weaver

Assurance • Tax • Advisory

Ron's Gone Wrong!

How To Guide Your RPA Program and Manage Compliance With Bots and Citizen Developers

Your Presenter:

Morgan Page, CIA
Partner, Digital Transformation and Automation
Weaver

SCAN ME

Today's Agenda

- What is RPA and citizen development?
- Benefits of RPA
- What are the risks?
- How can we control the chaos?
- How can IT and the Business manage the development?

Digital Transformation

Understanding Digital Transformation

- Digital transformation is the function of **understanding** the interrelation of **People, Processes, and Technology** and identifying where technology can **enhance** the process.
  - Digital transformation isn't about technology!
  - Culture is a bigger driver of success than anything else
  - The process doesn't have to change to be enhanced
  - The best value comes from the bottom
  - Your IT department can support, but not drive

RPA vs Automation

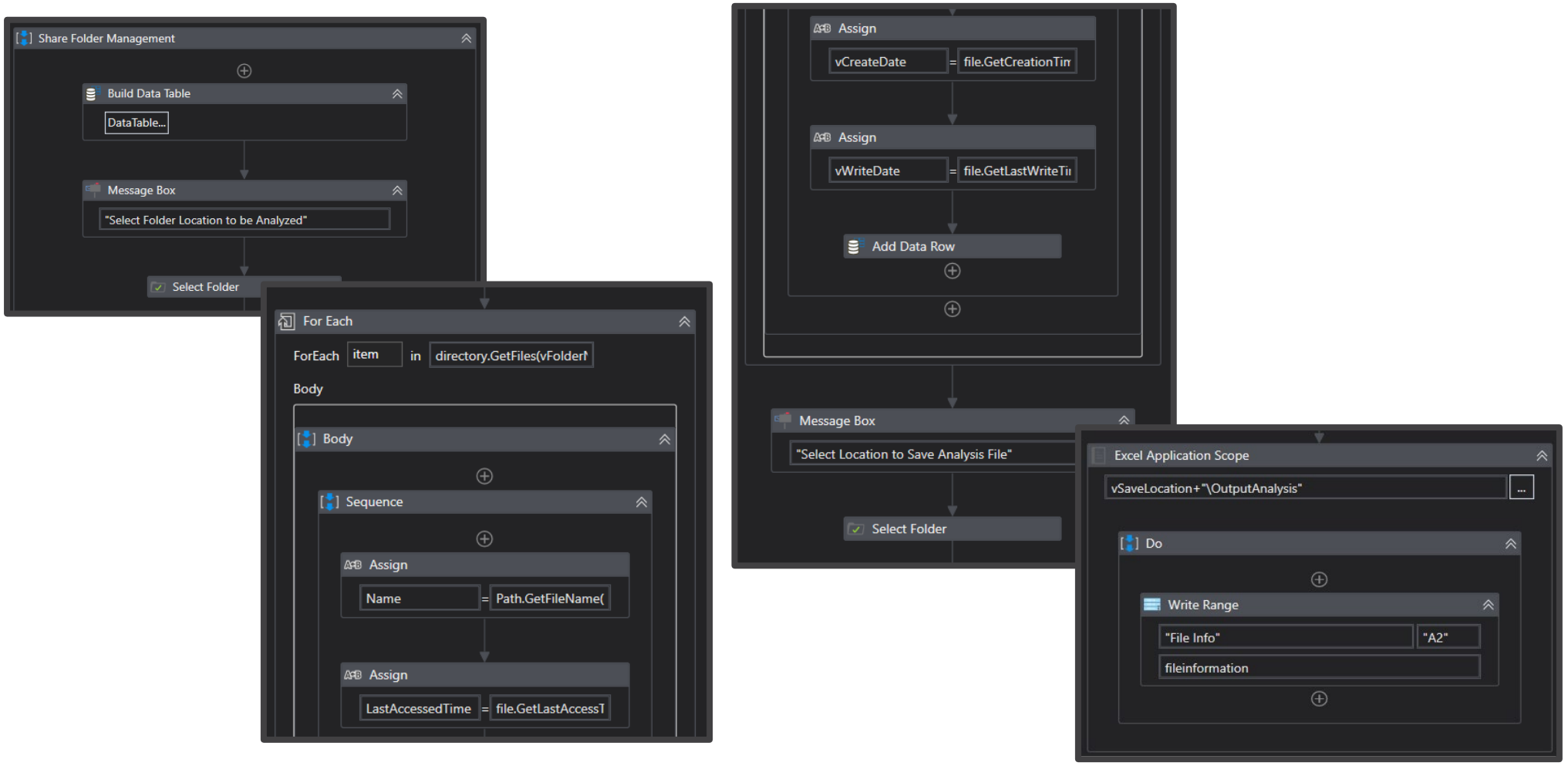
What is Robotic Process Automation?

- Robotic Process Automation (RPA) is the use of **applications** that leverage a **low-code** or no-code development schema to commonly in the application layer interface.
  - Applications include UiPath, BluePrism, PowerAutomate, AutomationAnywhere
  - Solutions are a platform and often use "marketplace" functionality
  - Most solutions have an Enterprise platform and a Personal platform
  - Solutions are expected to have a higher failure rate

What is RPA and citizen development?

RPA vs. Automation

An RPA Example



RPA vs Automation

What is Automation?

- Automation is the utilization of **the full technology ecosystem** of applications, technology enablers, scripting, and triggering events to **create a solution** to a business problem.
  - Automation solutions may exist within one application or many
  - Creative design may extend functionality in non-traditional methods
  - Functionality leverages same secondary services as RPA
  - Cost is typically already incurred or low
  - There is a higher learning curve and experience needed

RPA vs. Automation

An Automation Example

PowerShell Scheduled Initiation Script

```powershell
$input = @{}
$input = ConvertFrom-Json (Get-Content .\Sandbox_Tokens.txt | Out-String)

$access_token = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($input.Access_Token))
$refresh_token = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($input.Refresh_Token))

$refresh_headers = New-Object "System.Collections.Generic.Dictionary[[String],[String]]"
$refresh_headers.Add("Content-Type", "application/x-www-form-urlencoded")
$refresh_headers.Add("Accept", "application/json")
$refresh_headers.Add("Authorization", "Basic QUI2YjdyRnRPSU1vQjNXaG1VTGo2SkhxNXN5TDVhdXpyRGpyRmhyS2ZCe1k3NVZuNlo6U0Q3Z1JrM01RWXhNaUZNaW5zaUp2SWI4bXVaZzB0WU0xeX1nTHpFdg==")

$refresh_body = New-Object "System.Collections.Generic.Dictionary[[String],[String]]"
$refresh_body.Add("grant_type", "refresh_token")
$refresh_body.Add("refresh_token", $refresh_token)

$refresh_response = Invoke-RestMethod 'https://oauth.platform.intuit.com/oauth2/v1/tokens/bearer' -Method 'POST' -Headers $refresh_headers -Body $refresh_body

$access_token_bytes = [System.Text.Encoding]::Unicode.GetBytes($refresh_response.access_token)
$access_token_encoded =[Convert]::ToBase64String($access_token_bytes)

$refresh_token_bytes = [System.Text.Encoding]::Unicode.GetBytes($refresh_response.refresh_token)
$refresh_token_encoded =[Convert]::ToBase64String($refresh_token_bytes)
```

Python Analysis Script

```python
import matplotlib.pyplot as plt

def get_data(filename):
    # Check if file is as CSV or Excel file and read in accordingly
    if filename[-4:] == '.csv':...
    if filename[-5:] == '.xlsx':...

    # Define what columns are needed for analysis and their data types
    col_types = {...

    # Filter dataframe down to necessary columns and assign them the correct data types
    df = df[col_types]
    df = df.astype(col_types, errors='ignore')

    return df

def summerize(df):
    # Sum up the detail amount column
    summary_df = df.groupby(['@ID','Vendor','Vendor Name', 'Invoice #', 'Invoice date', 'Voucher', 'Due date', 'CC.NO', 'CC.NAME','Invoice amt'], as_index = False).sum()
    summary_df['Detail Amt'] = summary_df['Detail Amt'].round(2)
    return summary_df
```

Citizen Developers

What is a Citizen Development Program?

A Citizen Development Program is an architecture that provides tools that **require minimal technical knowledge** to a broad business user base to allow development of automations at a grass roots level to **create a solution** to a business problem

- Citizen Developers are Business Users
- Expands your resourcing by crowdsourcing design, MVP development and testing
- Faster speed to market but less traditional enterprise design

Benefits of RPA

The Benefits

- What is driving the transformation?

1. **Increased Productivity and Reduced Mental Stress**
2. **Increased Agility**
3. **Increased Customer Engagement and Satisfaction**
4. **Increased Opportunities**
5. **Higher Levels of Productivity**

The Detractors

- What is slowing or stopping the transformation?

94% of businesses are facing entrenched barriers spanning across technology, people and policy. (Dell Technologies Digital Transformation Index 2020)

1. **Data privacy and security concerns**
2. **Lack of budget and resources**
3. **Unable to extract valuable insights from data and/or information overload**
4. **Lack of the right in-house skill sets and expertise (analytics, technology, and business skills)**
5. **Immature digital culture: lack of alignment and collaboration across the organization**

What are the risks?

RPA Business Risks

- Automating makes a bad process be bad faster
- Consistency creates complacency
- Increased technical debt
- Automation is inherently historical
- Business owns the burden of maintaining the solution
- Often operate at a high level of privilege

RPA IT Risks - Governance

- Insufficient Governance over Citizen Development
- Lack of Monitoring or Logging of Bot Transactional Activity
- Lack of management of authentication or least access privilege

RPA IT Risks - Access

- Elevated Access Privileges
- Unattended vs. Attended Bots
- Co-sourced Developers
- Cybersecurity Risks
- Bots Operating at Database Layer

RPA IT Risks - Development

- Insufficient User Acceptance Testing
- Use of Unauthorized Plugins/Toolkits from Marketplace
- Incomplete user understanding of the total process

RPA IT Risks - Other

- Source Data Synch Dates
- RPA Platform - On Premises vs. Cloud

How can we control the chaos?

Best Practices for RPA

- Establish Governance and Oversight Program
- Communication between IT & Business
- Implement Strong Development Controls
- Access Controls for Bots – Principle of Least Privilege
- Use of Password Vaults / Credential Library
- Only Use Authorized Plugins from Development Platforms

Best Practices for RPA

- Create a framework for development
- Initiate with blended (IT / Business) teams to knowledge share development practices
- Create a CoE for development
- Create classification for data and ‘bots to identify higher risk activities

Best Practices for RPA

Process Area	Control Objective	ITGC Area	RPA Control Activity	Comments
User Administration	Control Objective 1: Financial reporting systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.	Authentication/ Passwords	Access to the secured tenant is authenticated through accounts and passwords or other methods to validate that users are authorized to gain access to the system. Password parameters are configured in accordance with company policies (e.g., password minimum length and complexity, expiration, account lockout).	This control may be subsumed into an enterprise single sign-on control.
		New/Modified User/Transfer (Access Provisioning)	N/A - No RPA specific control required.	No control is necessary if the access process follows the common process for the secured tenant.
		Termination/ Transfer (Access Revocation)	N/A - No RPA specific control required.	No control is necessary if the access process follows the common process for the secured tenant.
		User Access Review	User access is periodically reviewed to confirm access rights to applications and data.	
		Physical Access	Physical access to the data center is appropriately restricted to only those personnel who require the access to perform their assigned duties.	This control is only applicable to on-prem deployments (less common)
		Administrator Access to Application	Administrative access to applications is authorized and appropriately restricted.	
	Control Objective 2: All IT components, as they relate to security, processing, and availability, are well protected, would prevent any unauthorized changes, and assist in the verification and recording of the current configuration.	Administrator Access to Network	N/A - No RPA specific control required.	
		Administrator Access to Operating System (OS) and Database	N/A - No RPA specific control required.	
		Shared Accounts	Access granted to administrative generic, service, and/or vendor accounts is appropriately secured and restricted to authorized personnel only.	This control relates to access by developers or service accounts into the application and secured tenant.
			Access granted to users to view, edit, or modify RPA "assets" is appropriately restricted to authorized personnel only.	This control relates to the management of the access assets (service User ID and password) stored in the secured tenant environments.

Best Practices for RPA

Process Area	Control Objective	ITGC Area	RPA Control Activity	Comments
Change Management	Control Objective 3: System changes of financial reporting significance are authorized and appropriately tested before being moved to production.	Program Changes are Authorized/ Requested	System changes are appropriately requested/documented and authorized prior to development.	This control is only applicable to on-prem deployments (less common)
		Program Changes are Tested	System changes are appropriately tested before being moved into the production environment.	This control is only applicable to on-prem deployments (less common)
		Program Changes are Approved	System changes are approved by management before being moved into the production environment.	This control is only applicable to on-prem deployments (less common)
		Emergency Changes	Emergency change requests are documented, tested (prior to implementation or after implementation), and approved.	This control is only applicable to on-prem deployments (less common)
		Change Management SOD	Access to implement changes in the application production environment is segregated from the development environment.	This control is only applicable to on-prem deployments (less common)
		Access for Developing/Implementing or Monitoring	All automation designs developed and deployed to the production orchestration application are assessed for financial and compliance risks.	
Development and Acquisition	Control Objective 4: Systems are appropriately tested and validated before being placed into production. Processes and associated controls operate as intended.	Program Development User Acceptance Testing	User acceptance testing is performed, documented, and approved by management prior to the implementation of new or updated automation and evidence of testing and approval is appropriately retained.	
		Program Development Data Conversion Testing	N/A - No RPA specific control required.	
		Program Development Executive Go-Live Approval	Formal go-live approval is documented prior to system development, implementation, or upgrades are moved to production.	

Best Practices for RPA

Process Area	Control Objective	ITGC Area	RPA Control Activity	Comments
Backup and Recovery	Control Objective 5: Data recorded, processed, and reported remains complete, accurate, and valid throughout the update and storage process.	Backups	Production automation packages are backed up on a regular basis according to an established schedule and frequency.	
Job and Interface Monitoring	Control Objective 6: Authorized programs are executed as planned and deviations from scheduled processing are identified and investigated, including job scheduling, processing, error monitoring, and system availability.	Job Scheduling	Only authorized users have access to the automation scheduling and monitoring tool.	
		Batch Processing	Scheduled jobs are monitored to ensure successful completion.	Where this applies to critical ICFR controls, notification of control performer should also be considered as part of this control.
Incident Management	Control Objective 7: Problems and incidents are properly responded to, recorded, resolved, and investigated for proper resolution.	Incident Management	Incidents for automations in the secured tenant are documented and resolved in a timely manner.	
Vendor Management	Control Objective 8: Third-party services are secure, accurate, and available; support processing integrity; and are defined appropriately in performance contracts.	Third Party Reports Review	Third party reports are reviewed, including relevant System and Organization Control (SOC) reports.	This control is only applicable to cloud deployments (more common)

weaver

Assurance • Tax • Advisory

Morgan Page, CIA

Partner, Digital Transformation and Automation

SCAN ME

SCAN ME


weaver
Assurance • Tax • Advisory