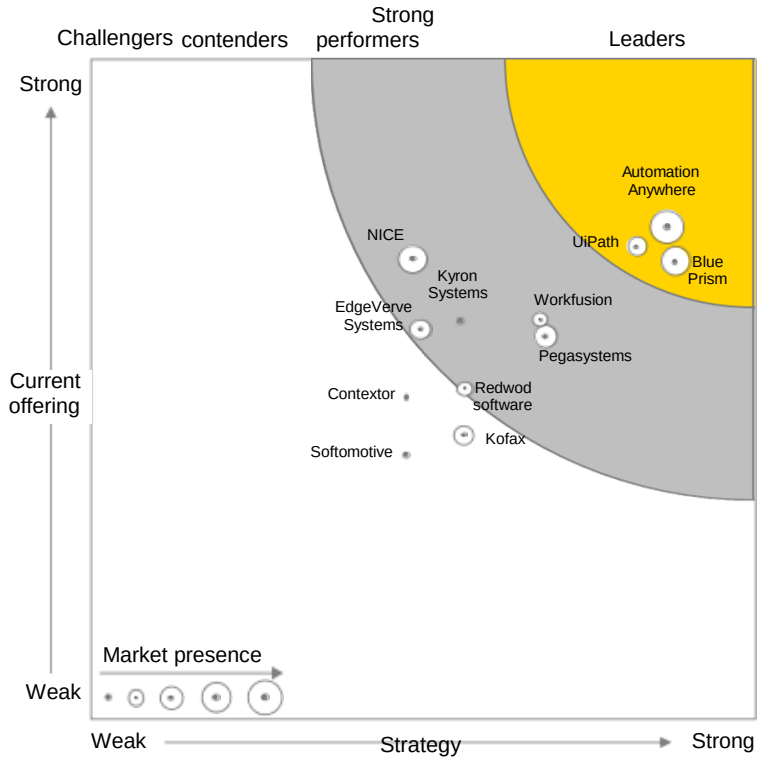
Key points of view on the current state of the RPA market:

- The landscape is rapidly developing, but three firms are currently top of class
- An innovative, high growth technology: we expect to see the marketplace continue to change as it reaches maturity in the coming years
- The software bots will grow increasingly smarter and more capable as artificial intelligence and machine learning become more mainstream
- Tools fall into two main categories:
  - Attended automation, where bots prompt humans to take actions in a workflow, such as next best action in a call center
  - Unattended automation, where bots operate independently in 'lights out' style

AUTOMATION VENDORS

Leading automation solution providers according to Everest Group and Forester





KEY DIMENSIONS IN SELECTING THE APPROPRIATE RPA SOFTWARE

Robotic Process Automation vendors can be distinguished across six key dimensions that determine suitability across the use cases.

Drive cost reduction

- Reduce “Grey IT” overhead e.g. spreadsheet management, macro workarounds
- Facilitate “Flat Growth”, maintaining workforce size whilst increasing productivity
- Reduce or avoid outsourcing

Enable business change

- Tackle IT development backlogs rapidly at low cost
- Reduce risk and adapt to client needs
- Support digital transformation and migration from legacy

Business friendly technology	Native OCR functionality	Out of the box integration	Unattended automation	Enterprise workforce management
				Â
► No coding development ► User friendly design ► Strong support community ► Comprehensive help library ► Short training timescale	► Can read non digital text ► Has the ability to learn/be trained ► Standard font recognition	► Web integration ► Desktop/thick client integration ► Mainframe integration ► Citrix/remote connection integration	► Automates rules based processes ► End-to-end, scheduled automation ► Multithreaded processing	► Robust enterprise architecture ► Schedule and control robot workforce ► Native work queues ► Exception reporting

INTERNAL AUDIT CONSIDERATIONS

INTERNAL AUDIT'S ROLE IN INTELLIGENT AUTOMATION

Consulting services - provide advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training. The "client" for consulting services can be any key stakeholder, such as the business owner, process owner, control owner, etc.

Assurance services - provide an objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.

If your organization is just beginning its intelligent automation program, internal audit may begin with an "in-flight" or "pre-assurance" assessment to provide valuable insights while the program or a particular use case is still being established.

INTERNAL AUDIT'S ROLE IN INTELLIGENT AUTOMATION

Key opportunities for internal audit within intelligent automation initiatives include the following:

First line of defense – Business owners

Internal audit can help to integrate **governance, risk, and controls** considerations throughout the automation program life cycle as an organization establishes and implements its program.

Second line of defense – Standard setters

Internal audit can help the organization identify opportunities to embed automation-enabled control activities within the impacted business processes and functions.

Third line of defense – Assurance Providers

Finally, the internal audit organization can capitalize on intelligent automation innovations to **increase the efficiency and effectiveness of its own activities**.

WHAT CAN WE LEARN FROM OTHERS?

Continuous monitoring

Consider the analogy of predictive policing, bring similar rigor and analytical insight to incident monitoring and resource deployment within Internal Audit.

Meaningful patterns in data

Align incidents and other internal and external data to standard risk dimensions that enable teams to understand and take action on linkages between risks, incidents, and audits.

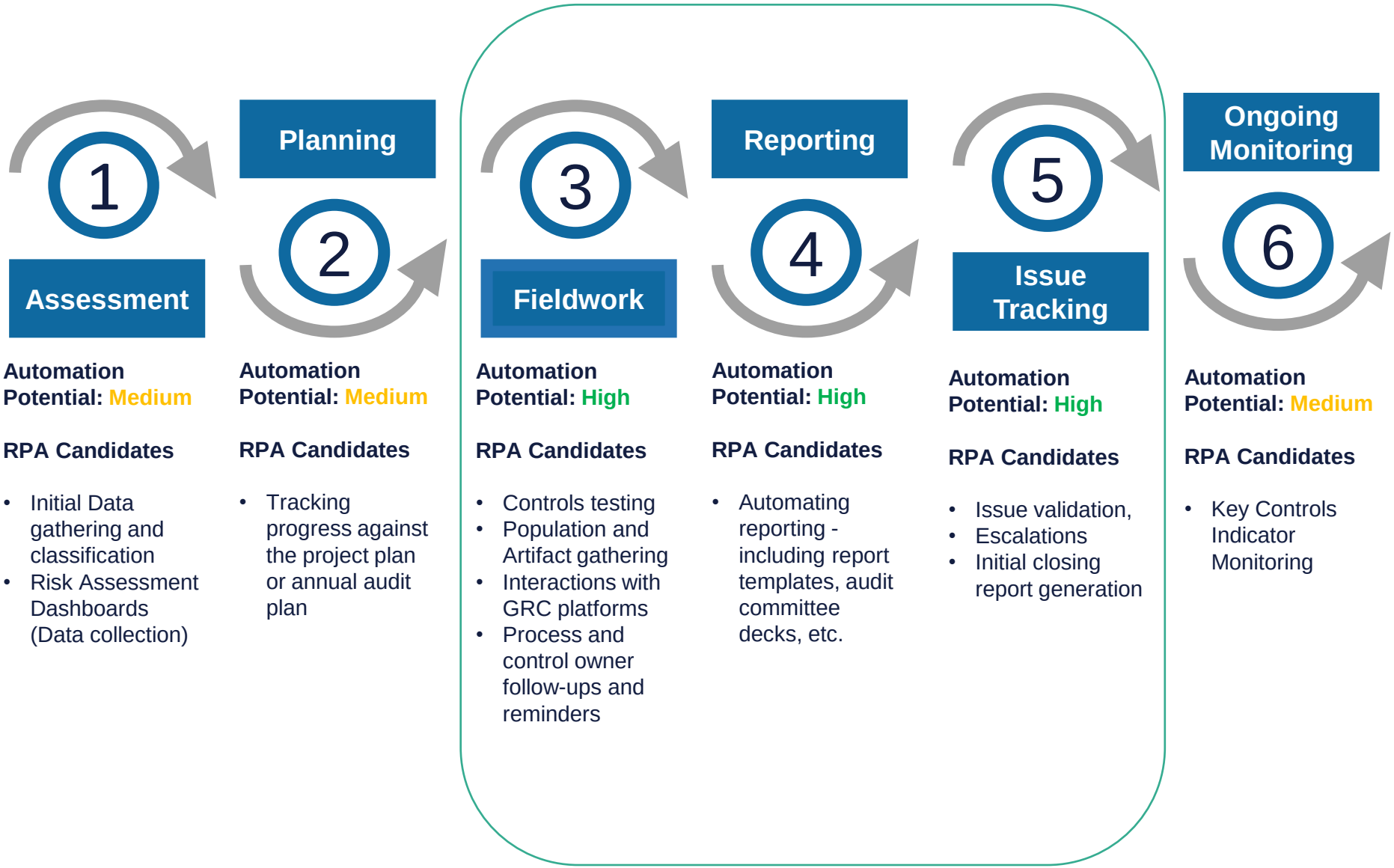
Modeling incidents and audits

Analyze available historical data to generate insights that advance continuous monitoring strategies, bring valuable insights about the patterns of risk and effectiveness of incident remediation.

Integrated solution

Combine data management and artificial intelligence capabilities, enabling teams to explore risk patterns and inform audit strategy, coverage, and resource deployment.

AUOMATION OPPORTUNITY MAP ACROSS AUDIT LIFECYCLE



Automation Potential: Medium

RPA Candidates

- Initial Data gathering and classification
- Risk Assessment Dashboards (Data collection)

Automation Potential: Medium

RPA Candidates

- Tracking progress against the project plan or annual audit plan

Automation Potential: High

RPA Candidates

- Controls testing
- Population and Artifact gathering
- Interactions with GRC platforms
- Process and control owner follow-ups and reminders

Automation Potential: High

RPA Candidates

- Automating reporting - including report templates, audit committee decks, etc.

Automation Potential: High

RPA Candidates

- Issue validation,
- Escalations
- Initial closing report generation

Automation Potential: Medium

RPA Candidates

- Key Controls Indicator Monitoring

ISACA

WHICH IA BENEFITS BEST ALIGN TO YOUR IA STRATEGY?

Reduced Cost
Automation replaces high-touch, repetitive, manual audit activities

Increased Quality
Automations, once configured and controlled, execute consistently and without error

Enable Continuous Auditing
Automation creates the potential for frequent, even continuous, monitoring

Increased Efficiency
Automation allows more to be done across a broader range of audit activities with the same number of

Increased Assurance
Automation permits evaluation of larger numbers of transactions, even up to one-hundred percent sample size

Improved Insights
Automation allows for efficient analysis of large data sets, with conditional analysis, to create betters insights

RETHINKING SOD WITH BOTS

EMERGING NEED FOR RPA ASSURANCE

As with any new technology adoption Boards and Management are now focusing on risks and related controls to mitigate risks associated with RPA.

Internal Audit typically serves as the steward for understanding RPA adoption implications and has been tasked with reporting to Management and the Board whether there are sufficient controls designed and operating effectively over RPA programs to address the identified risks.

In most RPA programs, the risks and controls are spread among various departments including IT and business functions resulting in the need for an integrated audit approach needing IA resources that are familiar with both IT and business processes.

SOX/JSOX/CSOX are often the catalysts to initially test RPA programs so financial functions are typically the leading adopters for RPA.

SIGNIFICANT RISKS ASSOCIATED WITH RPA

Significant risks relating to RPA include:

SDLC – Lack of system development life cycle controls can result in the deployment of bots that have not been properly designed, configured, secured, activated and monitored in the production environment resulting in various issues for management including data integrity, segregation of duties conflicts and processing errors.

Operational – Poor oversight and insufficient requirements gathering when designing and deploying robots can lead to inefficiencies due to poor pre-RPA process understanding. Resulting challenges include increased costs and often times the need to re-implement the bot.

Regulatory – Standalone bots may not meet compliance requirements since such requirements often involve high levels of documentation that may not be contemplated during the initial RPA design phase.

Organizational – Replacing employees or down sizing departments due to automation could have a negative impact on employees. Affected groups may not be fully aligned on robot requirements as automation requires an increase of communication.

SIGNIFICANT RISKS ASSOCIATED WITH RPA (CONTINUED)

Technology – The IT infrastructure may not always be powerful enough to handle the higher volume of transactions which could lead to a negative impact on other business functions. Additionally, IT and the Business are not aligned on robot requirements during an outage (Business Continuity Planning).

Financial – Process being automated by a robot may not be implemented to meet business requirements and can result in financial loss. Configurations or algorithms could result on mistakes during the processing of transactions they may not be identified timely.

Cyber Security – Implementation may have not considered security configurations of the robot environment. Since the bot will typically be within the Corporate domain, it may open new vulnerabilities to the network. Lack of monitoring the environment could lead to unauthorized access or use of robot service accounts.

Identity Access Management – Generic IDs or robot credentials are not stored in a restricted area. Segregation of duties is not considered which could lead to a robot having unauthorized permissions.

RPA RISKS CONSIDERATIONS

Using a risk based approach is recommended when evaluating RPA programs.

Fully understanding upstream and downstream direct and indirect risks can greatly enhance the “value add” of the RPA audit.

A pervasive risk throughout most RPA programs is the speed at which errors/control breakdowns can multiply and should be contemplated in all RPA audits (i.e. where is the is the “safety valve control” downstream or upstream from the bots).

IA APPROACH TO ROBOTIC PROCESS AUTOMATION (RPA)

IA's framework approach should be designed to identify risks and expected controls over the following domains:

Governance – Developing policy and procedures relating to RPA. Providing a consistent approach to ensure clear guidelines for implementing RPA, establishing overall responsibility, and manage the RPA life-cycle.

Selection – Determining which processes are suitable to automate and developing procedures for performing risk and benefits-based analysis'.

Design – Utilizing both IT and Business Owners to engage in business requirements. IT to determine leading practices in securing the robot environment and standards for protecting sensitive data.

Development and Testing – Engaging IT teams to determine feasibility of the current infrastructure. Engaging business owners to validate throughputs of automated processes.

Live Monitoring – Using tools to monitor, log, and notify on set thresholds to ensure availability, performance, and changes within the robot environment.

IA APPROACH TO ROBOTIC PROCESS AUTOMATION (RPA)

Process Continuity – Planning to ensure that robot remains available throughout the lifecycle. Determining process owners for potential manual processing during outage.

Change Management – Appointing key personal required to evaluate risk and approve changes within the robot environments. Establishing Change Procedures for making any source code or configuration changes.

DATA PRIVACY LANDSCAPE

LEARNING OBJECTIVES

Data Privacy Landscape and Audit

At the end of this module attendees should be able to:

- Understand some of the major items impacting the data privacy landscape today
- Understand and explain what GDPR and CCPA is and their impacts to companies and consumers
- Describe the considerations and approaches to implementing a privacy program within your organization
- Understand and describe Internal Audit’s role in an organization's privacy program

DATA PRIVACY IN THE NEWS

The New York Times

On Data Privacy, India Charts Its Own Path

A new law would give the country's 1.3 billion people more power over data collected by companies but allow the government to exempt itself from the rules.

StarTribune

New data-privacy law proposed for Minnesota insurers

Proposal follows revelations about computer systems at Blue Cross Blue Shield.

MARKETSMEDIA

Wall Street Frets Over Data Privacy

FierceHealthcare

Lawmakers taking steps to create federal data privacy law with tougher regulation of biometric, health data

GLOBAL government FORUM

Trudeau outlines Canadian data privacy reforms

yahoo! finance

California's new data privacy law will change the internet

Vox

2020 Democrats on who controls your data — and who's at fault when it's mishandled

Candidates agree: Americans should have more control over their data than they do now.

Bloomberg

Regulating Technology: Striking the Balance Between Data Privacy, Innovation and Freedom of Speech

FINANCIAL TIMES

Protecting data privacy needs constant evolution

It is already time to think about regulation in a post-GDPR world

BARRON'S

The First Real Effort to Regulate Tech Is About to Begin. It Could Get Messy.

abc 7 EYEWITNESS NEWS

New Laws 2020: Illinois laws that take effect January 1

USA TODAY

California Consumer Privacy Act of 2020: What the new privacy law means to you

NEWS

Trump signs law to reduce robocalls, though they won't end

Bloomberg Law

Thailand's First Privacy Law Carries EU-Like Rules

ISACA

DATA PRIVACY LANDSCAPE

Lei Geral de Proteção de Dados (LGPD) – Brazil

- New Data Processor Officer role, which is a mix of a Data Protection Officer and regulatory authority Data Processor Role will communicate Data Subject right requests and complaints to supervisory authority
- Data Subject Requests must be responded to within 15 days

China Data Protection Regulation (CDPR)

- Critical Information Infrastructure Operators (CIIOs) must store Personal Information collected or generated within the territory of the PRC
- A security assessment for transferring Personal Information collected and produced in China

Israel Data Protection

- Explicit technical safeguards that need to be in place (e.g., audit logging, periodic PEN testing)
- Requirement of appointing a Data Security Officer

Russian Data Protection Act

- Personal Data of Russian citizens collected must be stored in servers, IT systems, databases or data centers located in Russia
- Data subjects have the right to object to direct marketing

DATA PRIVACY LANDSCAPE

Washington Privacy Act (Senate Bill 5376)

- Expressly requires companies to perform risk assessments to evaluate the potential privacy or security impact of processing Personal Data, and perform assessments whenever the processing changes in a way that "materially impacts the risk to individuals" and at least annually.
- Specifically addresses the use of facial recognition technologies. It requires Controllers that use facial recognition for profiling purposes to employ meaningful human review prior to making final decisions and obtain consumer consent prior to deploying facial recognition service.

GDPR & CCPA OVERVIEW

GDPR & CCPA OVERVIEW

GDPR and CCPA:

The General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) guarantee strong protections to consumers. The GDPR is the most comprehensive data protection laws in the world, and the CCPA is the most significant legislative privacy development in the United States.

There are key differences in the following elements of these law:

- Who is protected
- Definitions of “personal data”
- Who needs to comply
- Individual rights granted to consumers
- Penalties imposed on violating organizations

GDPR & CCPA OVERVIEW: KEY FACTS

Key Facts	GDPR	CCPA
Effective Date:	May 25, 2018	January 1, 2020 with organization to provide Consumer with information from the preceding 12-month period.
Who is Protected:	Any Data Subject that is an EU resident. A Data Subject is any person whose Personal Data is being collected, held or processed. The regulation protects the rights and interests of individuals.	Uses the term “Consumer” rather than “Data Subject”. Consumer / natural person who is a California resident.
Personal Data:	Any information that identifies a natural person directly or indirectly, in particular by reference to an identifier, which can broadly include IP Address as online identifiers.	Contains a broader definition of “Personal Data” and also covers information pertaining to households and devices and any information that relates to a particular consumer or household

GDPR & CCPA OVERVIEW: KEY FACTS

Key Facts	GDPR	CCPA
Who needs to comply:	Data controllers and processors who process data of an EU resident, including organizations outside the EU.	Companies that process the data of at least 50,000 California residents annually or have more than $25 million in annual revenue.
Individual Rights	• Right to information • Right to access • Right to rectification • Right to withdraw • Right to be forgotten • Right to object • Right for data portability	• Right to know what data a business collects on you. • Right to say no to the sale of your information. • Right to delete your data. • Right to be informed of what categories of data will be collected about you prior to its collection, and to be informed of any changes to this collection. • Right to know the categories of third parties with whom your data is shared. • Right to know the categories of sources of information from whom your data was acquired. • Right to know the business or commercial purpose of collecting your information.

GDPR & CCPA OVERVIEW: KEY FACTS

Key Facts	GDPR	CCPA
Opt In / Opt	• Consent must be freely given; • Consent should be obvious and require a positive action to opt in. • Consent must specifically cover the controller's name, the purposes of the processing and the types of processing activity. • Explicit consent must be expressly confirmed in words, rather than by any other positive action.	The CCPA requires that a business allows a consumer to "opt out" of the sale of personal information. Further, a business must provide conspicuous notice of a consumer's right to withdraw consent of the sale of personal information at any time.

GDPR & CCPA OVERVIEW: WHAT'S THE BIG DEAL?

Penalties

GDPR	CCPA
The GDPR is enforced by EU Member State Data Protection Authority "DPA", and the penalties can range up to €20 million (approx. $22.1 million) or 2%-4% of global annual revenue.	Enforced by the Attorney General. The penalties are up to $2,500 per violation for unintentional violations and up to $7,500 per violation for intentional violations if the business fails to cure the alleged violation within 30 days.

POP QUIZ 1: GDPR & CCPA

How many GDPR related fines or notices were issued in 2019?

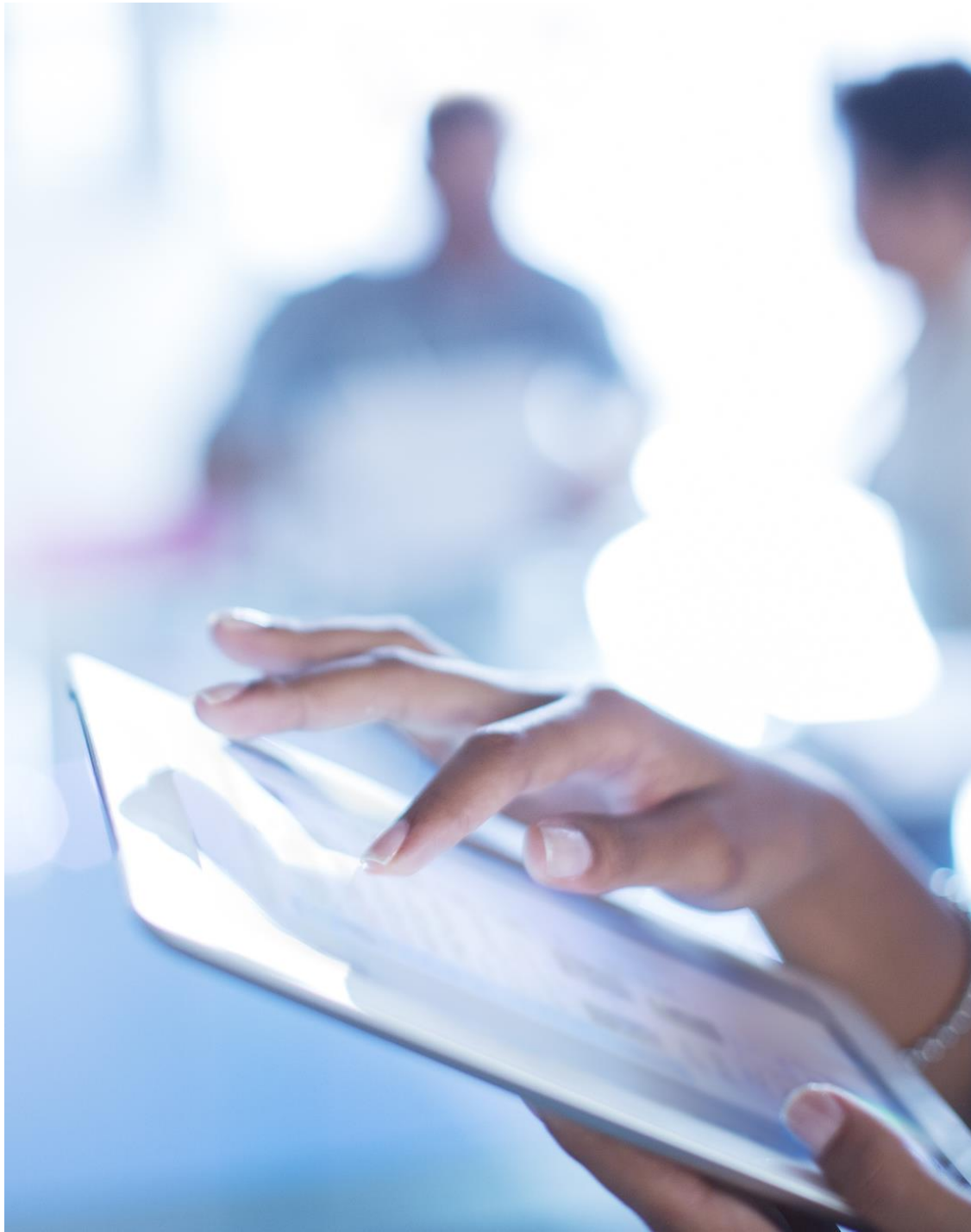
A. 34

B. 52

C. 21

D. 16

E. 89



POP QUIZ 2: GDPR & CCPA

Which of the following reasons were companies were included in the fines or notices in 2019?

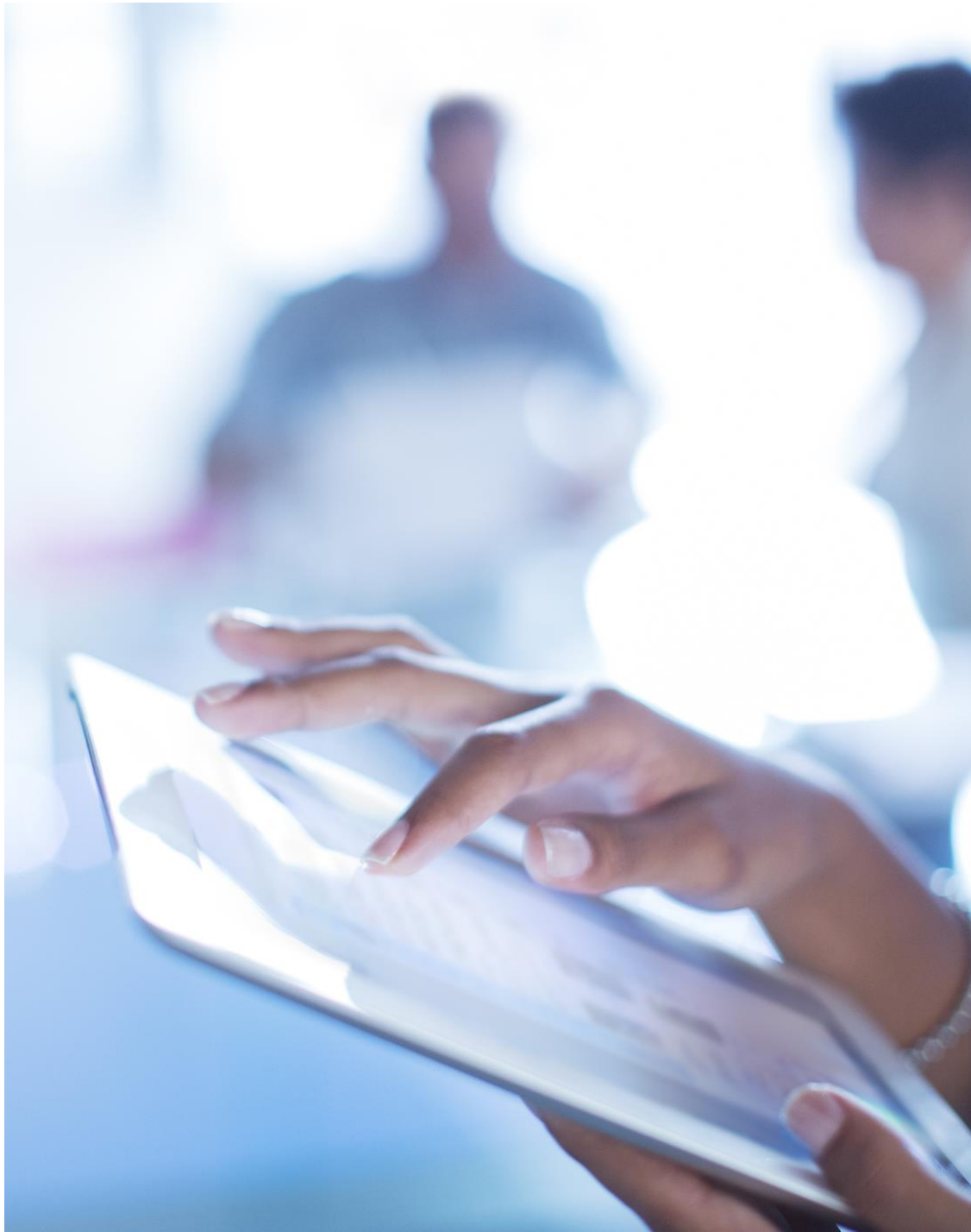
A. Insufficient transparency, control, and consent over the processing of personal data for the purposes of behavioral advertising

B. Poorly disclosing purpose for requesting GPS and microphone permissions within the football league's mobile app

C. Sending direct marketing messages to its customers, without consent

D. Unlawful processing of employee data

E. All the above



IMPLEMENTING A PRIVACY PROGRAM

HOW DO WE START MANAGING A DATA PRIVACY PROGRAM?

- The implications of the GDPR/CCPA reach well beyond the core, ongoing compliance functions.
- Alignment with the GDPR/CCPA has downstream implications on various business operations.

Privacy/ Compliance	Data subject / Consumer requests, DPIAs, data sharing, etc.	**Human Resources**	Training, employment agreements, etc.	**Product Engineering**	GDPR/CCPA product functionality
Cyber Security	Security assessments, monitoring of cyber security program, etc.	**Marketing**	Consent management, cookies, etc.	**Information Technology**	Protection-by-design, encryption, minimization, etc.
Legal	Regulatory guidance, third-party relationships, etc.	**Customer Support**	Data subject / Consumer requests, customer inquiries, etc.	**Procurement**	Third party relationships

COMPLIANCE ASSESSMENTS VS. AUDITS

Assessments

- Preliminary assessment focusing on what an organization must do to become compliant.
- Analyzes the type of Personal Data that is being collected.
- Establishes the legal basis for collecting data.
- Identifies the records of processing activities under the GDPR/CCPA.
- Determines the necessary policies and procedures.

Audits

- Comprehensive examination of the design of the policies and procedures.
- Ensuring operational practices are in alignment with the policies and procedures.
- Sampling/testing of processes to review effectiveness, etc.

COMPLIANCE ASSESSMENTS

Why is a Compliance Assessment important?

- This is the first step on identifying on how the company uses Personal Information.
- Understanding Personal Information lifecycle.
- Identifying what is the current state of the Corporation.

What are the benefits?

- Identify systems/assets/third parties that processes (e.g., collect, use, transfer, store and delete) Personal Information.
- Identifying accountability on the Data Privacy Program.

Who should perform a Privacy Assessment?

- IT Compliance/Data Privacy Officer.
- Outside Experts.
- Internal Audit.

IMPORTANCE OF DATA PRIVACY AUDIT

Why Conduct a Privacy Audit?

- Allows your organization to measure their alignment to relevant articles/sections by evaluating the policies, procedures, and practices that have been put in place.

What Are the Benefits?

- Pinpoints high-risk areas.
- Improves efficiency in operations.
- Ensures that policies and procedures reflect the current state practices.
- Establishes monitoring procedures.

Champions of remediation projects should be auditing their own processes as well.

Who Should Perform a Privacy Audit?

- Internal Audit.
- IT Compliance/Data Privacy Officer.
- Outside Experts.

When to perform the Audit?

- Depends on what is ready to be audited
- An opportunity to not use a *pass/fail* approach, but to provide enhancements/recommendations to assist with the operationalization.

ISACA

DATA PRIVACY AUDIT PROGRAM

What to do when there is a small Privacy Program:

- **Client:** Fortune 500 Retail Organization has some businesses in Europe and US. There are only two people in the Privacy Team.
- **Scenario:** They performed minimal Records of Processing and Asset Inventory Listing based on their own knowledge. They have updated Privacy Notice on their website based their own knowledge too.
- **Gathering:** Determine what documentation is currently available and who are the key departments.
- **Discovery:** Interview key departments on their use of personal data.
- **Lessons Learned:** This may surprise you how much is documented vs. what is actually taking place.

Case Study #1

ISACA

DATA PRIVACY AUDIT: KEY AREAS OF FOCUS

1. Implement **Encryption and Data Masking & Data Minimalization** Policies, Procedures, and Mechanisms
2. Implement **Data Subject / Consumer Rights** Policies, Procedures, and Capabilities
3. Enhance **Privacy Notices (Internal/External)** Policies, Procedures, and Capabilities
4. Implement **System-Specific Assessment** Program
5. Implement a **Data Protection Impact Assessment (DPIA)** Methodology
6. Establish **Protection by Design and Default** Mechanisms
7. Appoint and Implement **Data Privacy** Function
8. Establish **Privacy & Security Training**
9. Enhance **Breach Notification** Process
10. Enhance and **Maintain Records of All Processing Activities**
11. Enhance **Conditions for Consent** Policies and Procedures
12. Implement **Data Minimization Procedures**
13. Implement **Data Minimization Procedures**
14. Enhance **Data Retention** Policies and Procedures
15. Enhance **Third Party Risk Management Procedures**

ISACA

GROUPING OF ARTICLES/SECTIONS

The logical grouping of the GDPR or CCPA Articles/Sections allows for an efficient and structured baseline for which a measurement of alignment can be performed.

Topic	GDPR Article(s) / CCPA Section(s)	GDPR Article(s) No.	CCPA Section(s) No.
Collection and Consent	• Conditions for Consent • Personal Data Collected from the Data Subject/Consumer • Personal Data not Obtained from the Data Subject/Consumer	Article 7 Article 8 Article 13 Article 14	Section 1798.105 Section 1798.120 Section 1798.125
Breach Notification	• Notification of a Personal Data Breach to the Supervisory Authority • Communication Requirements for a Personal Data Breach	Article 33 Article 34	Section 1798.145 Section 1798.150

CONTROL OBJECTIVES

The Privacy audit program defines **control objectives** to meet the GDPR/CCPA articles/sections.

Topic	GDPR Article(s) / CCPA Section(s)	GDPR Article(s) No.	CCPA Section(s) No.	Total Control Objectives	Control Objectives Topics
Collection and Consent	• Conditions for Consent • Personal Data Collected from the Data Subject/Consumer • Personal Data not Obtained from the Data Subject/Consumer	Article 7 Article 8 Article 13 Article 14	Section 1798.105 Section 1798.120 Section 1798.125	3	1. Data Collection and Consent Management Policies and Procedures. 2. External Privacy Policy/Notice 3. Internal Privacy Policy

- The Privacy audit focuses on evaluating the **design** and **operating effectiveness** of the policies, procedures, and practices in place at the organization to meet these control objectives.
- **Test procedures** are defined for each control objective and should include a combination of inquiry, observation, inspection and reperformance.

OBSERVATION TYPES

For each GDPR/CCPA control objective requirement, one of the following determinations can be made:

- **No Finding:** Indicates that the organization fully meets the control objective of the GDPR/CCPA articles/sections.
- **Finding:** Indicates that the organization does not fully meet the control objective of the GDPR/CCPA articles/sections.
- **Enhancement:** Indicates that the organization meets the control objective of the GDPR/CCPA articles/sections, but there is opportunity to improve the safeguards and/or processes to better align with the GDPR/CCPA articles/sections.

A great opportunity to provide value!

EXAMPLE OF OBSERVATION TYPES

What's the difference between a Finding and an Enhancement:

- **Finding:** These are activities that are specifically stated in the regulation such as:
  - GDPR – Consent mechanism for Opt-In.
  - CCPA – Opt out for selling of Personal Information.
- **Enhancement:** These are activities that can help or improve a current process, but is not a requirement, such as:
  - GDPR/CCPA – Although both regulation state that there must be a mechanism for Data Subject/Consumer Request ("DSR" or CR", respectively), to facilitate DSR/CR a playbook (e.g., workflow, procedures, scripts, etc.) can be utilized to ensure consistency and training for all employees involved in the DSR/CR activities (e.g., system owners, business process owners, third parties, Legal, IT, etc.).

AUDIT APPROACH

Full Audit

Objective: To determine if policies and procedures relating to all applicable GDPR/CCPA Articles/Sections have been designed and operating effectively with limited samples.

In Practice: If formal policies and procedures have not been developed but related activities are being performed, the adequacy of these activities should be reviewed.

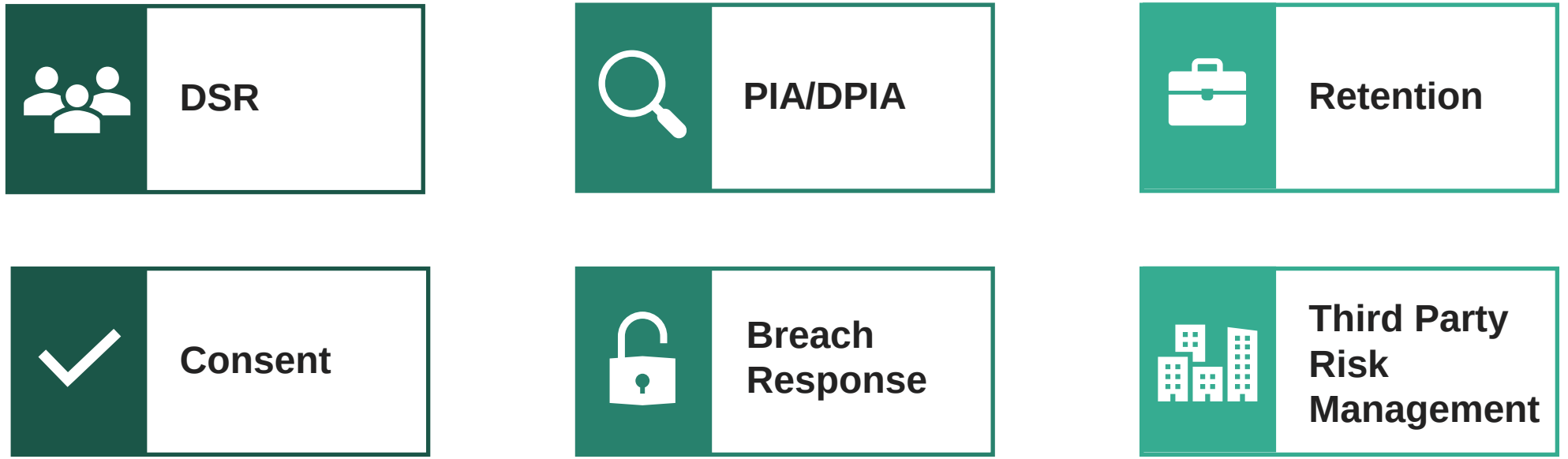
Micro Audit

Objective: To determine if implemented GDPR/CCPA activities are operating effectively with expanded samples.

In Practice: Micro audits are broken up by related Topic/Articles/Sections (and those which closely relate) to allow for comprehensive audits per the need of the organization.

POTENTIAL AREAS OF MICRO (FOCUSED) AUDITS

Micro Audits: Tests a sample of events for specific processes, beyond policies and procedures, to validate that controls are being followed in practice.



DATA PRIVACY AUDIT PROGRAM

Why would we want to do a micro audit vs. full audit:

- **Client:** Fortune 500 Corporation in the Food Industry with presence internationally.
- **Scenario:** They already have processes in place that are audited so why do they need to be audited again.
- **Discovery:** Interview key departments on their use of personal data and review a sample.
- **Lessons Learned:** What you may learn is that even when there are processes that may already be in place, either privacy considerations are not in place and/or there may be areas that have not been considered in existing processes.

Case Study #2

ISACA

LOOKING AHEAD

Task	Plan	Implement	Maintain	Demonstrate
Data Privacy Audit / Micro Audit	Develop test plans for either a full audit or micro audit, and define control objectives to meet the GDPR/CCPA articles/sections. Should consider: • Policies and Procedures • Data Subject / Consumers Rights • Consent • System of Record • PIAs/DPIAs • Retention	• Measure alignment to relevant GDPR/CCPA articles/sections by evaluating the policies, procedures, and practices that have been put in place • Provide enhancements/ recommendations to assist with the operationalization	• Determine frequency of Data Privacy Audits or GDPR/CCPA Micro Audits • Periodic review of test plans developed to ensure completeness and accuracy of test steps and controls	• Publish report showing test results from Data Privacy Audits or Micro Audit conducted

INTERNAL AUDIT'S ROLE

INTERNAL AUDIT'S ROLE

1. Oversight of programs that ensure accurate information mappings of Personal Data throughout the organization.
2. Advising on the identification of GDPR/CCPA in-scope systems.
3. Performing recurring, security and privacy specific gap assessments to benchmark program attributes against new data privacy requirements.
4. Increasing the frequency and/or scope of organizational privacy risk assessments.
5. Conducting audits focused on key privacy risks associated with processes for which Personal Data is collected, as well as transferred out of the organization (e.g., outbound).
6. Evaluation of security for privacy controls (e.g., logical access, authentication mechanisms, remote access, audit logging) for processes involving Personal Data.

REPORTING TO EXECUTIVES & THE BOARD

Why is Data Privacy and Cyber Security becoming an executive and board level concern:

- Consumers are becoming increasingly concerned about the security of their Personal Information.
- In 2019, there were increasing numbers of organizational breaches.
  - $8.19 Million - Average cost of a single data breach in the US.
  - $7.5 billion – Total Cost of All Ransomware attack in the US.
- Data breaches are expensive internally, but externally, company reputation (and revenue dollars) are at risk.
- Americans are concerned about businesses collecting and selling their personal information without permission.
- Americans say they are taking measures to protect their online privacy more today than they were a year ago.

PROVIDING VALUE ADDED SOLUTIONS

Where does Internal Audit come in:

- Internal Audit can be a partner with the Privacy Team/Data Privacy Officer.
- Helping Privacy Team's/Data Privacy Officer leveraging existing frameworks and programs to reduce extra cost of discovery and knowledge sharing.
- Leveraging the Audit Program to communicate and drive action of gaps in Privacy Program.
- Expand Internal Audit team's knowledge on key risk areas in regulation.
- Reducing cost associated with breaches due to proactive actioning of gaps.

DATA PRIVACY AUDIT PROGRAM

How does Corporation gain value of audit program if they don’t directly process personal data:

- **Client:** Fortune 1000 Corporation in the Technology Industry with presence internationally.
- **Scenario:** The technology company is a service provider why would they need to implement a privacy program.
- **Discovery:** Interview the Privacy, Information Technology and Marketing Teams to determine how they are using their client’s data. Confirm what Third Parties are being used as processors.
- **Lessons Learned:** Clients are more concerned now on how service providers are securing their customer’s data.

Case Study #3

ISACA

DATA PRIVACY AUDIT PROGRAM

Does a Corporation/Government Entity in Healthcare sector need to have Privacy Program:

- **Client:** Corporation/Government Entity in the Healthcare Sector.
- **Scenario:** Corporation/Government Entities already perform HIPAA/Hi-Trust Assessments does not see a need to perform a Privacy Compliance Framework
- **Discovery:** Interview Physicians, Practitioners, Clinic Operations, Patient Care, Research and Marketing.
- **Lessons Learned:** HIPAA/HI-Trust framework can be leveraged for a Privacy Audits as audits generally are more in-depth validation of safeguards in place. Electronic Health Records (EHRs) replacing outdated paper records has been a massive game changer for everyone in the medical world. However, often times Covered Entities and Business Associates are not prepared or understand the risks involved in technology.

Case Study #4

ISACA

CLOSING

IN SUMMARY

Gain a good understanding of the readiness activities performed prior to beginning the Privacy Audit.

If they are not ready, don't test it… yet!

Aim to add value with recommendation. It's not a pass/fail approach. Internal Audit's role should be working with various Business Operations to bridge the gap.

Increase your knowledge of the GDPR/CCPA:

- International Association of Privacy Professionals (IAPP)
- Obtain a certification (i.e., CIPP/E and/or CIPP/US)
- Reference online regulatory resources (e.g. www.ico.org.uk and https://www.caprivacy.org/)

QUESTIONS?

This training content (“content”) is provided to you without warranty, “as is” and “with all faults”. ISACA makes no representations or warranties express or implied, including those of merchantability, fitness for a particular purpose or performance, and non-infringement, all of which are hereby expressly disclaimed.

You assume the entire risk for the use of the content and acknowledge that: ISACA has designed the content primarily as an educational resource for IT professionals and therefore the content should not be deemed either to set forth all appropriate procedures, tests, or controls or to suggest that other procedures, tests, or controls that are not included may not be appropriate; ISACA does not claim that use of the content will assure a successful outcome and you are responsible for applying professional judgement to the specific circumstances presented to determining the appropriate procedures, tests, or controls.

ISACA

THANK YOU FOR ATTENDING THIS ISACA WEBINAR