Managing IAM in a startup world through automation

How to tame the beast of Identity and Access Management

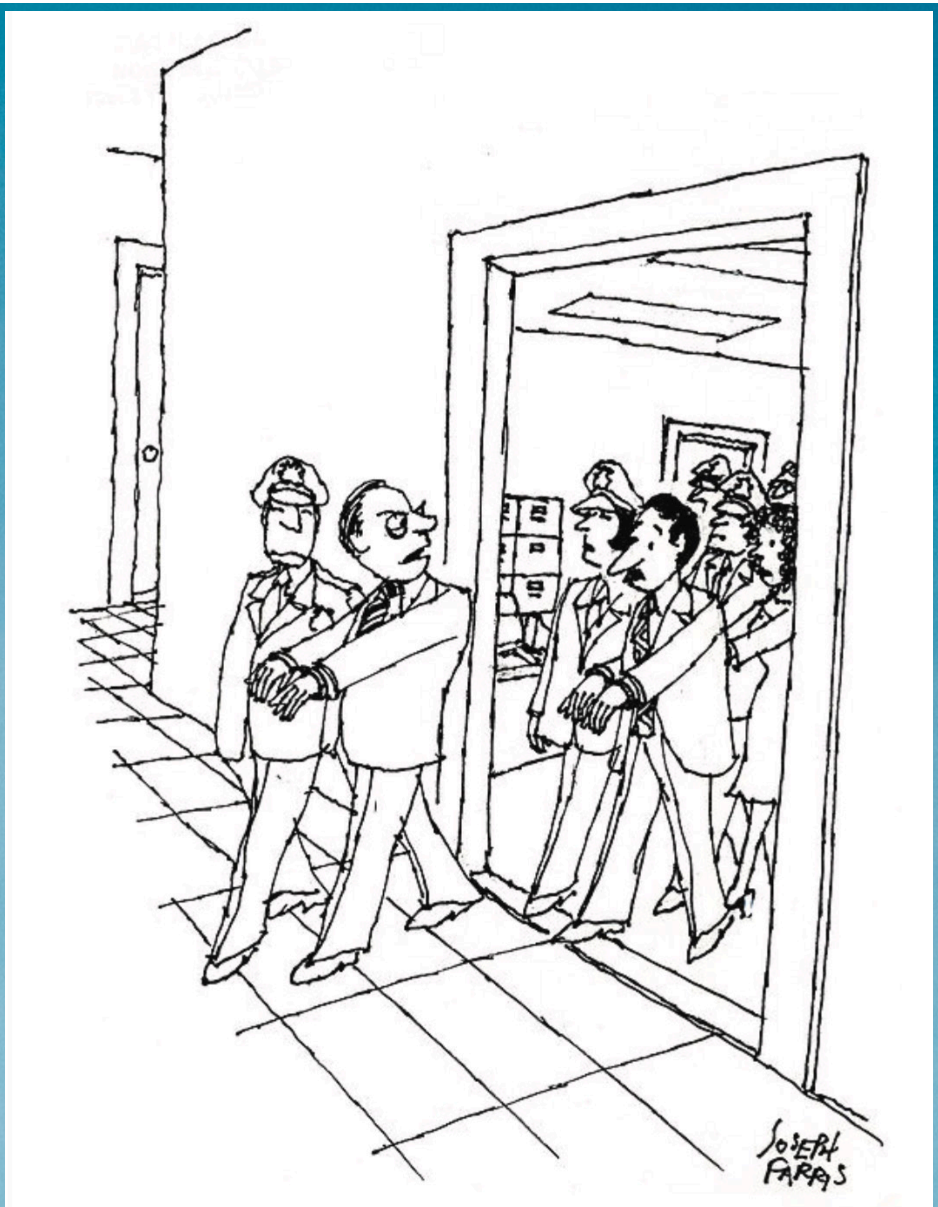
Fred Bret-Mounet, CISSP

2019

Disclaimer

This content is not

- Vendor sponsored!
- Employer sponsored!



"Whose idea was it that we give full disclosure?"

About Fred

- In the InfoSec field for the last 19 years
- Healthcare technology for 17 of those
- Developer at heart:
  - It's easier for me to talk to computers
  - I don't trust humans including myself

4/86

I’m also a Hacker!

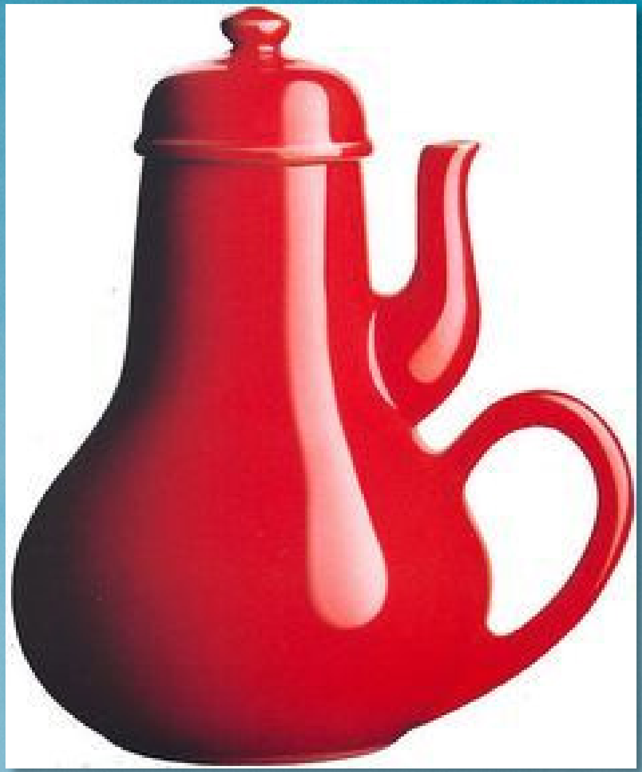
The problem

Understaffed

- Limited IT resources
- Manual provisioning / de-provisioning
- Unknown assets
- Unknown roles

User experience

- New employee onboarding
  - Takes weeks to get right
- Role changes
  - Never consistently processed
- Approval process
  - What approval process?!



Compliance

- If Best Practices is not driving you, here’s why!
- SOX, PCI, GLB, HIPAA, HITRUST all require:
  - Asset management
  - Regular access review
  - Access termination within 24 hours
  - “Need to know”
  - You will train your workforce appropriately

My situation

A lot of you will recognize yourselves!

- “One man show”
- 1-2 IT resources
- <200 employees
- >100 “apps”
- Most apps use stand-alone credentials
- Compliance pressures
- Limited definition of user roles

A solution

What has worked with me

- Application inventory
  - You need to know what you are managing
- Single Sign-On platform
  - Users love it
  - You have a single dashboard for monitoring and enforcement
- Automation (mostly using python)
  - You'll need to get your hands dirty or wait for vendors to integrate… in your next life!

It starts with an inventory

System Inventory

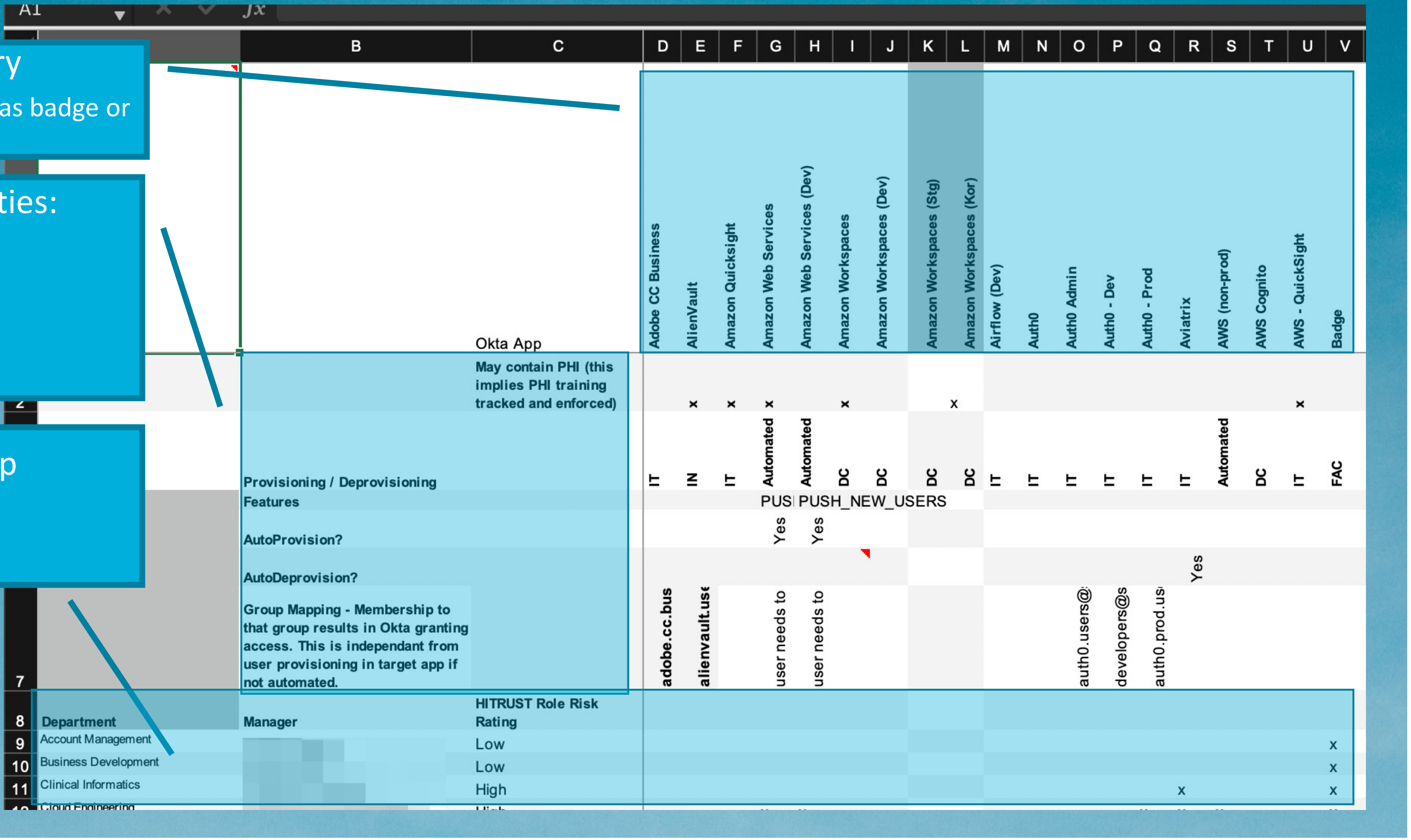
(also includes non apps such as badge or master keys)

Application Properties:

- PHI access?
- Owner
- Provisioning status

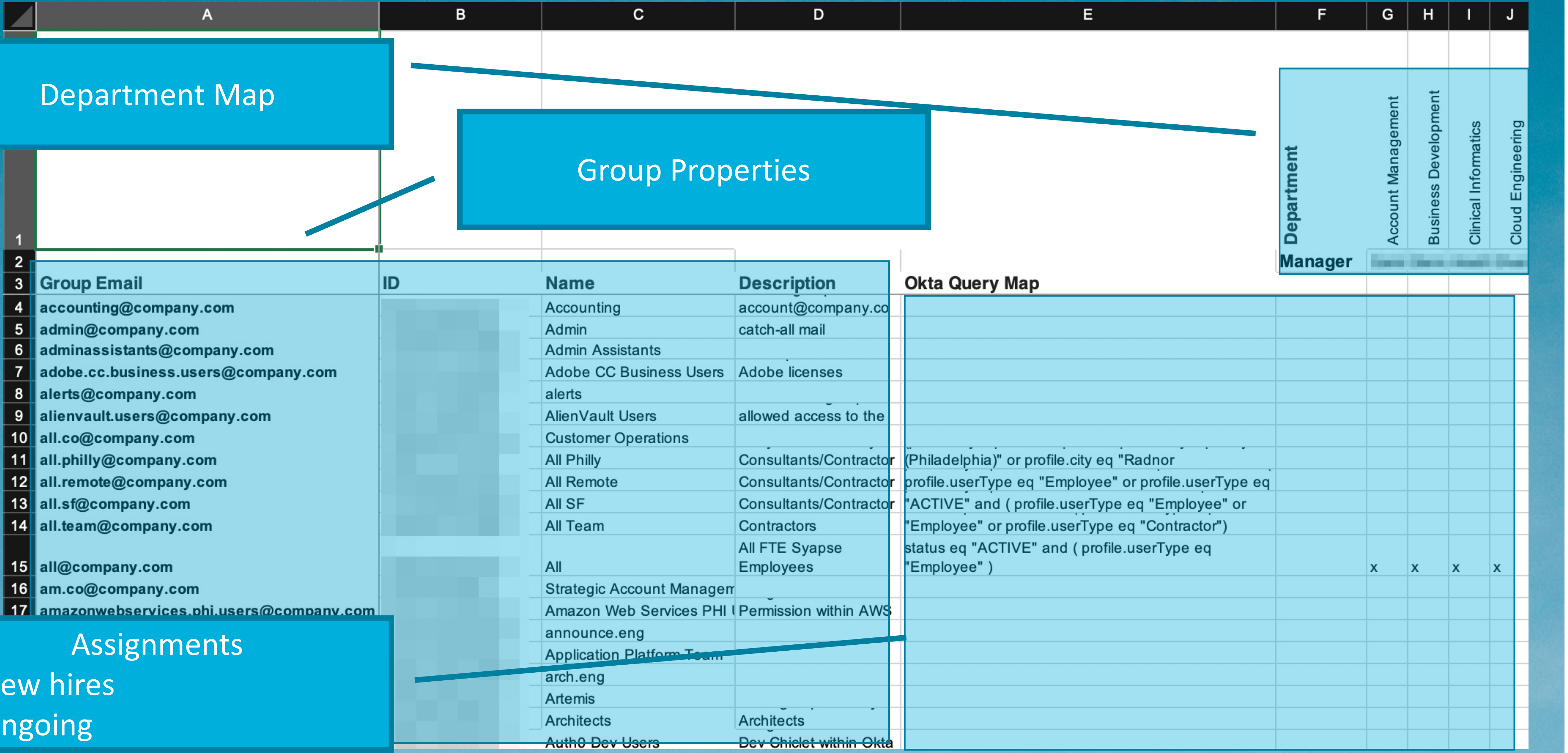
Department Map

- what, who
- Security risk rating



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
			Okta App	Adobe CC Business	AlienVault	Amazon Quicksight	Amazon Web Services	Amazon Web Services (Dev)	Amazon Workspaces	Amazon Workspaces (Dev)	Amazon Workspaces (Stg)	Amazon Workspaces (Kor)	Airflow (Dev)	Auth0	Auth0 Admin	Auth0 - Dev	Auth0 - Prod	Aviatrix	AWS (non-prod)	AWS Cognito	AWS - QuickSight	Badge
2			May contain PHI (this implies PHI training tracked and enforced)		x	x	x		x			x									x	
		Provisioning / Deprovisioning		IT	IN	IT	Automated	Automated	DC	DC	DC	DC	IT	IT	IT	IT	IT	IT	Automated	DC	IT	FAC
		Features					PUS	PUSH_NEW_USERS														
		AutoProvision?					Yes	Yes														
		AutoDeprovision?																Yes				
7		Group Mapping - Membership to that group results in Okta granting access. This is independant from user provisioning in target app if not automated.		adobe.cc.bus	alienvault.use		user needs to	user needs to							auth0.users@	developers@s	auth0.prod.us					
8	Department	Manager	HITRUST Role Risk Rating																			
9	Account Management	[redacted]	Low																			x
10	Business Development	[redacted]	Low																			x
11	Clinical Informatics	[redacted]	High													x						x
12	Cloud Engineering	[redacted]	High																			

It starts with an inventory - groups



	A	B	C	D	E	F	G	H	I	J
1						Department	Account Management	Business Development	Clinical Informatics	Cloud Engineering
2						Manager	[redacted]	[redacted]	[redacted]	[redacted]
3	Group Email	ID	Name	Description	Okta Query Map					
4	accounting@company.com	[redacted]	Accounting	account@company.co						
5	admin@company.com	[redacted]	Admin	catch-all mail						
6	adminassistants@company.com	[redacted]	Admin Assistants							
7	adobe.cc.business.users@company.com	[redacted]	Adobe CC Business Users	Adobe licenses						
8	alerts@company.com	[redacted]	alerts							
9	alienvault.users@company.com	[redacted]	AlienVault Users	allowed access to the						
10	all.co@company.com	[redacted]	Customer Operations							
11	all.philly@company.com	[redacted]	All Philly	Consultants/Contractor	(Philadelphia)" or profile.city eq "Radnor					
12	all.remote@company.com	[redacted]	All Remote	Consultants/Contractor	profile.userType eq "Employee" or profile.userType eq					
13	all.sf@company.com	[redacted]	All SF	Consultants/Contractor	"ACTIVE" and (profile.userType eq "Employee" or					
14	all.team@company.com	[redacted]	All Team	Contractors	"Employee" or profile.userType eq "Contractor")					
15	all@company.com	[redacted]	All	All FTE Syapse Employees	status eq "ACTIVE" and (profile.userType eq "Employee")		x	x	x	x
16	am.co@company.com	[redacted]	Strategic Account Managem							
17	amazonwebservices.phi.users@company.com	[redacted]	Amazon Web Services PHI U	Permission within AWS						
		[redacted]	announce.eng							
		[redacted]	Application Platform Team							
		[redacted]	arch.eng							
		[redacted]	Artemis							
		[redacted]	Architects	Architects						
		[redacted]	Auth0 Dev Users	Dev Chiclet within Okta						

Department Map

Group Properties

Assignments
- New hires
- Ongoing

Caveats

- Spreadsheet needs to be maintained:
  - Quarterly review with department leads
  - Adding new systems
  - Quarterly review with Finance to catch rogue systems
- Spreadsheet works but… It is fragile:
  - Can’t have too many cooks editing it.
  - Delete of cells / rows / columns messes everything
  - Department map pivot between sheets is a nightmare!
- This is based on departments – not individual roles
  - Auditors have not complained…

SSO Platform

- We used Okta, but any should work
- “Use SAML” they tell you… 25% of our apps where SAML-integrated…
- Lots of “poor man’s SSO”: script propagating deltas to target apps.
- HR system -> Okta -> everything else

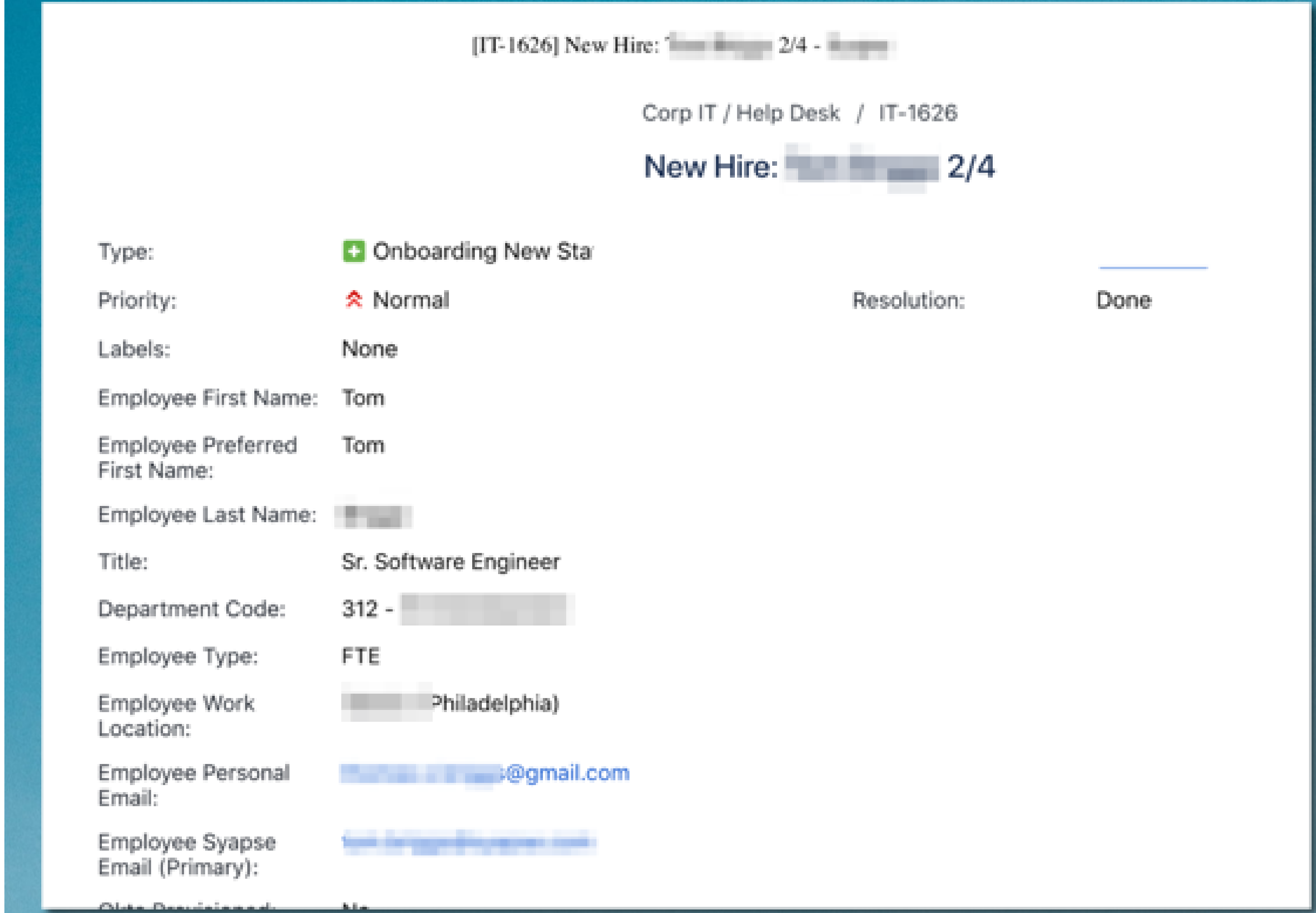
https://sso.tax/

The SSO Wall of Shame

A list of vendors that treat single sign-on as a luxury feature, not a core security requirement.

A solution – Provisioning / Deprovisioning access

Jira tickets - Provisioning



[IT-1626] New Hire: [redacted] 2/4 - [redacted]

Corp IT / Help Desk / IT-1626

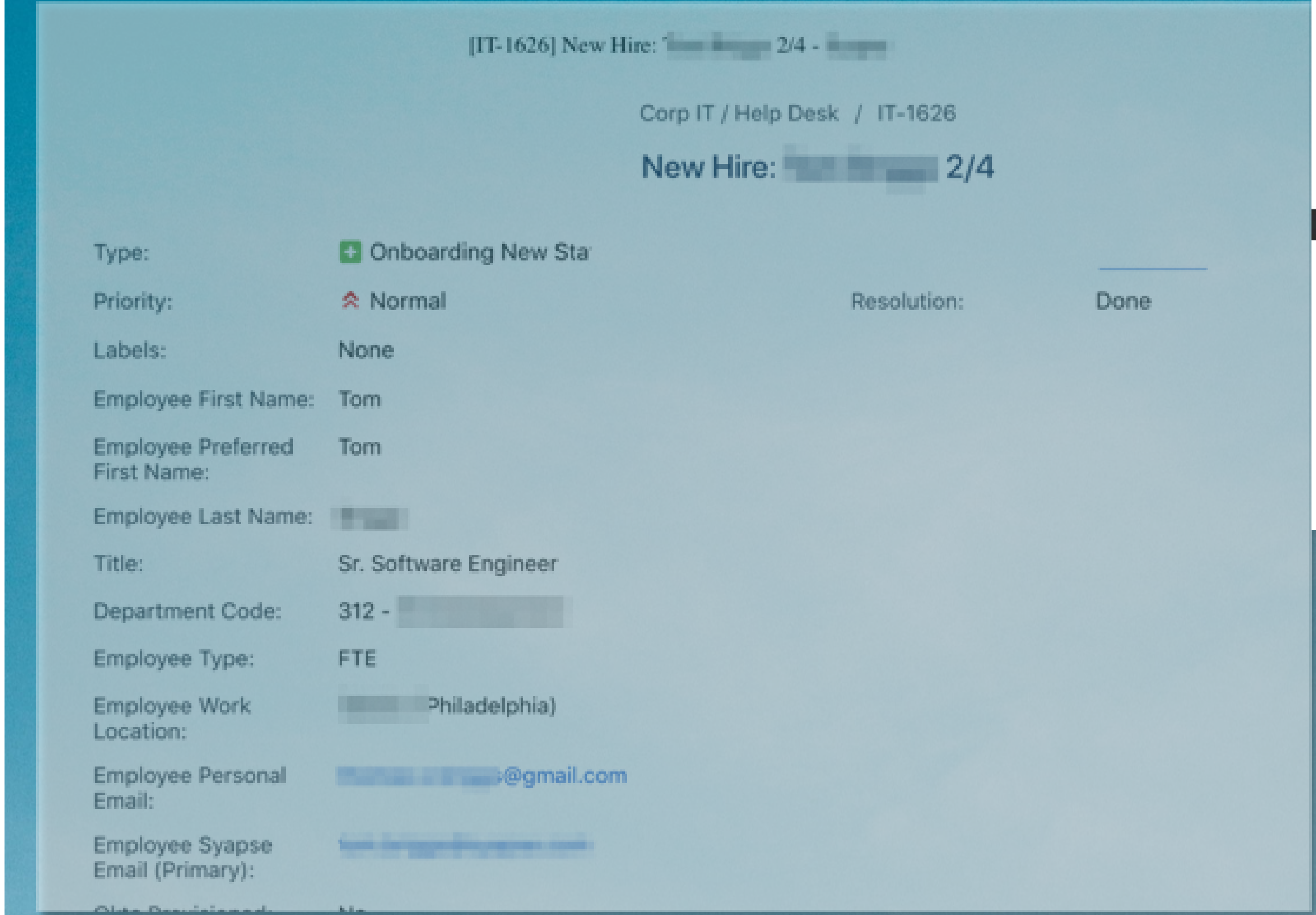
New Hire: [redacted] 2/4

Type:	Onboarding New Sta		
Priority:	Normal	Resolution:	Done
Labels:	None		
Employee First Name:	Tom		
Employee Preferred First Name:	Tom		
Employee Last Name:	[redacted]		
Title:	Sr. Software Engineer		
Department Code:	312 - [redacted]		
Employee Type:	FTE		
Employee Work Location:	[redacted] Philadelphia)		
Employee Personal Email:	[redacted]@gmail.com		
Employee Syapse Email (Primary):	[redacted]		
Okta Provisioned:	No		

New Hire ticket. Contains everything for successful provisioning:

- Start date
- Contact info
- department

Jira tickets - Provisioning

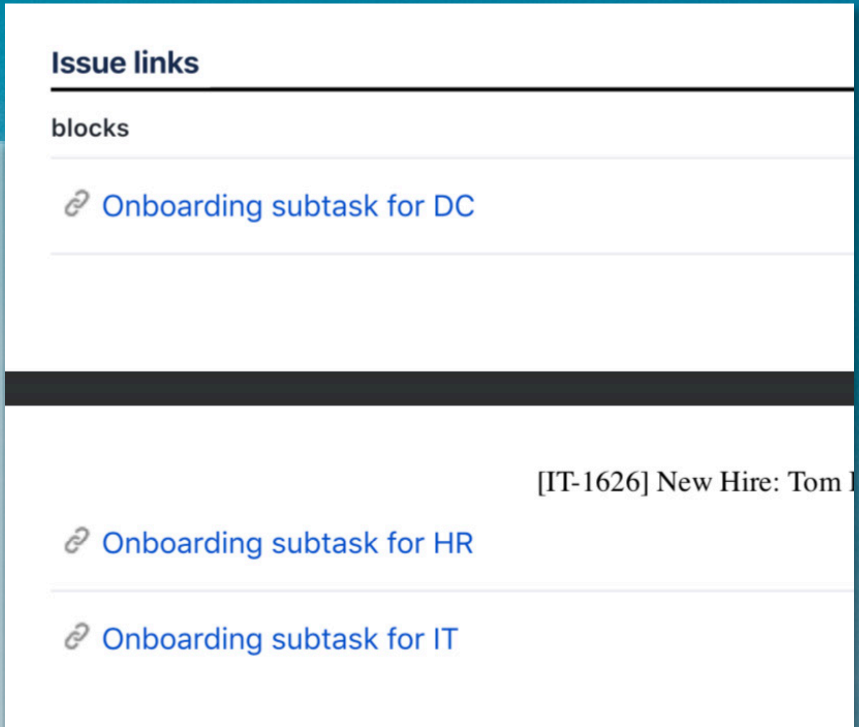


[IT-1626] New Hire: [redacted] 2/4 - [redacted]

Corp IT / Help Desk / IT-1626

New Hire: [redacted] 2/4

Type:	Onboarding New Sta		
Priority:	Normal	Resolution:	Done
Labels:	None		
Employee First Name:	Tom		
Employee Preferred First Name:	Tom		
Employee Last Name:	[redacted]		
Title:	Sr. Software Engineer		
Department Code:	312 - [redacted]		
Employee Type:	FTE		
Employee Work Location:	[redacted] Philadelphia)		
Employee Personal Email:	[redacted]@gmail.com		
Employee Syapse Email (Primary):	[redacted]		
Okta Provisioned:	No		



Issue links

blocks

Onboarding subtask for DC

[IT-1626] New Hire: Tom

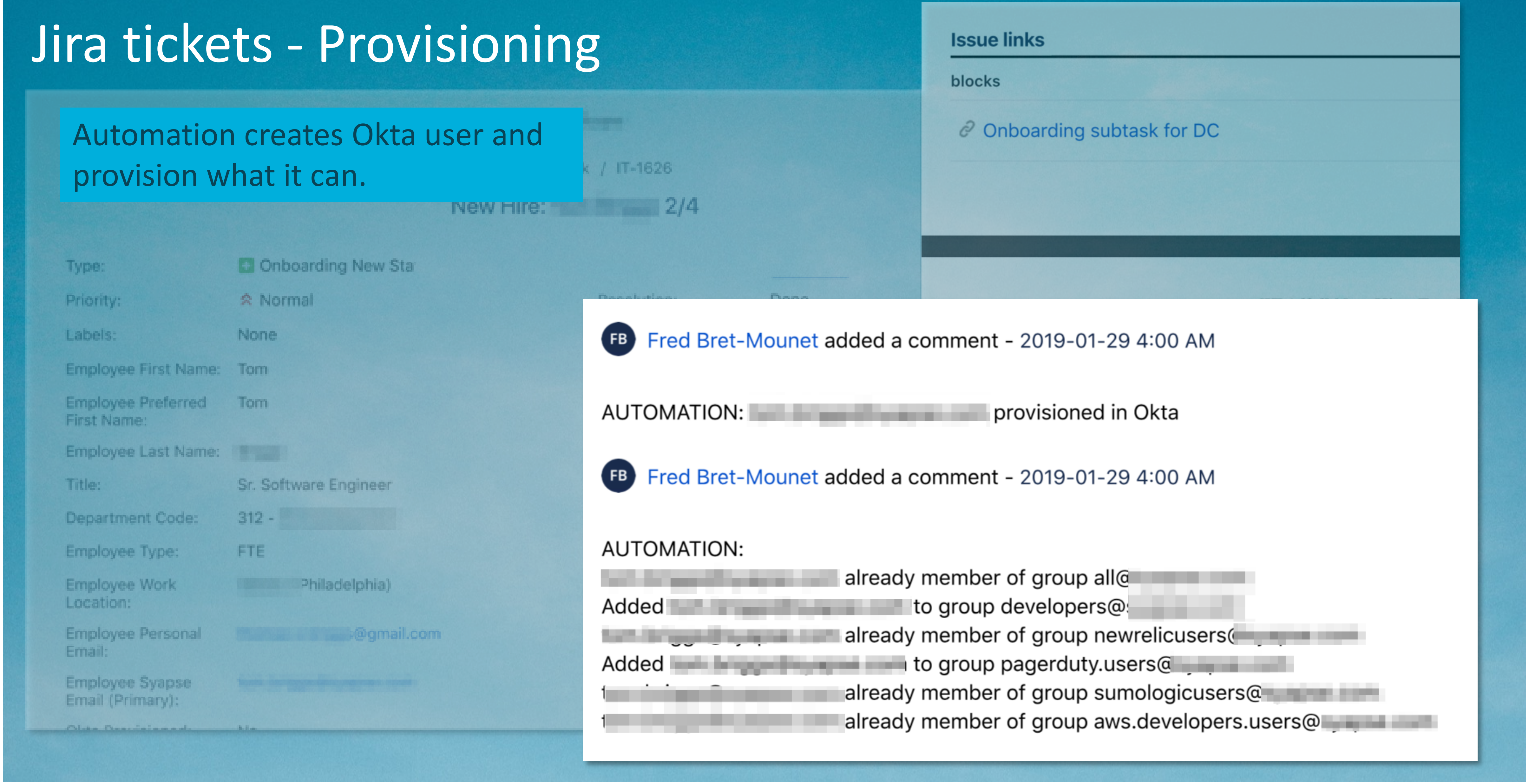
Onboarding subtask for HR

Onboarding subtask for IT

5 days before start day, automation creates subtasks for each department responsible for provisioning.

Jira tickets - Provisioning

Automation creates Okta user and provision what it can.



k / IT-1626

New Hire: [redacted] 2/4

Type:	Onboarding New Sta
Priority:	Normal
Labels:	None
Employee First Name:	Tom
Employee Preferred First Name:	Tom
Employee Last Name:	[redacted]
Title:	Sr. Software Engineer
Department Code:	312 - [redacted]
Employee Type:	FTE
Employee Work Location:	[redacted]Philadelphia)
Employee Personal Email:	[redacted]@gmail.com
Employee Syapse Email (Primary):	[redacted]
Okta Provisioned:	No

Resolution: Done

Issue links

blocks

Onboarding subtask for DC

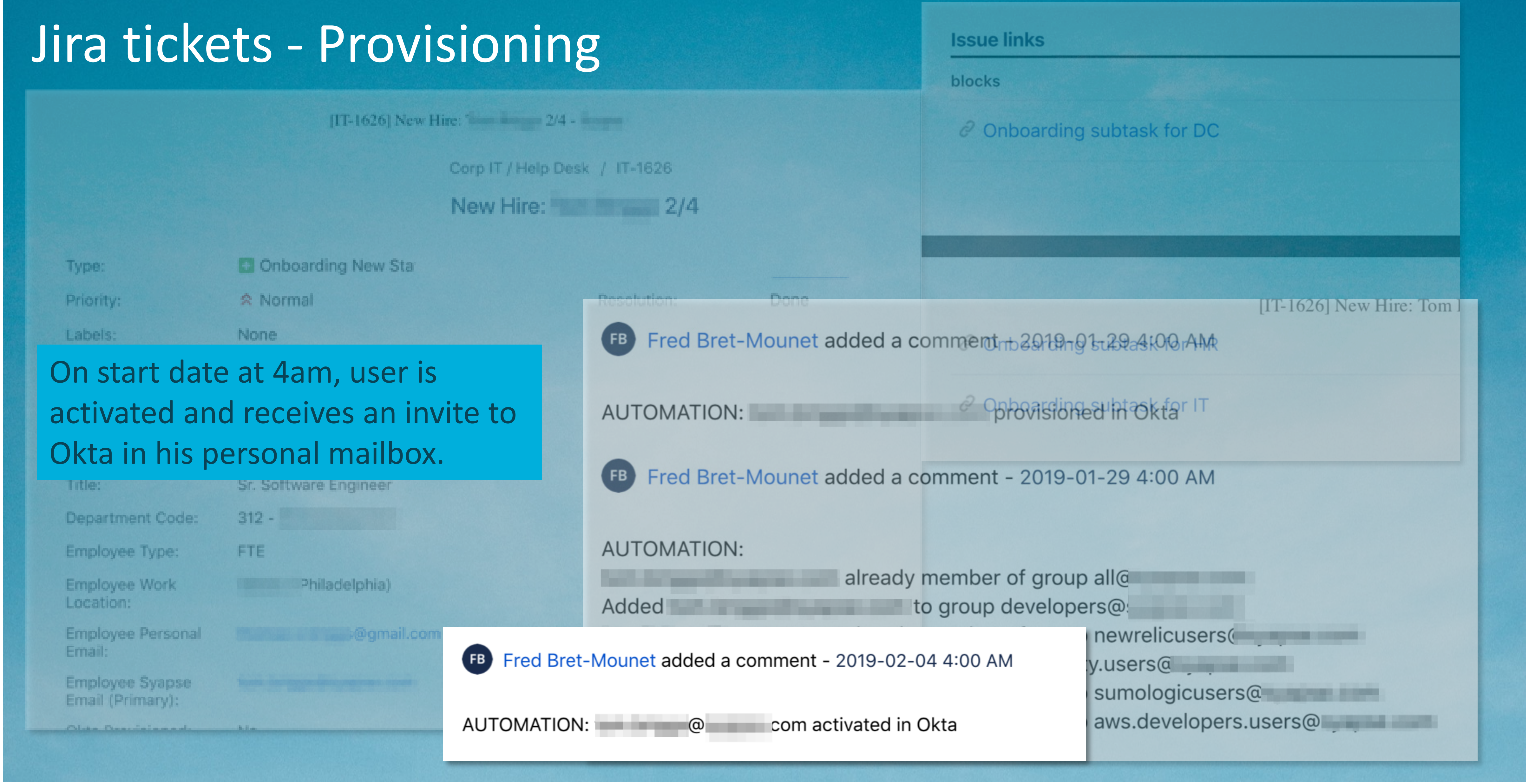
FB Fred Bret-Mounet added a comment - 2019-01-29 4:00 AM

AUTOMATION: [redacted] provisioned in Okta

FB Fred Bret-Mounet added a comment - 2019-01-29 4:00 AM

AUTOMATION:
[redacted] already member of group all@[redacted]
Added [redacted] to group developers@[redacted]
[redacted] already member of group newrelicusers@[redacted]
Added [redacted] to group pagerduty.users@[redacted]
[redacted] already member of group sumologicusers@[redacted]
[redacted] already member of group aws.developers.users@[redacted]

Jira tickets - Provisioning



[IT-1626] New Hire: [redacted] 2/4 - [redacted]

Corp IT / Help Desk / IT-1626

New Hire: [redacted] 2/4

Type:	Onboarding New Sta
Priority:	Normal
Labels:	None
Title:	Sr. Software Engineer
Department Code:	312 - [redacted]
Employee Type:	FTE
Employee Work Location:	[redacted] Philadelphia)
Employee Personal Email:	[redacted]@gmail.com
Employee Syapse Email (Primary):	[redacted]
Okta Provisioned:	No

Resolution: Done

Issue links

blocks

Onboarding subtask for DC

Onboarding subtask for HR

Onboarding subtask for IT

[IT-1626] New Hire: Tom

Fred Bret-Mounet added a comment - 2019-01-29 4:00 AM

AUTOMATION: [redacted] provisioned in Okta

Fred Bret-Mounet added a comment - 2019-01-29 4:00 AM

AUTOMATION:
[redacted] already member of group all@[redacted]
Added [redacted] to group developers@[redacted]
newrelicusers@[redacted]
y.users@[redacted]
sumologicusers@[redacted]
aws.developers.users@[redacted]

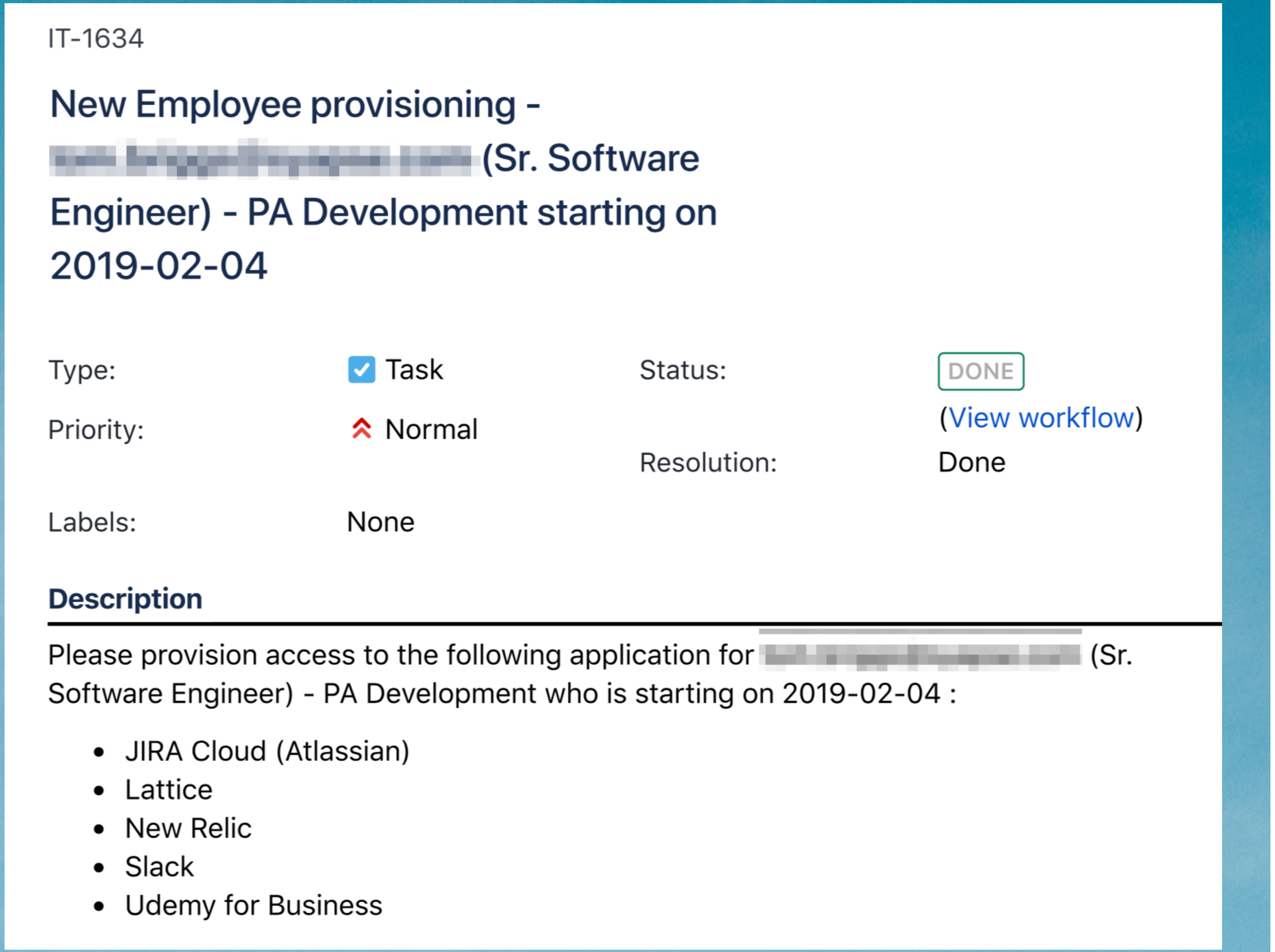
Fred Bret-Mounet added a comment - 2019-02-04 4:00 AM

AUTOMATION: [redacted]@[redacted]com activated in Okta

On start date at 4am, user is activated and receives an invite to Okta in his personal mailbox.

Jira tickets – sub tasks

- Subtasks created based on department mapping
- Clear paper trail



IT-1634

New Employee provisioning - [redacted] (Sr. Software Engineer) - PA Development starting on 2019-02-04

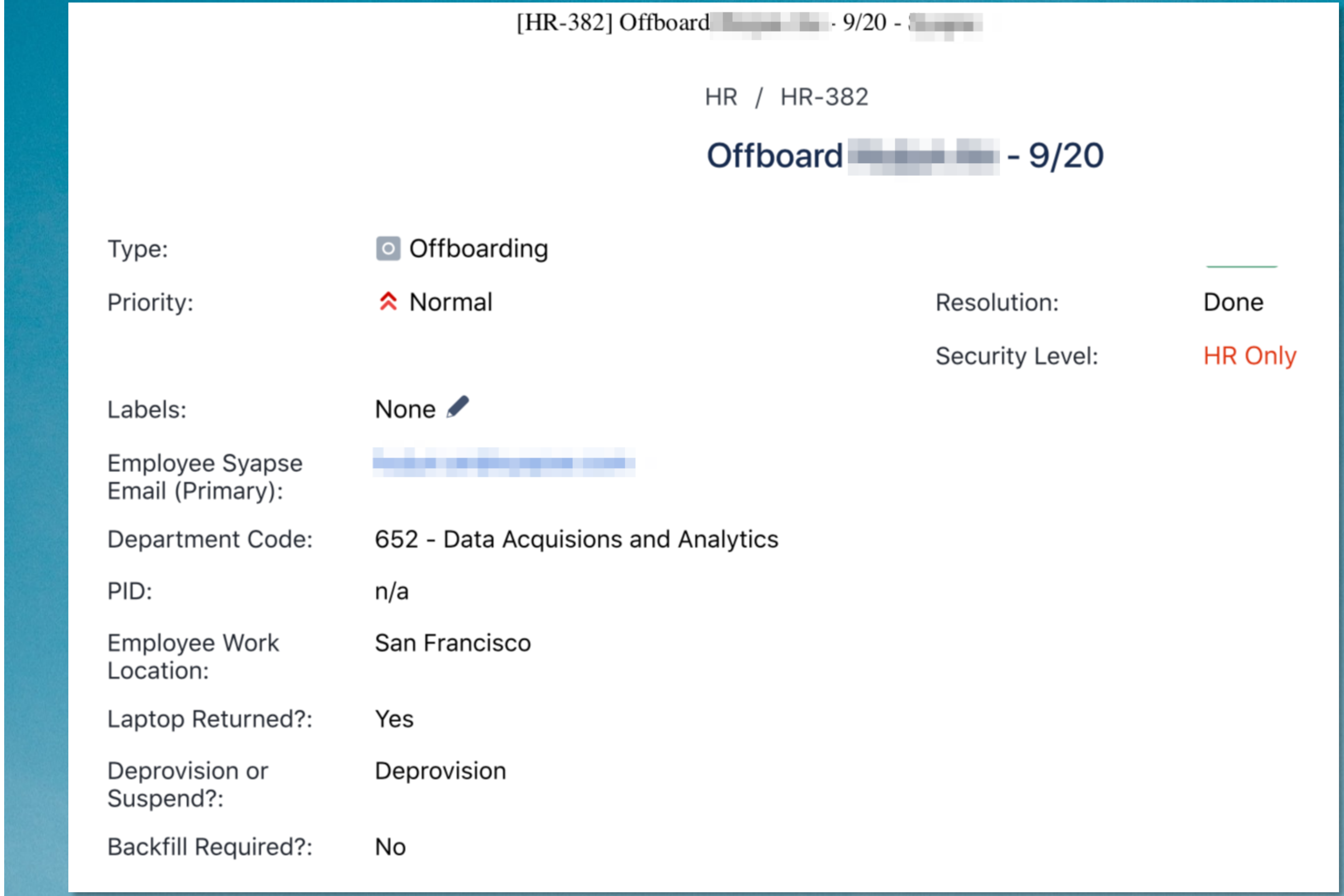
Type:	☑ Task	Status:	DONE (View workflow)
Priority:	Normal	Resolution:	Done
Labels:	None		

Description

Please provision access to the following application for [redacted] (Sr. Software Engineer) - PA Development who is starting on 2019-02-04 :

- JIRA Cloud (Atlassian)
- Lattice
- New Relic
- Slack
- Udemy for Business

Jira tickets – deprovisioning



[HR-382] Offboard [redacted] - 9/20 - [redacted]

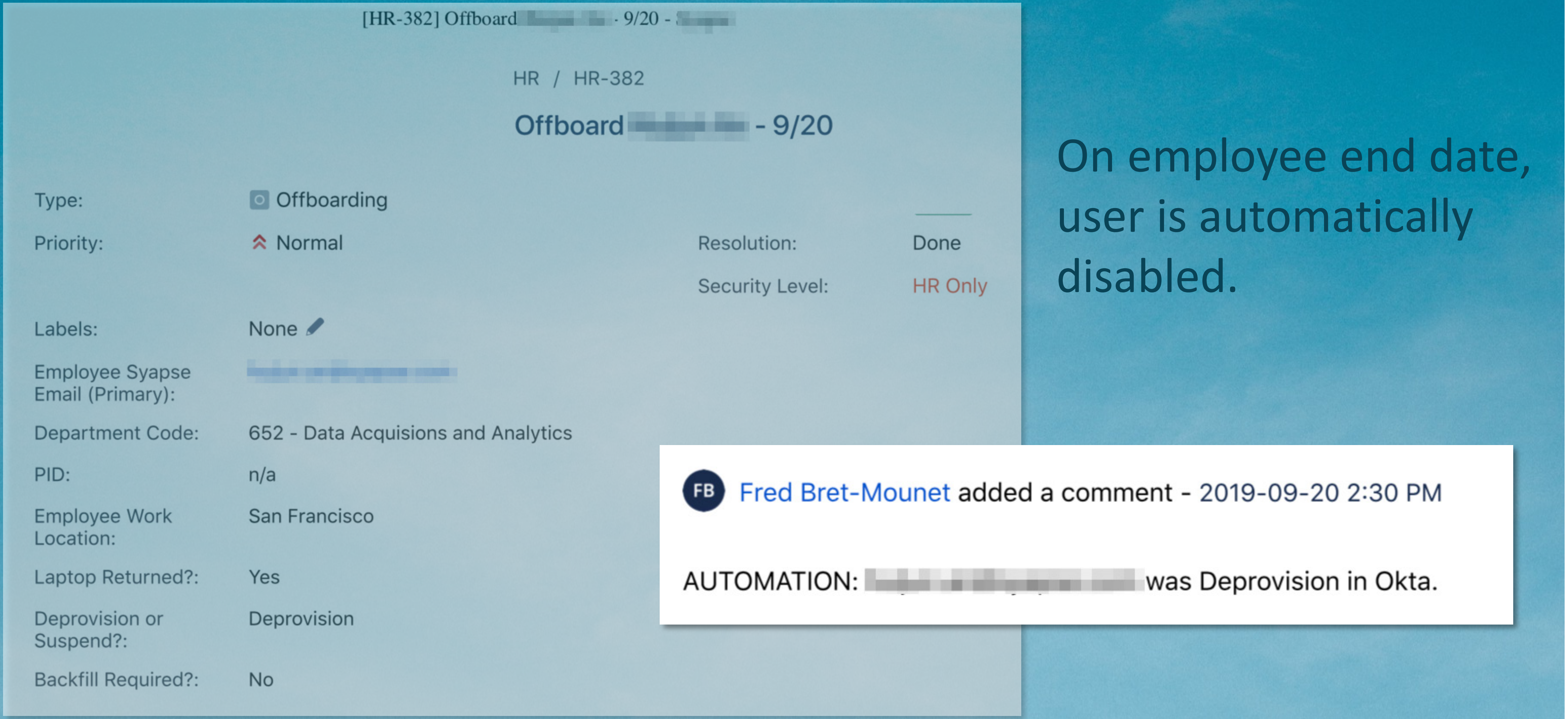
HR / HR-382

Offboard [redacted] - 9/20

Type:	Offboarding		
Priority:	Normal	Resolution:	Done
		Security Level:	HR Only
Labels:	None		
Employee Syapse Email (Primary):	[redacted]		
Department Code:	652 - Data Acquisions and Analytics		
PID:	n/a		
Employee Work Location:	San Francisco		
Laptop Returned?:	Yes		
Deprovision or Suspend?:	Deprovision		
Backfill Required?:	No		

- The reverse!
- Remember to deal with ACLs.

Jira tickets – deprovisioning



[HR-382] Offboard [redacted] - 9/20 - [redacted]

HR / HR-382

Offboard [redacted] - 9/20

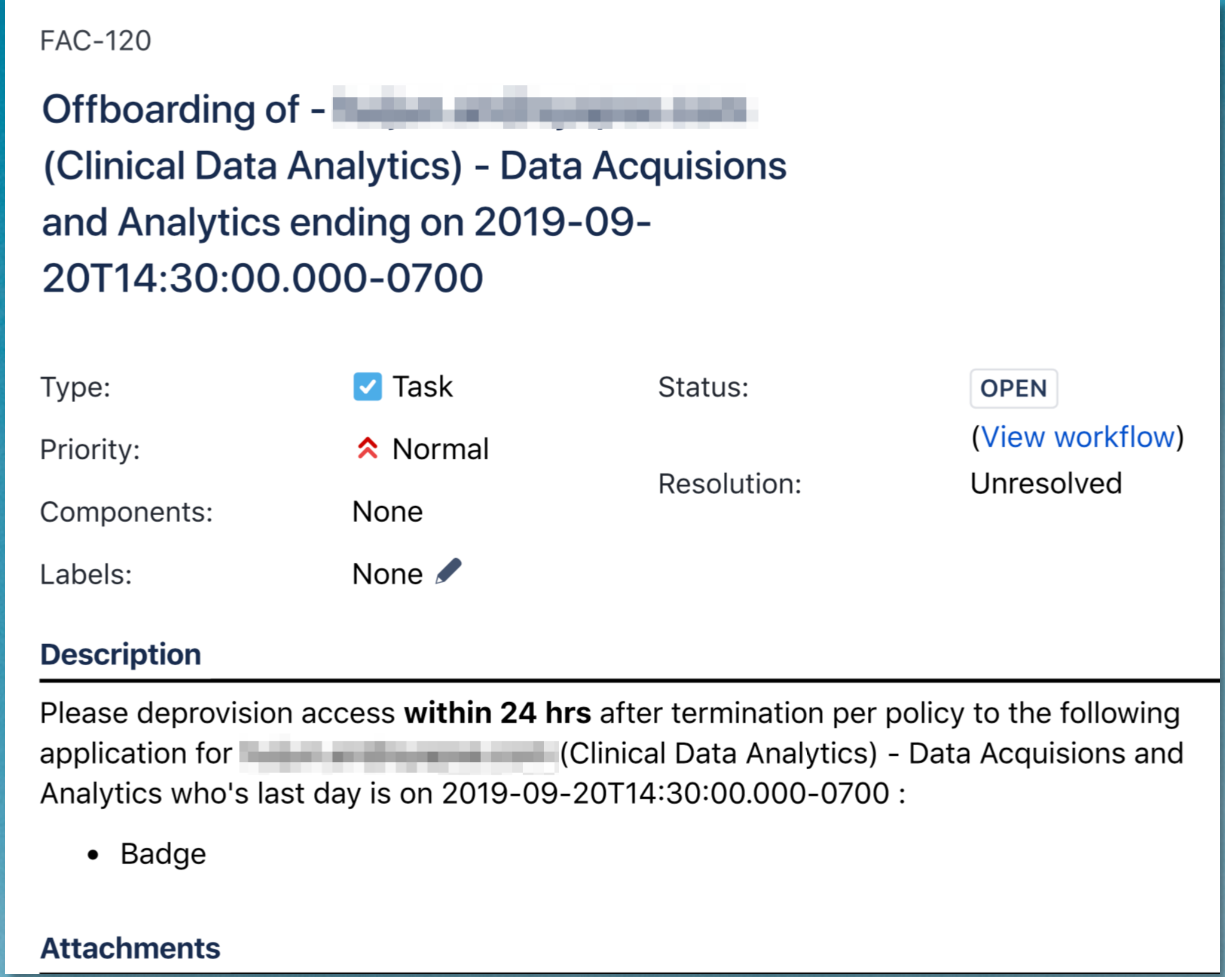
Type:	Offboarding		
Priority:	Normal	Resolution:	Done
		Security Level:	HR Only
Labels:	None		
Employee Syapse Email (Primary):	[redacted]		
Department Code:	652 - Data Acquisions and Analytics		
PID:	n/a		
Employee Work Location:	San Francisco		
Laptop Returned?:	Yes		
Deprovision or Suspend?:	Deprovision		
Backfill Required?:	No		

FB Fred Bret-Mounet added a comment - 2019-09-20 2:30 PM

AUTOMATION: [redacted] was Deprovision in Okta.

On employee end date, user is automatically disabled.

Jira tickets – deprovisioning



FAC-120

Offboarding of - [redacted] (Clinical Data Analytics) - Data Acquisions and Analytics ending on 2019-09-20T14:30:00.000-0700

Type:	☑ Task	Status:	OPEN (View workflow)
Priority:	Normal	Resolution:	Unresolved
Components:	None		
Labels:	None		

Description

Please deprovision access **within 24 hrs** after termination per policy to the following application for [redacted] (Clinical Data Analytics) - Data Acquisions and Analytics who's last day is on 2019-09-20T14:30:00.000-0700 :

- Badge

Attachments

- Similar subtasks
- Some systems need manual processing
- While HR ticket can be created weeks in advance, subtasks are only generated 24 hrs before the event.

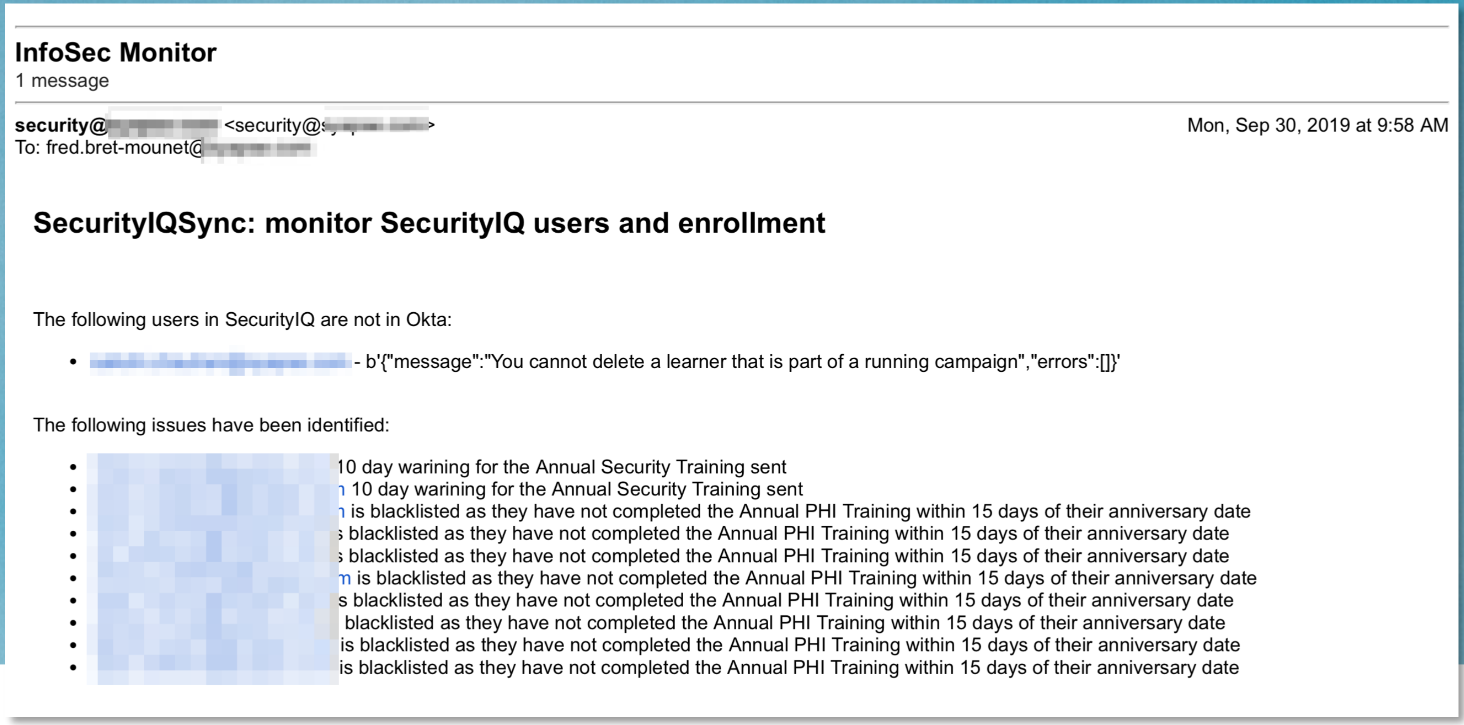
A solution – Training

New way of thinking

- Remove the resistance:
  - A Q4 training that shuts the business down for a few hours is not Agile!
- Anniversary-based training
- Don’t be a cop - Embrace acceptable risk: disable access if training is not taken in a timely manner.
  - 30 days window for InfoSec training
  - 15 days for PHI handling.

New way of thinking

- This can only work with automation!
  - Department Role map knows what apps have PHI
  - Okta has anniversaries and employee access inventory
- Bonus: “Sorry, I can’t give you a pass… automation will override!”



InfoSec Monitor
1 message

security@[redacted] <security@[redacted]> Mon, Sep 30, 2019 at 9:58 AM
To: fred.bret-mounet@[redacted]

SecurityIQSync: monitor SecurityIQ users and enrollment

The following users in SecurityIQ are not in Okta:

- [redacted] - b'{"message":"You cannot delete a learner that is part of a running campaign","errors":[]}'

The following issues have been identified:

- [redacted] 10 day warining for the Annual Security Training sent
- [redacted] 10 day warining for the Annual Security Training sent
- [redacted] is blacklisted as they have not completed the Annual PHI Training within 15 days of their anniversary date
- [redacted] blacklisted as they have not completed the Annual PHI Training within 15 days of their anniversary date
- [redacted] blacklisted as they have not completed the Annual PHI Training within 15 days of their anniversary date
- [redacted] is blacklisted as they have not completed the Annual PHI Training within 15 days of their anniversary date
- [redacted] blacklisted as they have not completed the Annual PHI Training within 15 days of their anniversary date
- [redacted] blacklisted as they have not completed the Annual PHI Training within 15 days of their anniversary date
- [redacted] is blacklisted as they have not completed the Annual PHI Training within 15 days of their anniversary date
- [redacted] is blacklisted as they have not completed the Annual PHI Training within 15 days of their anniversary date

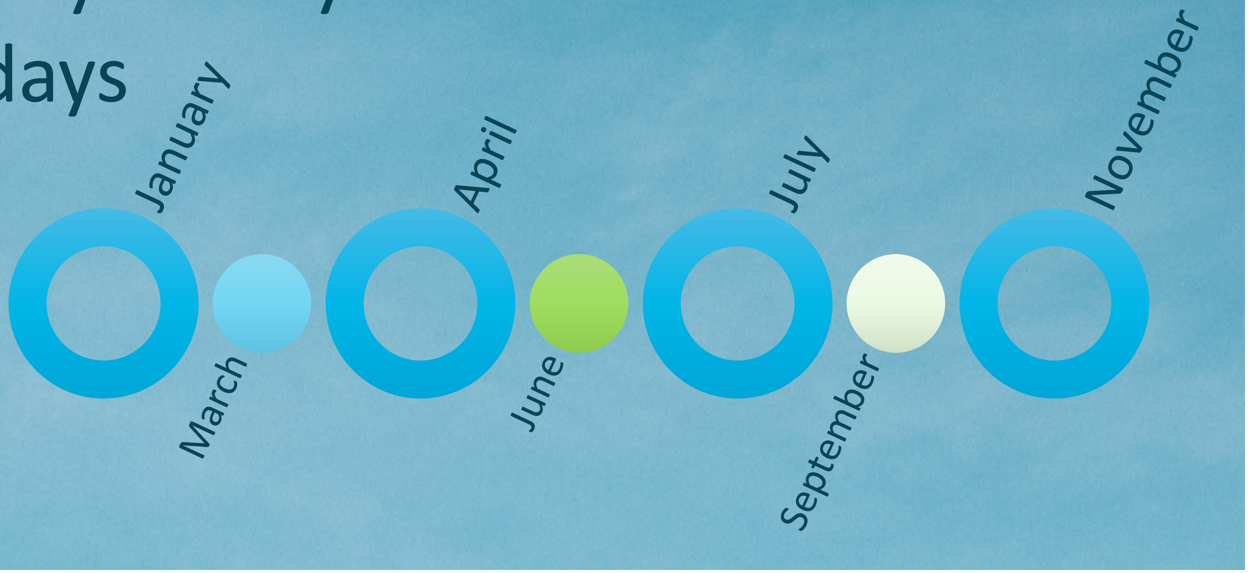
A solution – Crowdsourcing access reviews

The old way

- InfoSec / Compliance resource guesses what access every employee should individually have…
- 5-10 min / employee = 1 FTE week of effort
- HITRUST requires a review every 60 days

The new way

- Crowdsource review to managers!
  - Okta understands the hierarchy
  - Okta understands the systems one has access to
- For HITRUST:
  - Privileged access review every 60 days
  - All access review every 90 days

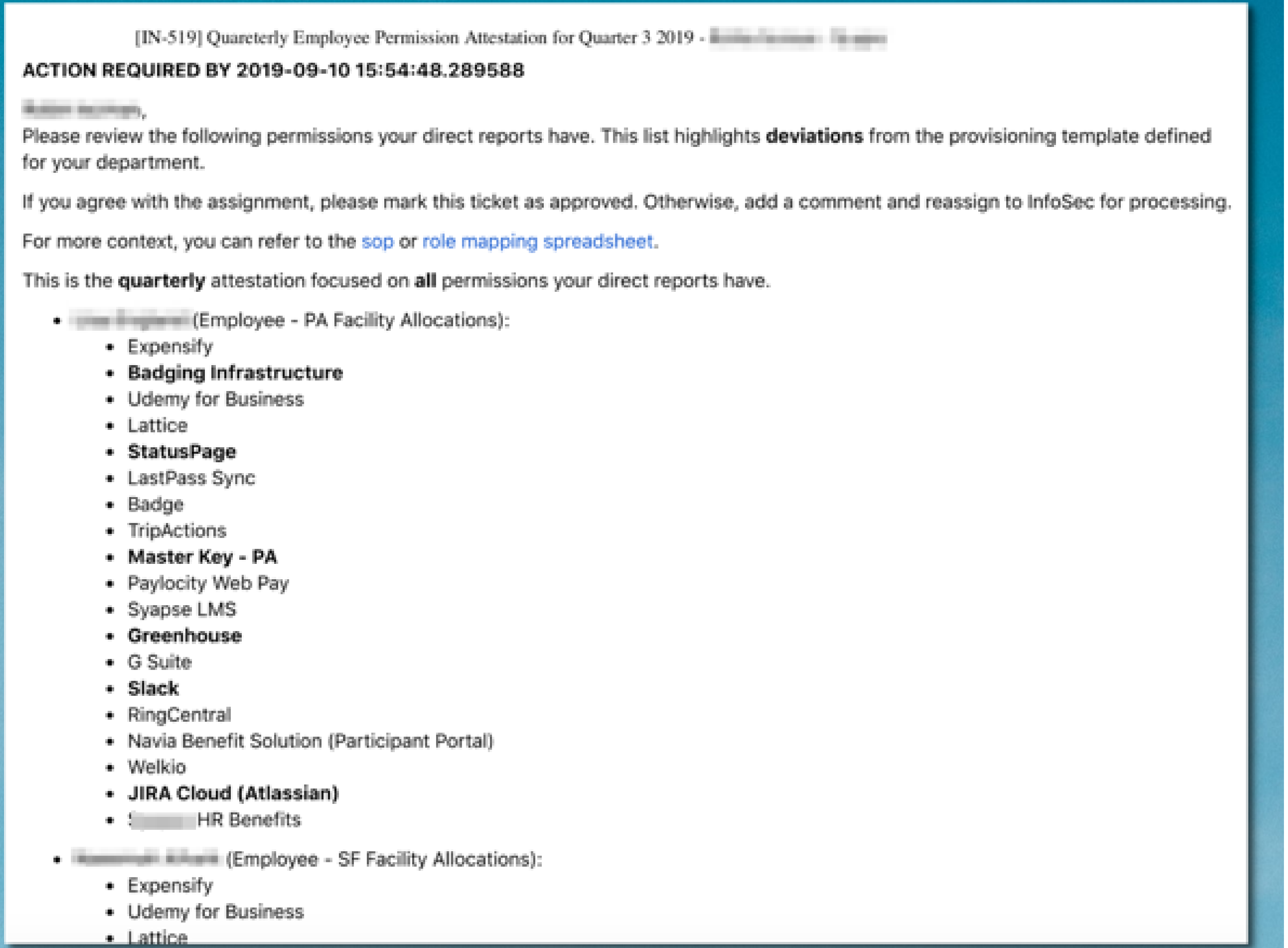


Jira tickets

The Why and How

For each direct report:

- List of systems
- How their access differs from baseline for that department



[IN-519] Quareterly Employee Permission Attestation for Quarter 3 2019 - [redacted]

ACTION REQUIRED BY 2019-09-10 15:54:48.289588

[redacted],

Please review the following permissions your direct reports have. This list highlights **deviations** from the provisioning template defined for your department.

If you agree with the assignment, please mark this ticket as approved. Otherwise, add a comment and reassign to InfoSec for processing.

For more context, you can refer to the sop or role mapping spreadsheet.

This is the **quarterly** attestation focused on **all** permissions your direct reports have.

- [redacted] (Employee - PA Facility Allocations):
  - Expensify
  - **Badging Infrastructure**
  - Udemy for Business
  - Lattice
  - **StatusPage**
  - LastPass Sync
  - Badge
  - TripActions
  - **Master Key - PA**
  - Paylocity Web Pay
  - Syapse LMS
  - **Greenhouse**
  - G Suite
  - **Slack**
  - RingCentral
  - Navia Benefit Solution (Participant Portal)
  - Welkio
  - **JIRA Cloud (Atlassian)**
  - [redacted] HR Benefits
- [redacted] (Employee - SF Facility Allocations):
  - Expensify
  - Udemy for Business
  - Lattice

Outcome

- Only works with automation!
  - Same amount of collective work. 30 minutes of InfoSec work to babysit the tickets.
- The lesser of 2 evils: InfoSec doesn’t understand individual roles vs managers may not take the task seriously…
  - Remind them of the paper trail they are leaving
  - Spot check a few tickets

Call to action

Call to action

- I / We need an open source platform!
  - Is there anything to build on?
  - Coders in the audience want to jump in?
- I spent 10% of my time building, maintaining and monitoring
  - This should go down with a community-driven solution…

Parting thoughts

- Use the tools your audience uses. In my case that was Jira.
- Practice good software engineering practices.
  - This also helps your street creds with the dev groups.
- Invest in automation skills on your infosec team.
  - I’ve had a really hard time transitioning my baby ☹
  - You can only scale through automation, so do it!
  - Agile and CICD are faster than your click!

Questions?

fred@clarifyhealth.com