Intelligent automation controls and internal audit considerations

April 2018

Building a better working world

What is intelligent automation?

***What** you do is defined by your integrated business events…*

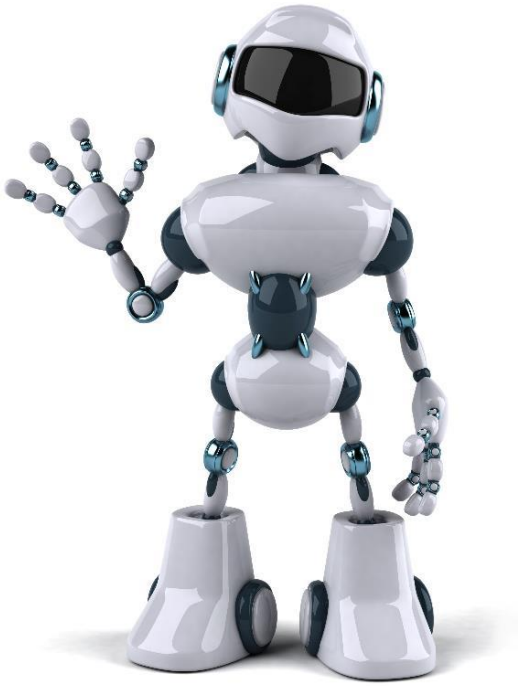
You:

- Buy, make, ship, store and sell products
- Manage customers and vendors
- Recruit and retain employees
- Manage internal and external financial reporting
- Procure goods and services
- Manage internal and external risks

- *And many more…*

***How** you do it is enabled by your systems and tools…*

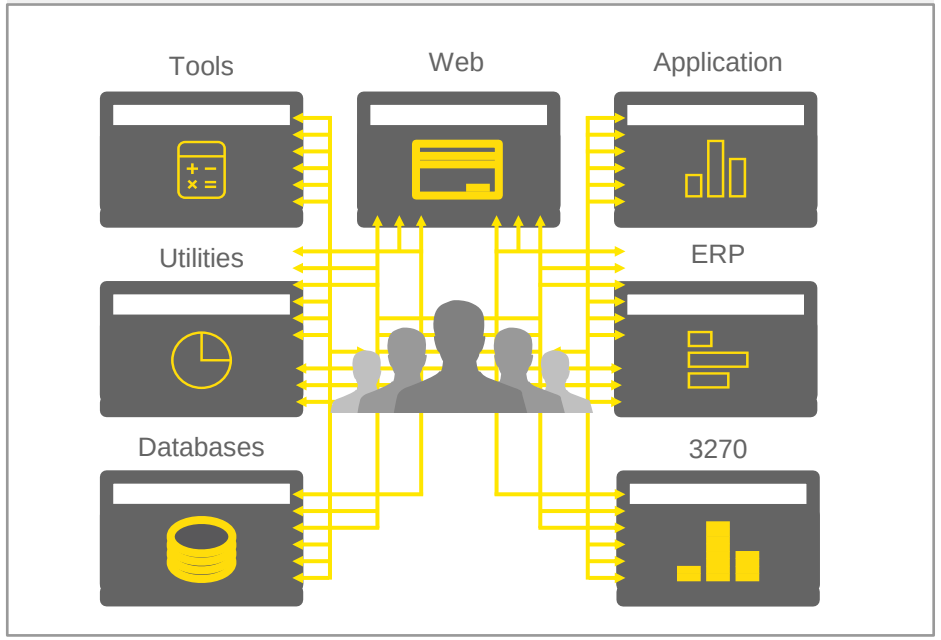
***Who** does it is where intelligent automation fits in*



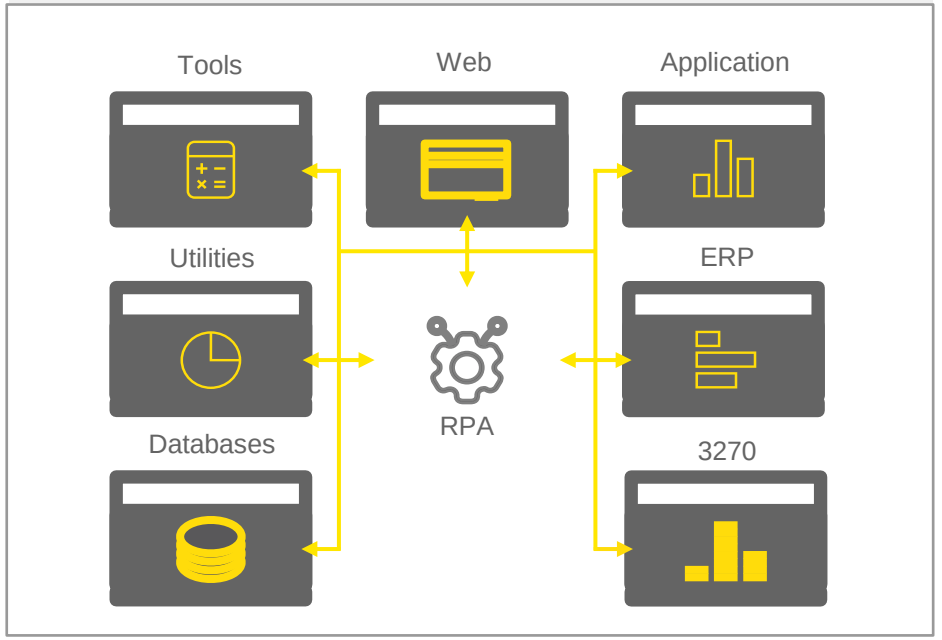
RPA will change WHAT people do and HOW they will add value, fundamentally impacting operating models

Robotic process automation

Today, organizations often need people to execute processes and handle data manually across disparate systems and tools, which adds risk and takes time and money.



With RPA, organizations can streamline and automate the execution of repetitive business processes, which improves quality, security and execution time.



Unbundled manual workflows

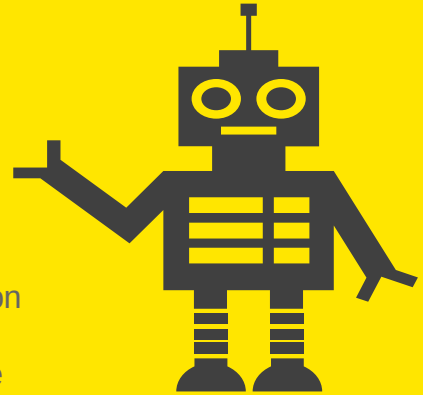
Bundled automated workflows

Benefits of intelligent automation

Low risk

Non-invasive technology

Overlaid on existing systems and integrated with existing data, minimizing disruption to existing IT strategy and architecture. Automation technology can begin with simple rules-based tasks and scale to more sophisticated algorithms and machine-learning functions as the organization matures.



Accuracy
The right result, decision or calculation the first time

Consistency
Identical processes and tasks, eliminating output variations

Cost savings

Ranging from 20%-60%[1]
of baseline FTE cost

Right shoring
Geographical independence reduces need to offshore jobs while still delivering cost savings

Productivity
Freed-up human resources for higher-value-added tasks.

Cross-system
Across systems since it works through the user interface layer

Reliability
No sick days; services are provided 365 days a year

Audit trail
Fully maintained logs essential for compliance

Retention
Shifts toward more stimulating tasks

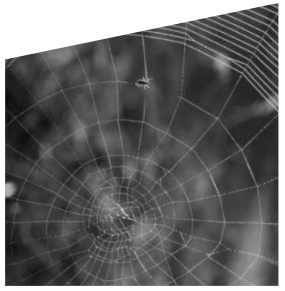
Scalability
Instant ramp up and down to match demand peaks and troughs

ROI
Typical RPA projects include multiple functional "pilots," but the program is completed in 9 to 12 months with an ROI in <1 year

[1] Based on proprietary data

Trigger points for intelligent automation

High data entry volumes

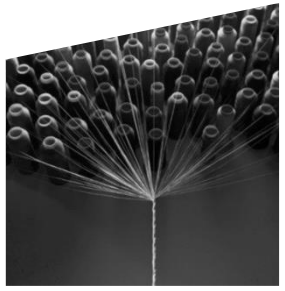


Compliance and control requirements

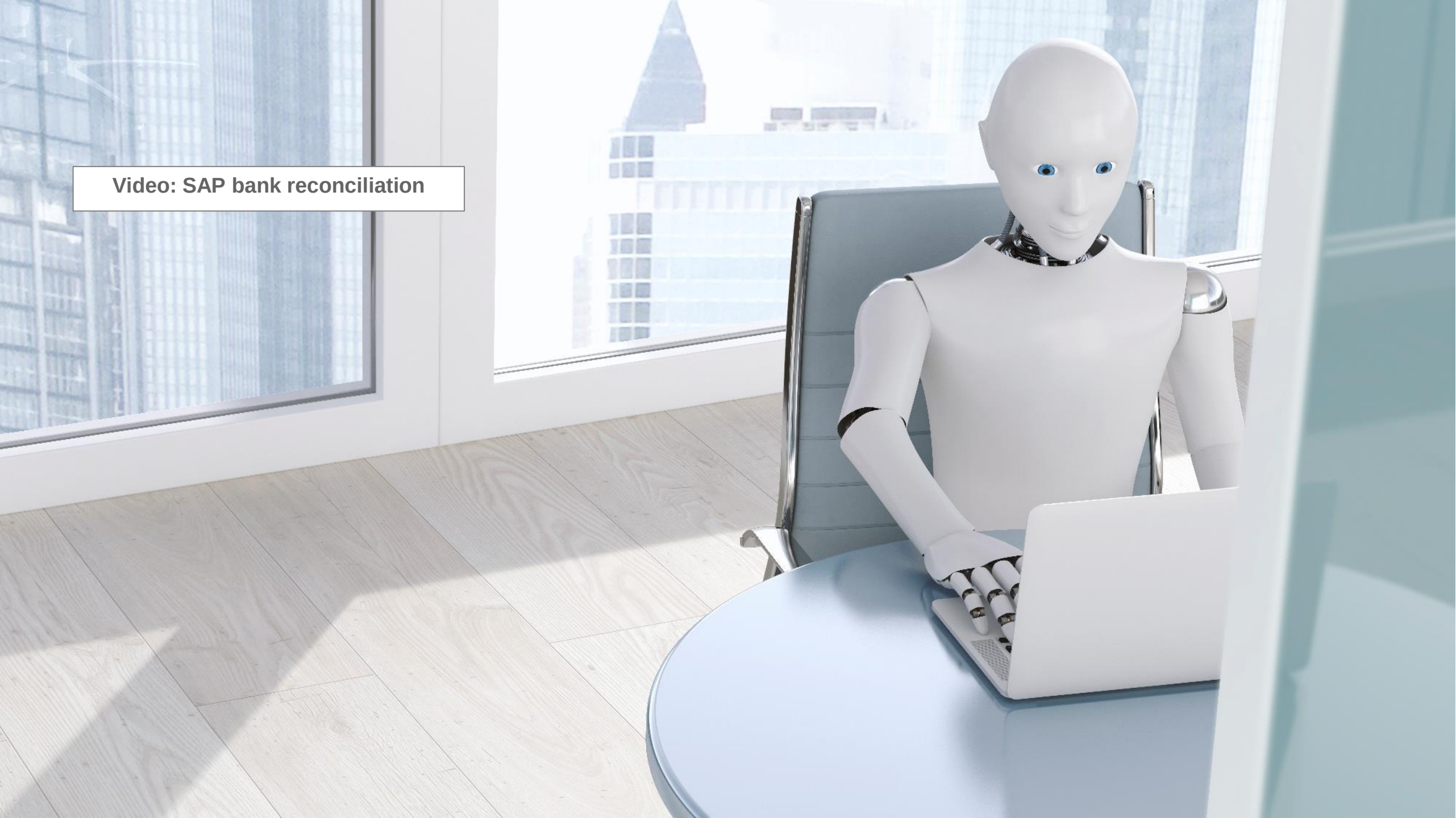
Significant rework

Numerous manual processes

Multiple disparate legacy systems



High turnover due to repetitive/low-value-added activities


Video: SAP bank reconciliation

Lessons learned

1. Not considered a business-led initiative
2. Not having a strategic business case, and postponing planning until after a proof of concept
3. Not understanding what happens after processes have been automated
4. Targeting intelligent automation at the wrong processes
5. Applying traditional methodologies
6. Automating too much of a process, or not optimizing for intelligent automation
7. Forgetting about IT infrastructure, security, risk and controls
8. Expecting one tool/technology to provide all of the automation capabilities

Key risk and controls considerations for intelligent automation

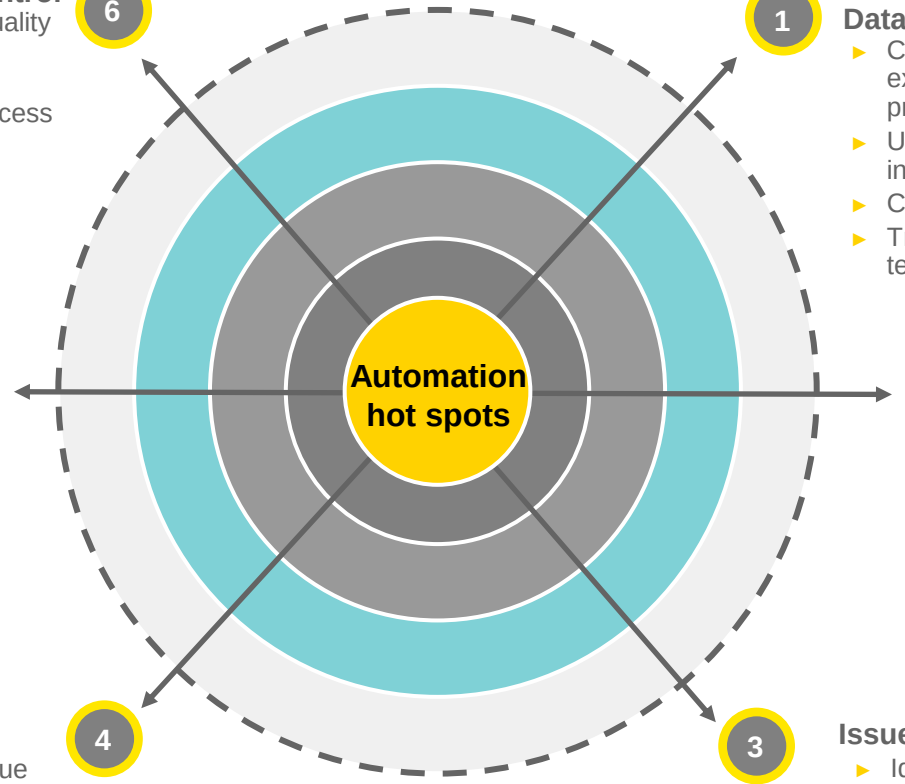
Intelligent automation risks and related control activities

Risk domain	Risk description	Illustrative controls
Policy and governance	A lack of robotics governance can lead to ineffective and inefficient process automation and an inability to support and meet business requirements.	• Policies and procedures – change management, access control, segregation of duties, operations, issue management, RPA Center of Excellence (COE) • Ongoing monitoring – performance, control processing and quality assurance • Governance, risk and control – risk and control requirements defined in RPA strategy and deployment, i.e., approval of new robots, approval of robot ID, development controls for change management process and access, user acceptance testing, migrate to production approvals
Logical user access (GCC)	Robotics access management is ineffectively managed, leading to the compromise of systems, applications and their associated data.	• Security – privileged access to provision, de-provision and modify robot IDs is limited to COE; documentation is maintained • Humans interacting in the same process do not have access to create robots or change robot processing (SOD) • Robot permissions and profiles are restricted; audit logs are maintained of each robot user ID
System change management (GCC)	Robotics implementations are not appropriately designed and tested, leading to requirements not being met or a negative impact on production systems resulting in a negative impact on the business and financial losses.	• RPA development and change management – key life cycle controls, authorization, testing, approval, restriction to change in production to COE members; business users can perform approvals • Security – privileged access to make robot changes, host system profile protection, restriction of use • Humans interacting in the same process do not have access to make changes to robot instructions or tasks

Intelligent automation risks and related control activities

Risk domain	Risk description	Illustrative controls
Timely system outage/issue detection	Automation problems are not timely identified and managed, leading to a delay in their resolution and resulting in a negative impact to business processes.	• Interface and system error reports are generated and reviewed periodically to verify robots are running as planned and gathering the planned data through interfaces • Human review of issue and error reports and identifying next steps • Security – privileged access to correct system issues limited to COE and documented as incidents
Vendor/ third-party management	Risks are not effectively mitigated for robotics vendor relationship and outsourced services, leading to financial and reputational exposure.	• SOC report reviews, right to audit clauses, appropriate SLAs, defined maintenance contracts, limited vendor access with monitoring
Completeness/ accuracy of RPA processing	Input/upstream data is not completely/accurately received by the robot, or the robot may fail to completely/accurately process and calculate data to hand off downstream.	• Input data used in the execution of the process and any controls is generated completely and accurately from source systems (test of one configuration) • Data is processed completely and accurately by the robot prior to report generation or handoff to human or downstream application (test of one configuration) • Robot calculations are performed automatically based on preconfigured programming (test of one, configuration and recalculation)

Automation "hot spots" for risk and controls



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

1 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

5 Report development
- Generate consolidated reports using predefined logic for various aggregated reporting required
- Generate reports based on trends and issues identified in test execution (cognitive)

2 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 analysts to review based on set criteria and self-learning algorithms using structured information (cognitive)

4 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

3 Issue identification and upload
- Identify failures and report issues in issue management platforms
- Consolidate issues and conduct bulk uploads of test issues

Internal audit implications

Risk assessment areas for intelligent automation
Illustrative audit coverage

Regulators

SEC (Securities and Exchange Commission)

FDA (Food and Drug Administration)

HIPAA (Health Insurance Portability and Accountability Act)

CIP v5/6 (NERC)

GDPR (General Data Protection Regulation)

FRB (Federal Reserve Board)

OCC (Office of the Comptroller of Currency)

HITRUST (Heath Information Trust Alliance)

Risk assessment area	Risk assessment steps/considerations
Process/system identification	**Develop an end-to-end view of the RPA impact on the audit universe** • Demonstrate total inventory of processes/systems that utilize robotics

Impact on auditable entities and risk assessment	**Impact on RPA-related processes and systems should be explicitly incorporated in the risk assessment**
	• Map robotics process/systems to the organization's functions and entities
	• Determine incremental risks associated with robotics solution
	  • Processes/systems risks are already covered by existing controls
	  • Existing controls need to be enhanced to cover RPA processes/systems risks
	  • Incremental controls need to be developed to cover RPA processes/systems risks
	• Demonstrate how auditable entities will be covered based on regulatory requirements

Risk control matrix update	**Gain an understanding of risks and controls for each RPA process** • Risk-control matrices for each of the impacted business processes, with respect to both the inputs/transformations/outputs of the process, and the specific compliance standards required by the rules • Risk-control matrices for robot governance and robot platform

Audit procedures update	**Expand scope and depth of audits to cover the complexity of RPA processes**
	• Audit procedures to address the risks and controls of the processes in scope, for example:
	  • Business process and controls walkthroughs integrated with robot governance process and controls walkthroughs
	  • Procedures to validate consistent robot execution, incident management monitoring, robotic process scheduling change management and sequence
	  • Confirmation of information completeness and accuracy (user-defined attributes and extraction parameters)
	• Audit procedures will significantly vary based on risk and should follow the updated risk-control matrices

Reporting	**Consolidated view of compliance status and downstream impact of issues**
	• Provide an overall assessment of the effectiveness of RPA processes and controls
	  • Effectiveness of the controls around governance, processes, technology and integrations
	  • Status of issues identified by management and control functions

Intelligent automation internal audit coverage
Illustrative model

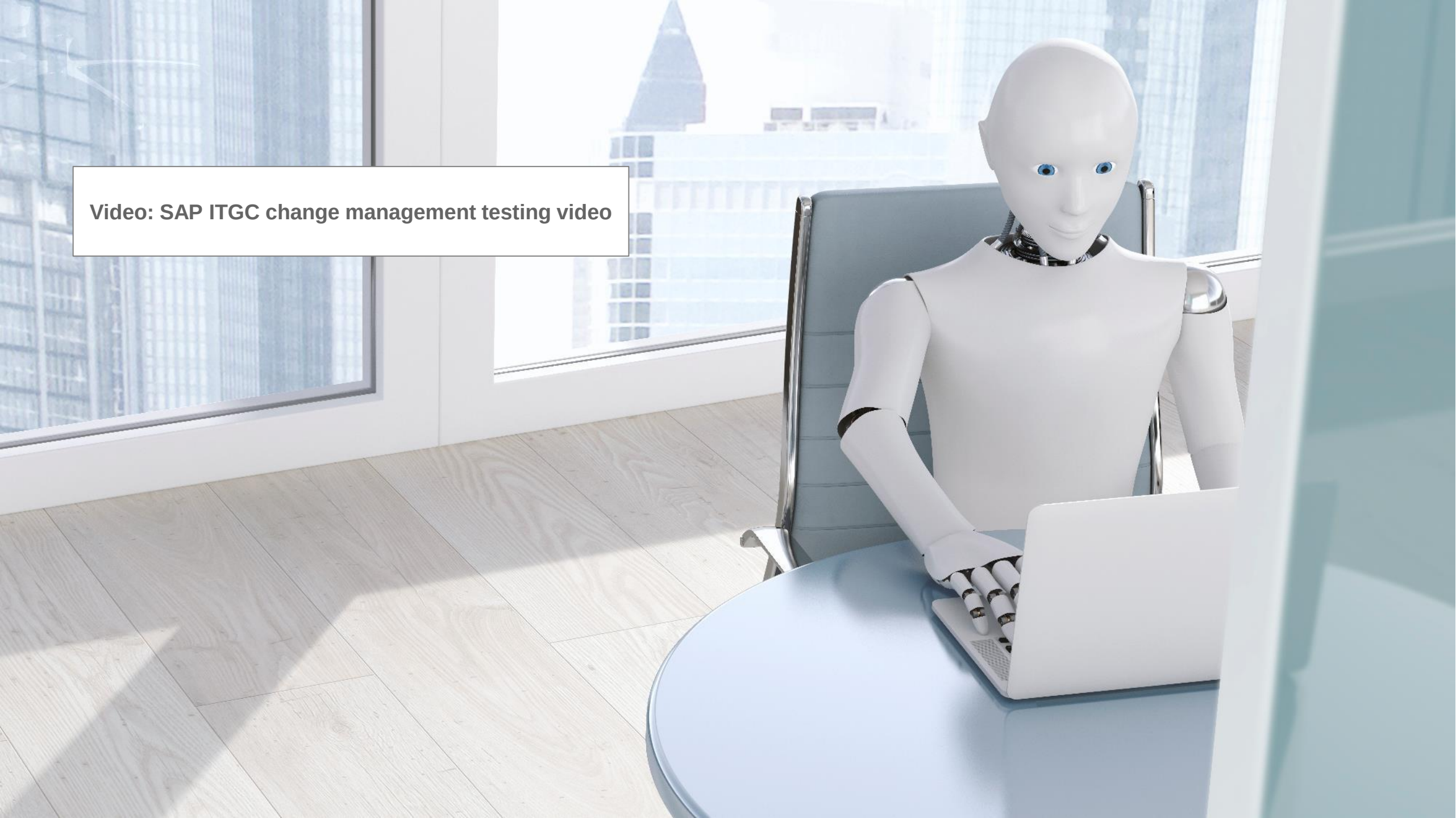
The following illustrates certain focus areas and enhancements to new and/or existing audits for IA functions to consider during their risk assessment and audit planning process.

	RPA program domains		
	Governance	**Value measurement**	**Processes**
Focus areas	• Standards, policies and procedures • Business and IT strategy • Organizational structure • Budget and resource management • Program ownership/accountability • Regulatory compliance requirements, monitoring, escalation, reporting and resolution • Risk management/appetite • Information and data management	• Opportunity criteria • Prioritization • KPI/KRI definition • Systematic anomaly/trend detection • Cost savings and efficiencies gained • Management/Board/executive reporting	• SDLC framework adherence • Requirements definition, assessment, prioritization and approval • Design specifications and definition • Test environment (staging and validation) • Testing (user, unit, system integration) • Change and release management/deployment • Incident response/escalation • Independent validation • Workflow configurations
High-impact audits	• RPA data governance • Infrastructure and data program management • Strategic architecture governance • Risk management and oversight • Disaster recovery (horizontal)	• Incident and problem management • RPA governance	• RPA SDLC • Configuration management • RPA logic validation

Intelligent automation internal audit coverage
Illustrative model (cont.)

The following illustrates certain focus areas and enhancements to new and/or existing audits for IA functions to consider during their risk assessment and audit planning process.

	RPA program domains		
	Alignment and change	**Technology**	**Enterprise integration**
Focus areas	• Communication • Training/knowledge transfer • Culture/job security • Reallocation/reprioritization of resources	• Information security/authentication • Encryption requirements • System maintenance/updates/service management • Code protection • Version control • Scalability options • Hosting options • Interfaces • Baseline settings	• Architecture design, management and compliance • Availability management • Capacity management • Service continuity management • Vendor management • Business continuity/disaster recovery service-level agreement
High-impact audits	• Change management • RPA governance	• Data privacy • Cloud computing • Vendor risk management • Network/information security	• Organizational change management • Monitoring of RPA process capabilities • Skills development assessment • Business process redefinition


Video: SAP ITGC change management testing video

Brainstorming the potential use cases for internal audit…

IT general control testing

- Change management
- New user access
- Terminated user access
- User access reviews

- *Other?*

Business process

- Manual journal entry review
- Time & expense
- PPE reconciliation (fixed assets)
- Revenue recognition monitoring

- *Other?*

Communication/reporting

- Manage creation, population and positioning of status reports
- Draft audit reports inclusive of issue description, impact and recommendations
- Document testing lead sheets to reflect closure of issues identified
- Perform reconciliation between scope, risk and control matrix, design and testing observations, issues log and final report to ensure alignment

- *Other?*

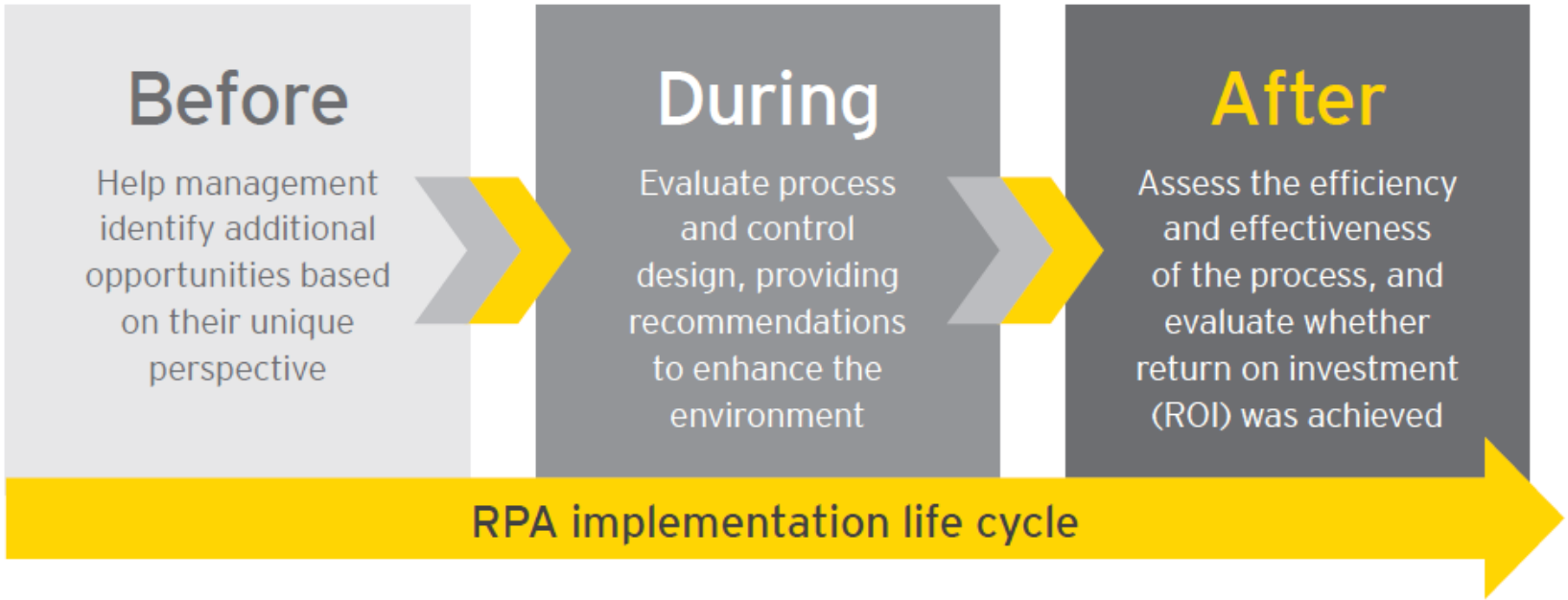
Consider activities where you are…

- Manually accessing and gathering data from several different applications to complete your activities
- Manually moving data from one system to another
- Manually checking the consistency of data between multiple systems
- Manually updating the same information in multiple systems
- Manually remediating data across several accounts

What’s the bottom line?

Whether your organization is embarking on its RPA journey or is already well on its way, it’s vital for your organization to establish an RPA strategy that includes comprehensive governance, risk and control practices, and IA can bring business, risk and internal control insights to that strategy.

Organizations may bring in IA after implementation to assess how well the process and controls are operating, but what they fail to understand is the contribution IA can provide before, during and after RPA implementation. IA can help management navigate each stage of RPA implementation by providing an independent evaluation and strategic advice. The financial and reputational implications of waiting to act and getting it wrong are steep. IA can help chart a course for success.



RPA application - Control Automation vs Controls Testing automation…

Bringing value to the organization through innovation in the IA function

- Opportunities for 3rd line of defense automation to become 2nd line of defense controls

Audit process enhancement opportunities

Control testing automation	Control automation
► We will be looking to technology to address new audit testing needs and increase efficiency. A number of technical approaches such as Controls Compliance Automation can help achieve targeted automation of the audit process. ► RPA can be leveraged to test high volume, high transaction controls with limited human intervention(3-way match testing, user access testing).	► Robotics can be leveraged to perform controls across a wide array of processes. Ideal candidates are high volume high-transactional controls(pricing changes, access provisioning). ► Robot can read different file types to take human error out of critical data entry controls.

Key benefits of automation

Control testing automation	Control automation
► The robot would perform the defined test attributes for the control, fill out the required testing information, and identify and alert the necessary individuals of control test exceptions. ► Robots can perform substantive tests on control exceptions to determine exact impact in control aggregation and assessment(if a control fails, the robot can check every single transaction to determine the actual impact, hence more accurate reporting).	► If a control leverages robotics for the performance of the control, the assessment of the control will shift to a test similar of a current day automated control(with some limited scope ITGC associated to the bots).

Contact information

Daryl Box | Partner | Advisory Services
EY Houston | Direct: +1 713.750.1498 | Mobile: +1 214.507.4902
daryl.box@ey.com

Jon Smith | Senior Manager – Risk Assurance | Advisory Services |
EY OKC | Direct: +1 405.278.6835 | Mobile: +1 405.612.7322 |
jon.smith2@ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

ED None

ey.com