# JOINERS, MOVERS AND LEAVERS (JML) PLAYBOOK

**Stephen Mowll**

RSA Identity Management Architect

**June 2016**

# INTRODUCTION

This document provides an overview of the Joiners, Movers and Leavers (JML) process, including all of the different elements that you will need to be successful in creating or improving and maintaining that the JML process.

Using the information provided, you will be able to define what success looks like for your organization, and define a maturity path to get there.

There are 2 key elements needed for you to be successful in managing the JML process. The first is understanding ALL of your identities and why they are working in your organization and having processes to capture all of them.

The second is understanding how they interact within your organization. Are they just a normal employee or do they have unusual work patterns such as working for 3 months and then leaving for a month before returning?

In this JML playbook we will look at the details of these elements.

## Audience

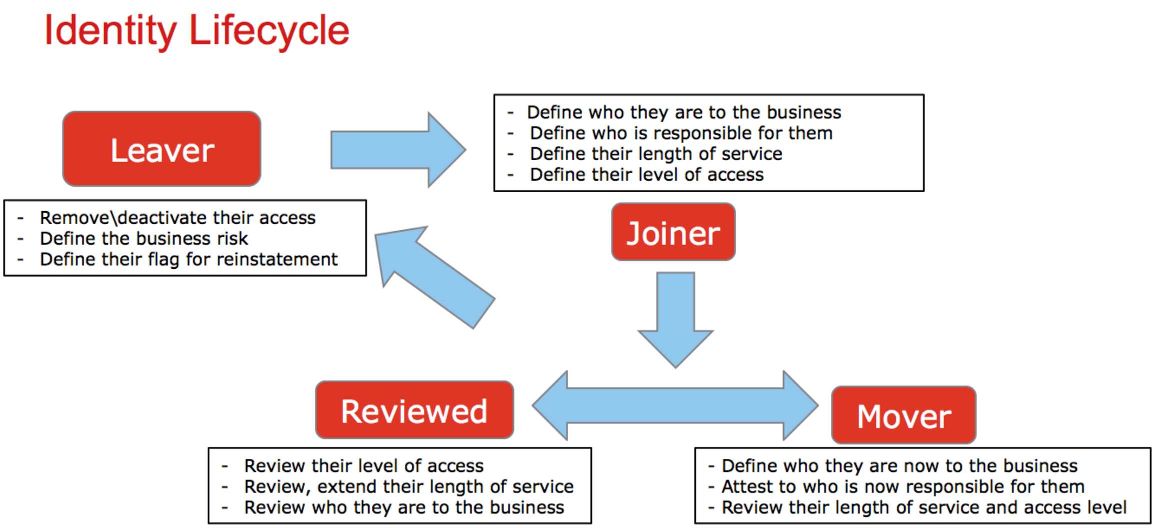
Anybody who is interested in implementing or improving JML processes or understanding more about them.

## What are Joiners, Movers and Leavers (JML)?

The short answer is “A business process to manage people and their business needs as they work within your organization.”

This is a very short description for what you will see is a very complex problem.

One key point to remember is that this is a business process and not just about the management of access.



Identity Lifecycle
Leaver
- Remove\deactivate their access
- Define the business risk
- Define their flag for reinstatement
- Define who they are to the business
- Define who is responsible for them
- Define their length of service
- Define their level of access
Joiner
Reviewed
- Review their level of access
- Review, extend their length of service
- Review who they are to the business
Mover
- Define who they are now to the business
- Attest to who is now responsible for them
- Review their length of service and access level

# SETTING THE SCENE

Today, the JML process is typically implemented for employees and/or contractors as they move through your organization. The process itself is driven by changes in Human Resources (HR) data although sometimes companies have contractor management systems or repositories such as Microsoft Active Directory.

What companies often find with this process is that the HR data is not created or maintained in such a way as to allow the process to be 100% successful. This is because the HR data and processes where never built to drive Identity and Access Management (IAM). This leads to delays and errors in the process and ultimately, continued problems with JML processes. These could be business related such as a contractor never getting the access they need and not completing their work in the time given, or people who have left the company but still maintain active privileges or access to sensitive data.

There are also typically gaps in the process because other identity types are not included.

This can be because they do not get registered with HR such as Temporary Workers, summer interns, Auditors (quite a big one there) or vendor/support consultants. In these cases, often accounts are just created for them using other people’s identities or via direct requests.

Also many organizations have multiple sources of Identity that can further complicate the problem, particularly if they do not use the same data structures.

### Defining a JML Process

Now that we have set the scene, in this section of the playbook we will look at the JML process and its different components. As companies are at different levels of maturity we will look at the best practices for each element.

## IDENTITY MANAGEMENT

For this process to be successful, every physical person that has access to an IT system or application must have an Identity. At a minimum, their identity must provide the context needed to determine, who they are, why they are here, what will they do while they are here, how long are they staying and who is responsible for them. The information should also contain (1) or multiple unique identifiers so you can differentiate users with the same context e.g., John Smith, Developer, Permanent Employee.

As the first step, you must define all of the processes in which an Identity will be created, changed and ended. This is really the true identity lifecycle as the other elements of this process will be reliant on this data and any gaps will cause issues in your organization.

It is also very important to map the FULL process and not just the process from where you take action. This includes, for example, the HR process preceding any identity creation or access management. Why do this? Because once you understand the full process you can influence it and add in components you need to be successful.

Some examples:

- Asking a new user to select their email address in their HR onboarding process, removing the need for complicated automated email determination processes.
- Knowing if the attributes you need for your JML process are not required fields in the HR process.
- Understanding that temporary staff can be brought in to cover receptionist functions with 1-day notice and are not in HR.
- Being aware that the Payroll system is always updated automatically with a change in employee role and level but HR is a manual process.
- Managers calling HR to notify them of users leaving the company rather than using the automated portal, meaning termination attributes are not updated for over 24 hours.

All of these types of information affect your JML process and its effectiveness!

It is also important to note that depending on the size for your organization, you may have more than one JML process flow depending on the line of business or types of identities you have.

## JOINER, MOVER & LEAVER IDENTITY MILESTONES

During the identity lifecycle of a user, there are a number of key milestones that can help you understand what is happening and help you to ensure you have a successful JML process. These milestones are also very good Key Performance Indictors (KPI) to measure your success.

### Hire Date

The date your company knows they will be bringing in a new user. This would be when they are entered into the HR system for the first time, when they register their identity or when a contract is signed to engage in work with a 3rd party.

### Start Date

The first day the user will work for the company and needs access to systems and applications. The amount of time between the hire date and start date is your lead time for onboarding the new hire. Typically for employees this is 2-4 weeks and sometimes longer depending on the notice period of the user. For contractors this is often less than 24 hours and in at least 10%+ of cases is actually after they are onsite. This general culture of waiting until the last minute to request access is also a big driver for automation where in reality it is the culture that needs to change.

Also consider that some users first days onsite might be in training and they may not require systems access until this is completed. Why does this matter? Because if they do not complete the training they might never need it.

### New Hire Flag

For the first 90 days of a new hires employment, it is good practice to set a flag to alert others in the company to the fact that they are newly employed. This can give them priority for access request, training and asset requisition.

### Transfer Date

The commonly used process for identifying a transfer is to look at how identity attributes change and trigger mover processes based on this, but this can generate a lot of fail positives and business notifications going out when they should not.

When a person moves within your company there will be a process for the manager, or appropriate person, to advise of the transfer.

A transfer process should generate a transfer date. Using a date also has the benefit of giving you lead-time to understand what needs to change in their new position.

For many HR systems, that can be a challenge and often a transfer of a user is actually a new HR record and not an amendment of an existing one. Due to this, transfer dates may need to generate out of the process and not collected from the HR record.

### Leaver Notification Date

Date the manager or responsible person notified HR that the user was leaving the organization.

### Termination Date

This is the last working day of the user.

## IDENTITY DATA

The JML process, as with many other Identity and Access Management processes, is data driven. This means that you must have the information needed to make effective decisions or have the ability to ask the question and get the information needed.

Get this data right and you will always be successful, get it wrong and your processes will never work properly!

The following are common data sources of Identity Data.

### HR Data sources

HR is a good source of information, but as already mentioned, it was not created to drive identity management but to manage employees and sometimes contractors through their employment. That might sound like the same thing, but it's not usually seen that way. In many companies HR and IAM teams wage war over poor data and bad processes. To be successful in your JML process, communication and collaboration between these two teams must be established.

Collecting data from an HR source is not enough. You also need to understand the processes that are in place to change the data and how it can and will change. Once this is understood then 2 things can happen.

1. You can ask for changes in the processes to fit your requirements.

2. You can adapt your process to take account of situations that might break it.

The best way for you to integrate with any Identity source, but particularly from HR for JML processes is to integrate into the HR process and set flags or dates when actions occur rather than guessing when something has happened, particularly for transfers and leavers.

In almost all of the JML projects RSA has been involved with for people moving in the company, project leads are guessing as to whether the user has moved based on a change in attributes such as department and supervisor. Why so much guessing? Because the attributes that are used can change for all kinds of other reasons! Organizational change is very common in companies today, initiating mover processes for many people who have not moved at all.

For terminations, the JML process commonly works on the fact that if the HR record is removed or a termination flag is set, then the termination process begins. However, one of the biggest challenges with terminations is people being set to 'Terminated' in error and being corrected shortly after. This is too late for most termination processes as access has been disabled or deleted.

In both of these cases, the HR process knows a user is changing roles or leaving the company weeks and sometimes months before it happens. Having HR processes with set Mover or Leaver dates enables your JML process to:

1. Notify the user and their sponsor that there is an event pending and if it's incorrect to contact HR to correct their data.

2. Have significantly higher assurance that when you trigger a mover or leaver process that they have actually moved or left.

### Identity Registration

Identity registration is a process often setup for users who are not managed within HR, e.g., temporary workers, contractors, auditors, partners or customers.

It requires the same types of considerations as your HR data sources, but the nice thing about this process is that you can control it and the data you get from it.

The challenge with identities created in these processes however, is that they usually change a lot more often than those coming from HR, and also the rejoiner use case becomes much more important. Examples might be:

- A retailer who hires staff to cover busy shopping periods. These people might come and go depending on how busy they are.

- A hospital employing contract doctors and clinical staff who come and work ad-hoc. They might work for a week, leave for a month, and then come back. It is important to know that they are the same person that keeps returning.

- An out-sourcing company is used to manage your infrastructure and regularly changes the people performing the work depending on who is available. It is also important to know what 3rd parties have access to and when.

It is also important to note that with these kinds of processes you have a very short lead time to manage changes as there is no upfront process. On average you will be made aware of the change less than 24 hours before it takes place.

### Active Directory (AD)

While AD is used is many companies today as an identity source for temporary workers, this is a very bad approach. The 3 main reasons are:

1. Account creation processes are creating the identities. This means that there is no separate record to understand who they are in the company and the process itself does not ask the right questions to manage them correctly.

2. Their identity is an account with access and when you want to remove that access you have to delete their identity. This means you might never know they existed in your company previously. Some companies get around this by disabling the account and moving it to a different place in AD creating a messy and hard to manage process. Why keep an account, even a disabled one if you do not need it.

3. Creating accounts in AD as identities does not support the triggers you need to manage the users for movers or leavers processes. This can often mean the person leaves, but the account just remains active in AD.

## IDENTITY ATTRIBUTES

As we go through the JML process, we will define these elements in more detail but at a minimum you will need to have the following details in your identity dataset.

### Unique Identifier

Usually this is a random or sequential generated by your HR system or identity registration process. However, one of the biggest challenges you will face as you mature your JML process is people re-joining your company or moving from one type of identity to another such as contractor to permanent employee. These types of events can create duplicate identities and access creating the need for manual remediation and audit headaches.

Two good ways to resolve this are:

1. Include in the user identity data a hashed or subset of their national identifier such a Social Security Number or National insurance number. This must be an identifier that never changes so that you can always be sure that the identity is the same person.

2. Combination of non-unique identifiers. This must be at least 3 values such as full name, date of birth, mother's maiden name.

Both values should be masked so that personal information is not being exposed in the Identity management system.

### Name

Full name of the user

### Job Status

As you might imagine, the job status of the user is very important to the JML process. While there are the obvious statuses, there are a number of others you might consider as you build and mature your JML process.

| JOB STATUS | DESCRIPTION |
|---|---|
| Joiner | A new user is joining your organization and will require initial setup |
| New Employee | Status of the new user for their first 60 days in the company, ensuring they get priority in the set-up of their access and support in getting enabled |
| Long Leaver | The user has chosen to take a break but is still an employee or is a contractor that has left but will definitely return to the company |
| Maternity/Paternity | There are specific requirements in the way a user's access must be managed as they are still employees. Access must not be removed but elements can be disabled |
| Long Term Sick | Could be covered in the long leavers status but as with Maternity/Paternity, there are specific requirements as to how the access for these users must be handled |
| Leaver | The user has left the organization |

### Job Role

This attribute is often used to determine the access that a user needs and also is a common trigger for mover processes. Depending on the size and complexity of your company, there can be multiple values that make up the job role of a user.

It is very important that you know how these values change, who can change them and when they are changed. In simple processes this might be an HR change and a simple rule e.g., Bob Smith was an IT administrator and is now an IT architect.

In more complex companies such as Retail Banking or Retail there are often more complex decisions that need to be made e.g., Mike Jones is a Teller at the Bournemouth branch but as the manager is off he is 'promoted' to acting manager until the manager returns.

Also note that these values are often used by HR teams to define pay scales and job levels of employees. This means that if the business changes these levels the entire structure could change.

### Location

The location attribute is also often made up of more than 1 value and can also be a trigger for the mover process.

### Organization/Department

The department attribute is another that can be made up of multiple values or a hierarchy. While this value is probably the most commonly used to trigger the movers process, care must be taken to not generate a huge amount of work when no move has actually taken place, such as reorganizations.

It seems in today's world, companies are constantly changing/merging/splitting and because of this, these values are not a reliable trigger for mover events. These values should always be used in combination with another identity value change.

### Supervisor

This value defines the person in your company that is responsible for this user. It could be this person's supervisor, manager or sponsor. This person is needed to perform the management tasks for the user to validate their identity attributes, access and entitlements.

### Contact Information

Email address is the main value here, but others include desk phone and mobile phone numbers. These are important for notifications during your IAM processes.

## NEW JOINERS PROCESS

### The Joiner Process

It is hugely important for people joining your company to have the best experience possible. It can have a big effect how long they stay, and whether they become a positive and productive member of your business.

Also, it is important to ensure that you take account of all the joiner processes this would include.

### New Joiners

A brand new person to the company. This is the simplest form of joiner.

### Rejoiners

The person has worked at the company previously. There are a number of evaluations that need to be done in this process as the user may have existing access that needs to be re-enabled or changed depending on if they are coming back to perform the same role or a different one.

### Non-employee to Employee and Employee to Non-employee

While this is sometimes seen as a transfer process, this is generally not the case. In scenarios such as a contractor becoming a permanent employee they need to be treated as a new joiner as fundamental elements of their access could change such as unique ID or email address. The process is typically more like a rejoiner.

The Best Practice joiner process would be as follows:

### Identity Creation/Discovery

New Joiner – HR/Contractor Process

- New Joiner confirms if they have worked for the company previously and provides previous identity details if possible
- New Joiner selects their email address from the available list
- New Joiner defines challenge response questions/ information for authentication
- New Joiner selects their User ID from available list

- New Joiner provides personal email and mobile number plus usage preference
- New Joiner is assigned a buddy for their first 4 weeks in the company
- Information is synchronized from the new HR joiner process into your identity repository

### Identity Validation

- Validation of the users attributes including unique identity
- Advise of any possible identity duplication

### Identity Evaluation

- New Joiner access is assessed based on their identity attributes
- Role evaluation is done to assign Role for standard access
- Evaluation of common, suggested access for the user based on analytics

### New Joiner Access Orchestration

- Standard birthright access should be assigned. This should be the same for every new user joining the company
- Role Assignment. A standard role with all of the access that is 100% required/common to the team the user is joining should be assigned
- Assignment of all additional access should be done in a single process using Identity Analytics to suggest other access that is held by the team

## REJOINER

### Identity Creation / Discovery

Rejoiner – HR/Contractor Process

- New Joiner confirms if they have worked for the company previously and provides previous identity details if possible
- New Joiner claims their previous email address or selects their email address from the available list
- New Joiner defines challenge response questions/ information for authentication
- New Joiner claims their previous User ID or selects their User ID from available list
- New Joiner provides personal email and mobile number plus usage preference
- New Joiner is assigned a buddy for their first 4 weeks in the company
- Information is synchronized from the new HR joiner process into the Identity repository

### Identity Validation

- Validation of the user’s existing attributes including unique Identity
- Validation of the identity values that have change since they were last active

### Identity Evaluation

- Evaluate access status for any existing access of the re-joiner

### New Joiner Access Orchestration

- Standard birthright access should be assigned or re-enabled. This should be the same for every new user joining the company
- Role Assignment. A standard role with all of the access that is 100% required/common to the team the user is joining should be assigned or re-enabled
- Assignment or enablement of all additional access should be done in a single process using Identity Analytics to suggest other access that is held by the team

# MOVERS PROCESS

The definition of madness is doing the same thing over and over again and expecting a different result. In many organizations, this describes the mover's process that is defined.

As discussed previously, the Mover process is often triggered when identity attributes change, typically manager, department or location attributes. However, these attributes can change for many other reasons such as the manager leaving the company. While it is safer to trigger the transfer based on a combination of attribute changes, this is still not fool proof.

As a best practice approach, the notification of a mover should come from the business process that is used to instigate it. If this was a mover flag or date, it is a solid assurance that you are triggering access changes based on a true event.

### Identity Change

- Mover flag is set for an identity

### Mover Validation

- Notify the manager that the move has been identified and that access changes will be evaluated

### Mover Evaluation

- Send access review to previous and new manager to remove access that is no longer required
- Send new manager a request suggesting any other new access required based on the common access of the current team

### Mover Access Change Orchestration

- Change role based access removing old role and adding the role for the new position
- Add/remove access selected in manager reviews
- Add new access requested by manager for new role

# LEAVER PROCESS

Within the leaver process there are 2 key things that you need to understand.

*Is the user truly leaving?*

There are many use cases where users leave and re-join companies frequently. Any company that uses outsourcers, has a branch network or call center will often see this situation.

Again, understanding the business need and the business process will help to define if access can remain dormant securely or if the period from leaving to re-joining is too great to consider leaving the access disabled in the environment.

*If the user is leaving, how quickly do you need to remove their access?*

Users with privileged access, confidential information or are leaving to join a competitor will need to have access removed in a more timely manner than normal users.

Both of these elements of information have to come from the business managers and answering these questions correctly will save a lot of pain for the business when users lose access, and will improve efficiency as access will not need to be re-created.

### Identity Termination Evaluation

- User advises that they will leave the organisation
- Termination notification sent by manager or set termination date approaching
- Manager advises the type of termination immediate or future dated

### Termination Validation

- Notification sent to manager prior to access removal
- Allow the manager to set a common rejoiner flag

### Termination Change Orchestration

- Disable all account access
- Remove all access entitlements after 5 business days or allow the access to remain for a longer period if the common rejoiner flag is set

# IMPLEMENTING JML PROCESSES

It is one thing to understand what your JML processes should be and quite another to implement them successfully. Implementing a successful JML process requires executive sponsorship, buy in from the business and most importantly, support and partnership with your identity providers, typically HR internally.

## Project Stakeholders

### CIO/CTO

C level sponsorship is essential to the success of the project. Changes to the JML process can be disruptive in the initial stages and changes in business process have to be sponsored otherwise pushback from the people impacted means that the most important improvements may never happen.

### CISO

The CISO or possibly the head of Identity Management must be the lead project sponsor. This is again to ensure the project has the executive power needed to push changes through.

### HR Executive

To ensure that any changes required to HR data and processes are supported and delivered, the Head of HR or a Senior Executive must be involved and sponsor the project. Without this the project will almost certainly fail to be completely successful.

### Line of Business Management

As the business is the area that will be most impacted by changes in the JML Process, sponsorship and inclusion of key executives in the business is important. They can provide feedback of the approach, changes to processes, areas of concern, while also giving you a vital communication channel to your end users.

### IT Management

Inclusion and sponsorship from IT is important to understand how the access management elements of the process can be completed.

# FIRST STEPS

Understand your current state – How do your processes work today? How successful are they? What do your end users think of them? How good is the data that drives them?

Define what success looks like – What to you want the JML process and experience to be?

Understand what's missing – Perform a gap analysis to understand what elements such as data and processes are missing to be successful.

Create measures to prove success – Key Performance Indicators (KPI's) should be created for this. KPI's you should measure include:

- Lead-time. This is the amount of time between when you are notified that a JML action is needed and the event happening. The more notice you have the more chance you will be successful. This is also a good indicator of the culture of your business in relation to IAM.

- Number of Users managed by the JML process, indicating the turnover of people but also the scale you are managing.

- Number of requests raised. Measuring the number of requests that are raised for users in your JML process gives you an indicator to how much effort users need to put in to use your process. Time to create a request and time to process the request are both quantifiable allowing you to show cost/effort reduction.

- Requests raised after start date.

- Movers with movers' reviews completed / not completed. This shows that access for users has been validated after they made a job change.

- Terminated users with Access. This metric shows the efficiency of your process. The reporting should show a timeline for how quickly access is removed after the users termination date.

- Number of Accesses removed for terminated users.

## Initial JML Service Implementation

In the initial project scope you must take an access governance based approach to orchestrate your JML process, validate the changes being made and confirm that they have completed successfully.

Using this approach you can confirm not only that the process works but also have visibility of any data issues you were not aware of.

Use your KPI’s to measure the successful improvements that have been made.

The initial set of systems and applications in your scope should be the key accesses needed by a new hire and the high risk systems where users must be removed in a timely manner.

If you are constrained and need to prioritize further, then the removal of access for leavers should be completed first as this is the simplest process to complete and poses the most risk to your business.

Movers should be the last process that you look to implement, as even with the recommendations made in this playbook the triggering of this process is the most complex of all JML activities.

## Expand your JML service

### Include integration for more applications

Once you have defined your JML process and implemented your initial service the onboarding of new applications into the orchestration of the process becomes straightforward.

Include in your project a standard onboarding process for new applications. The process should include the data and format you expect information to be received in or define the standard process and support needed to collect the data from the application directly.

Including more applications will reduce the amount of effort needed by the business to manage new users throughout their IAM lifecycle and also provide the control and visibility to assure access is managed correctly across your wider system and application estate.

### Introduce compliance checks and SoD (Segregation of Duties)

As you on-board applications and mature your JML process, the next key item to implement is the ability to detect access violations or potential violations of users as they move around your business.

Movers accumulating access as they change roles form one of the biggest potential threats to your organization for both risk and fraud.

Using a governance based approach to JML and including the standard application collections classification of Access for Compliance and SOD checks is important to making this process easy and dynamic.

Also include KPI’s in your JML service metrics for:

- Accesses without a classification.
- Number of access violations removed by month.

These metrics will show the control improvement your service has made to the business and auditors.

### Automate Provisioning

Automation of access provisioning is what a lot of people think about when they think of JML processes. While this can improve the efficiency of the process automation of some of the decisions involved, it can lead to a lot of compromises in the way access is created.

That said, it can greatly improve the user experience. Automation should be provided for all birthright access such as AD account and Email access. This means that users can login, perform essential tasks and get to know the organization.

For all other access automation you should look to prioritize the systems/applications and capabilities that provide the most benefit once you ensure that you can trust the data that your process is using to drive these decisions.

# GLOSSARY OF TERMS

**Identity** - The identifying information to provide context to.

**Joiner** – A new identity joining or potentially re-joining your organization.

**Re-joiner** – An identity that is returning to your organization after a period of absence, typically through termination or long leave.

**Long Leave** – An identity in your organization that is not active for a period of time, extending longer than 2-3 weeks. Examples include long term sickness, maternity leave or sabbatical.

**Mover** –Also called a transfer. This is an identity whose access needs to be reassessed because it has changed. For example, they have moved location, changed job role or moved to a new department.

**Leaver** – An identity that has left the organization and whose access needs to be reassessed.

**On boarder** – the person within a company that is responsible for the actions needed to enable a new user within an organization. This is often the user's manager.

**Lead time –** The amount of time you have from being notified of a JML change event until the actual event takes place.

RSA believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

www.RSA.com