

# Don't Be Scared...of Licence Audits: A Tale of Two Audits

Barry Pilling, Managing Partner, Cortex Consulting

# Setting the Scene

IBM – UK financial services client

July 2015 – January 2016

Attachmate – UK retail client

July 2014 – January 2015



The audit letter arrives

# Typical IBM Audit Letter

*Dear Mr / Mrs / Ms / Miss ...*

**Ref:** *Selection for IBM Software License Compliance Review*

*Your organisation and its Enterprise (as defined in the applicable license agreement) has been selected for a Software License Review (“SLR”).*

*The next paragraph will try to get you to identify an executive sponsor for the review and commit to a kick off meeting / call in a specific week.*

*These reviews are performed in line with Section 11 “Compliance Verification” of IBM’s International Program Licensing Agreement (IPLA).*

*Towards the end of the letter you will generally get an offer to resolve any licence discrepancies before the audit commences.*

# The Audit Timeline



IT Asset Management  
C-Suite  
Procurement  
Commercial  
Legal  
IT Security  
Service Delivery  
Service Management  
Application Management

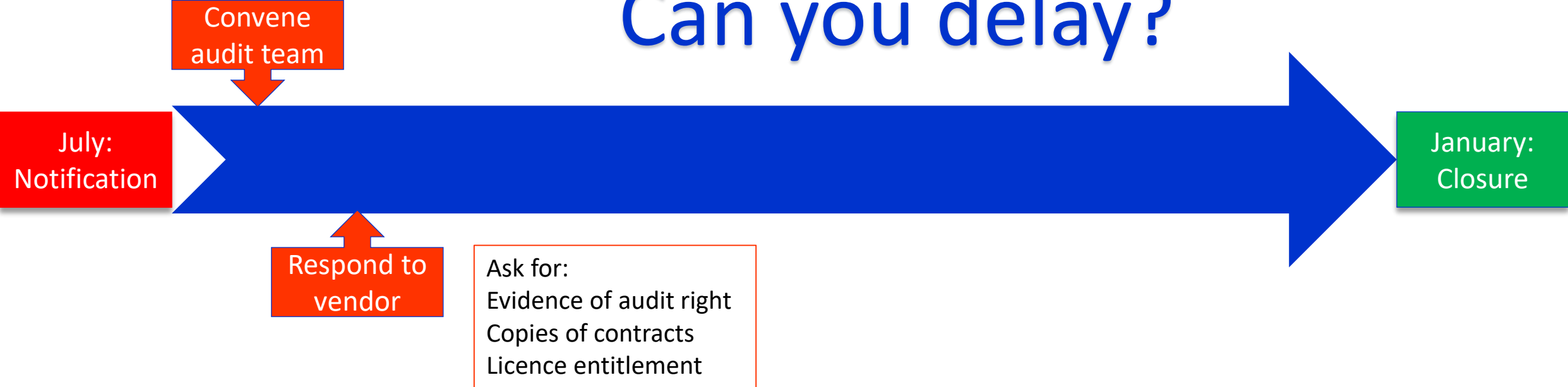
Discuss:  
Right to audit  
Scope of audit

- Business unit(s)
- Contracts
- Products

Audit strategy  
3<sup>rd</sup> party support?

# The Audit Timeline

## Can you delay?



# Initial Steps...

Can you please send me the relevant contracts to prove your audit right?



They'll be archived by now. We haven't used the software in years.

Possibly but I don't have the contracts to hand, so I'm going to need you to prove it to me.

Yep, I totally get where you're coming from. I'm just asking for you to prove your right.



We supplied them when you bought the licences so you should have them already.

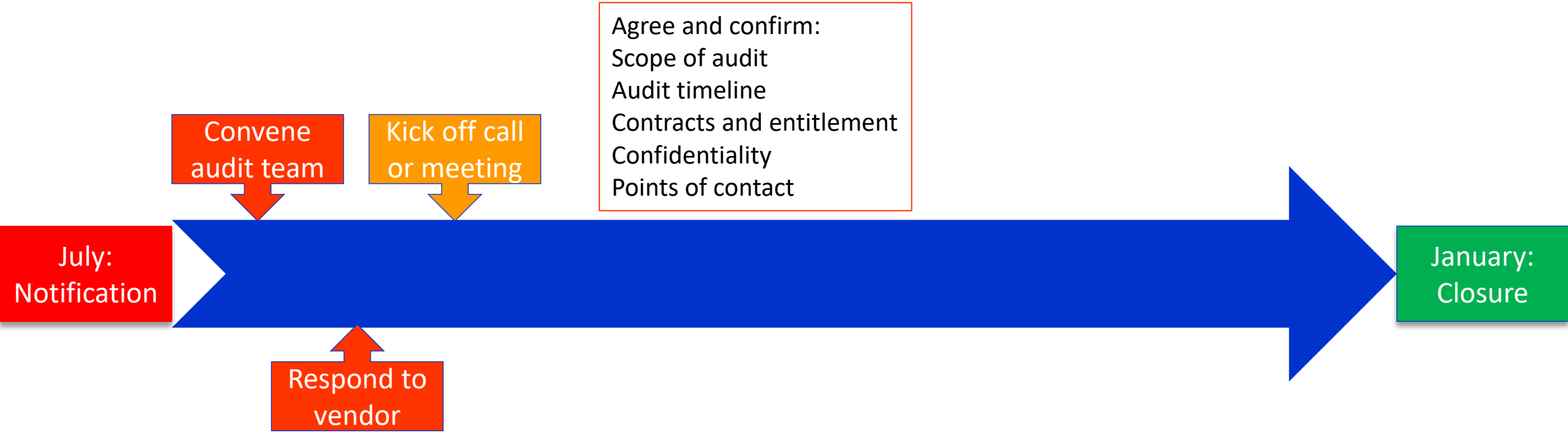
That's not our problem. We have a right to audit regardless of your usage.

A licence gives you the right to use the software in a FAIR way, we just want to check you are.

OK fine. I've attached our standard EULA, you'll see the audit right under "Verification".



# The Audit Timeline



“minimize disruption to your business”

# Is That the Right EULA?

Hold on...that EULA version is dated 2006. We last bought licences in 2002.

Well that's our standard EULA. You can clearly see the right to audit.



Any chance you can send me a EULA that actually applies to the licences we bought?

But our audit clause hasn't changed, it will say the same thing!

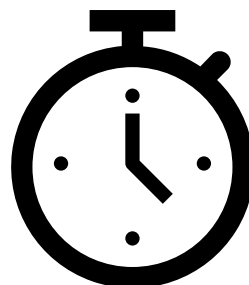
I'm sure it will but I'd still like to see it. Oh, can you send the entitlement over too please?

You want the licence entitlement too?!? Don't you have that either?



Of course we do but I want to be sure that you're auditing the correct licences.

Right. I've attached the 4 contracts that apply plus your entitlement.



4 weeks later



# A Closer Look at the IPLA Audit Clause

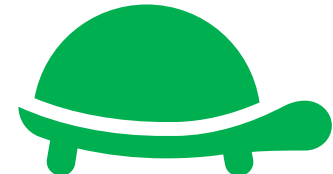
Licensee agrees to create, retain, and provide to IBM and its auditors accurate written records, system tool outputs, and other system information sufficient to provide auditable verification that Licensee's use of all Programs is in compliance with the IPLA Program Terms, including, without limitation, all of IBM's applicable licensing and pricing qualification terms. Licensee is responsible for 1) ensuring that it does not exceed its Authorized Use, and 2) remaining in compliance with IPLA Program Terms.

Upon reasonable notice, IBM may verify Licensee's compliance with IPLA Program Terms at all sites and for all environments in which Licensee uses (for any purpose) Programs subject to IPLA Program Terms. Such verification will be conducted in a manner that minimizes disruption to Licensee's business, and may be conducted on Licensee's premises, during normal business hours. IBM may use an independent auditor to assist with such verification, provided IBM has a written confidentiality agreement in place with such auditor.

# The Audit Timeline

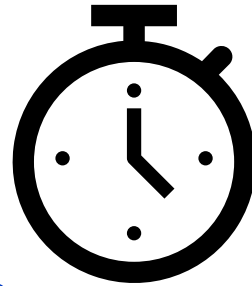


Lawyers work slowly



# Agreeing the NDA

Hang on...we've got to sort out the non-disclosure agreement first



8 weeks later

Can we proceed with the audit now please?



Yeah but our lawyers aren't happy with it. It's really out of my hands, sorry.

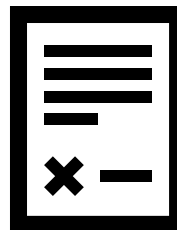
But our contracts contain a confidentiality clause about handling of data.



Very nice. We're going to be using our standard non-disclosure agreement.

OK, I've attached a copy of our standard non-disclosure agreement.

If you want our data, it has to be our NDA. The lawyers insist, sorry.



Agreed NDA

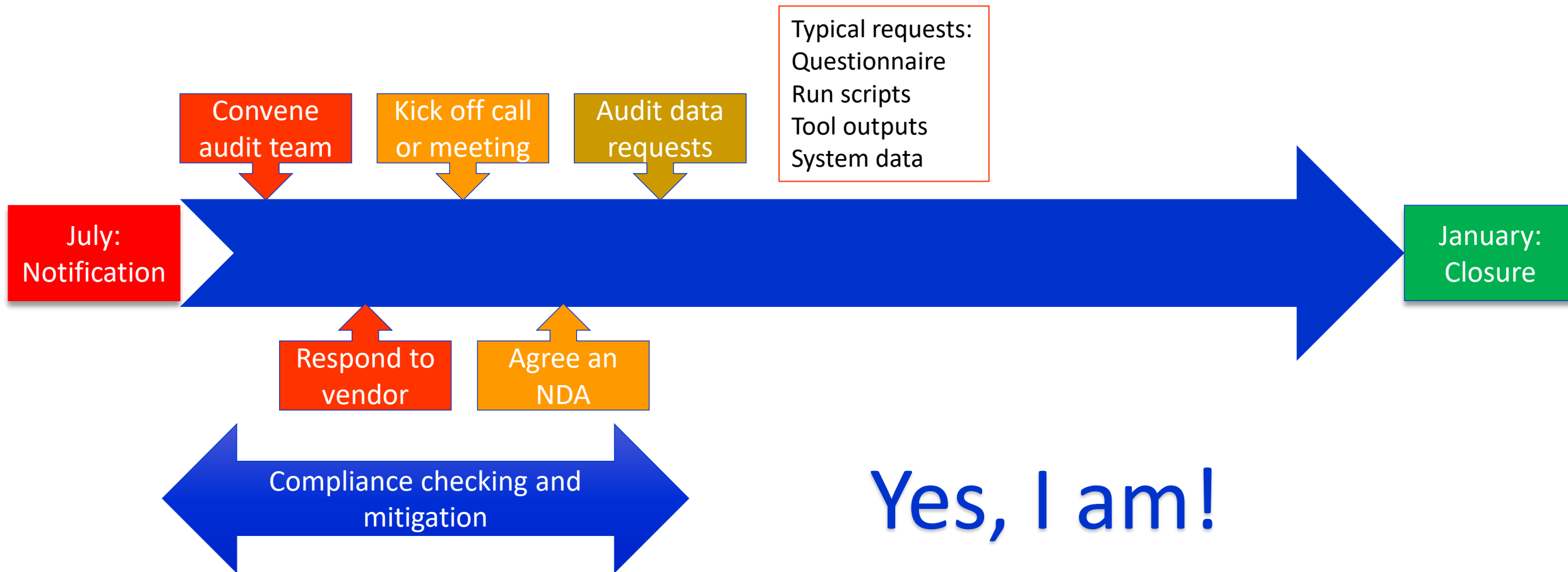
Ours is fine, surely?

# The Non-Disclosure Agreement



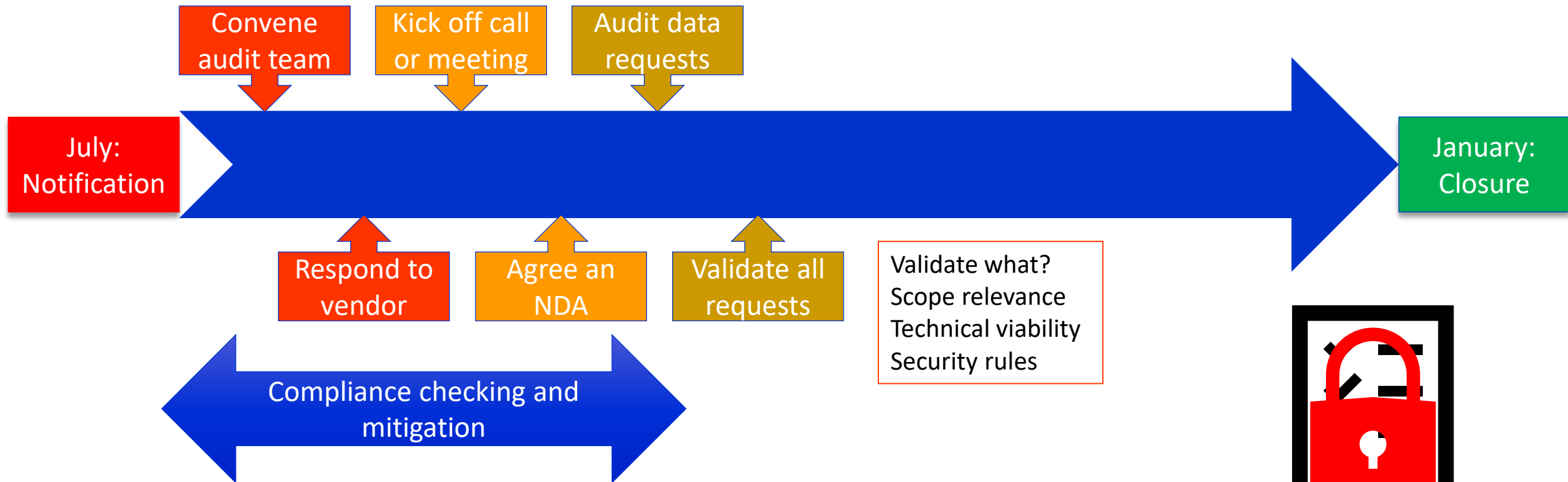
- Use your own NDA
  - Make sure your lawyers have all the definitions locked down tight
  - Do not allow the auditor to drive who gets to see data within their organisation
- “Representative”
  - *Its principals, members, directors, partners, officers and employees that need to know the Confidential Information for the Purpose*
  - *Its professional advisers or consultants who are engaged to advise that Party and / or any member of its Group in connection with the Purpose*
  - *Its contractors or sub-contractors engaged by that Party and / or any member of its Group in connection with the Purpose*
- “Group”
  - *In relation to **the Auditor** it shall include any **Auditor** Entity, irrespective of whether such Entity is controlled by, controlling, or under common control with **Auditor***
  - *Any entity (including **Auditor**) that is a member of the **Auditor** worldwide network and the affiliates and subsidiaries of each such entity*

# The Audit Timeline



# The Audit Timeline

## Use security to your advantage



# Data Requests

Oh sorry. It's December 2<sup>nd</sup>,  
we're in Christmas change  
freeze now.

Run these scripts and submit  
the data output to me.

If it was up to me, we'd do it  
now but the change manager  
has forbidden it.

They only interrogate your  
SCCM and AD databases.



## Decompiling the scripts

# IBM Audit Requests We Refused

- Scoping Questionnaire

- *“What is the purchase and deployment strategy for your Windows servers?”*
- *“Describe the organisation’s user password reset policy.”*
- *“What line of business applications is WebSphere MQ supporting?”*

**“We do not consider this request relevant to the audit”**

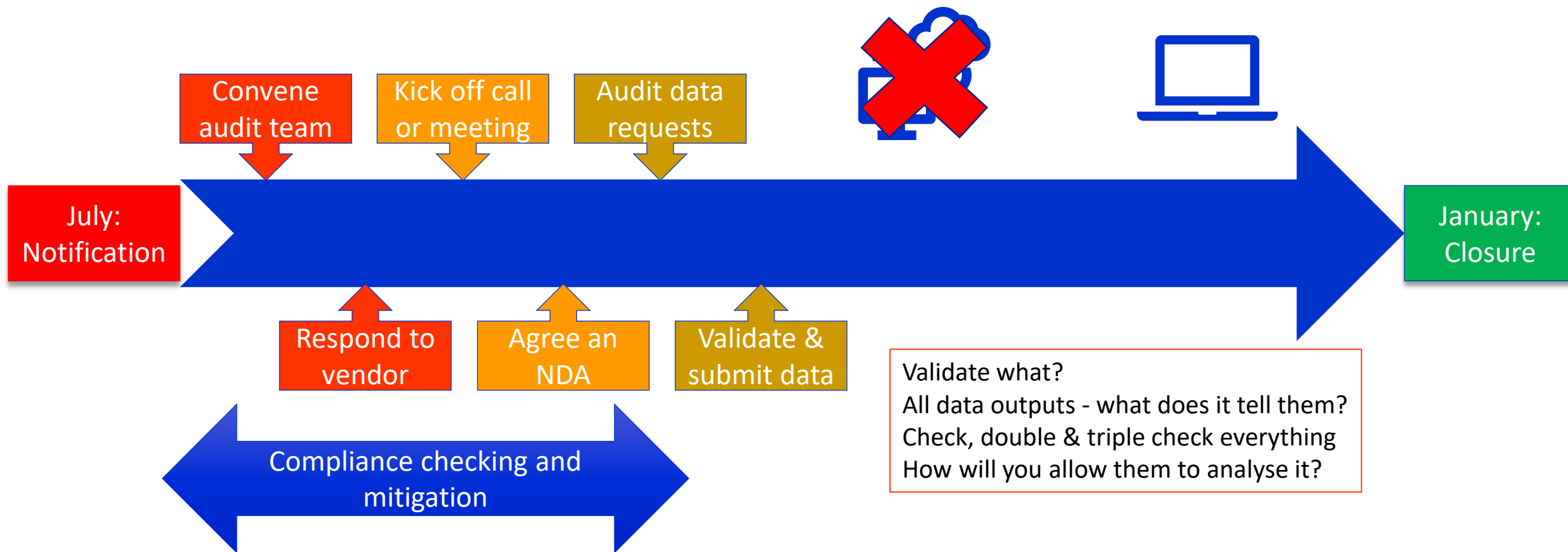
- Data Requests

- *“Please run the **Auditor** inventory tool across your complete environment and provide the resulting outputs.”*
- *“If you are virtualizing using VMware software, please run the **Auditor** Power CLI tool and script.”*

**“We do not run 3<sup>rd</sup> party scripts in our IT environments”**

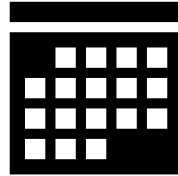


# The Audit Timeline



# Gathering Data

Sure. I'm organising it now, it'll be done next week for you.



Jan 2<sup>nd</sup> 2015

Can you run the scripts now?



The change record has to go through its approval process.

Why next week?  
Why not today?

Because you're asking us to run scripts against production databases.

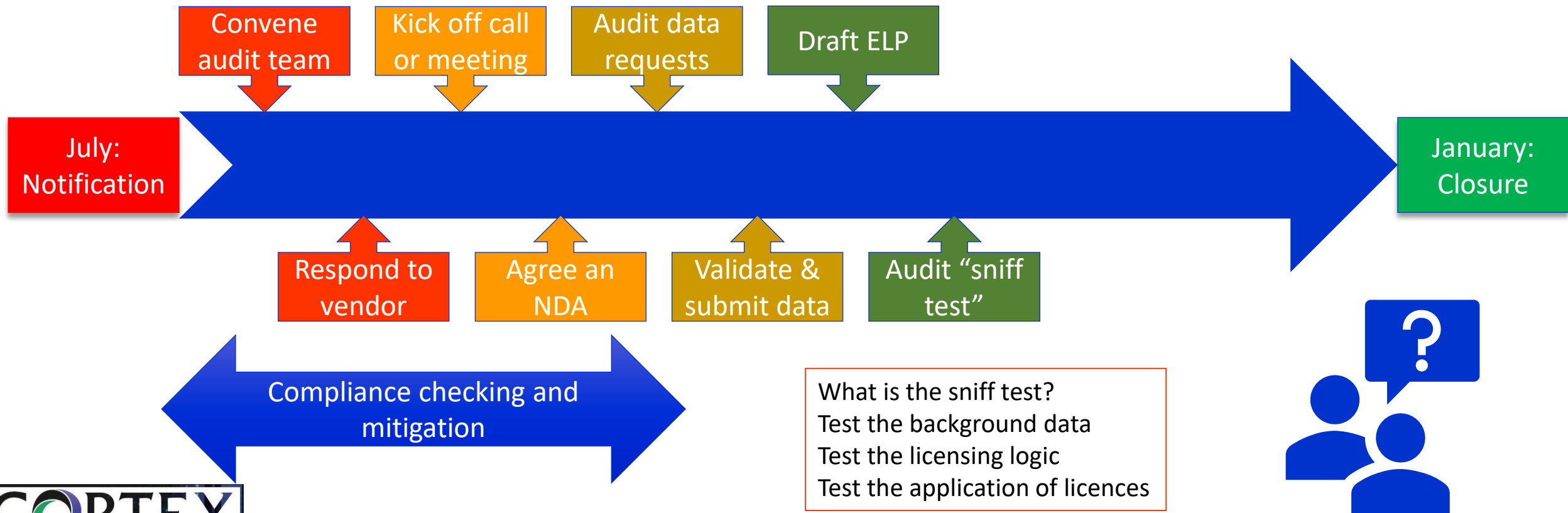
Why does it have to go through change control?



## Checking the output

Fine. Send us the output as soon as you have it.

# The Audit Timeline

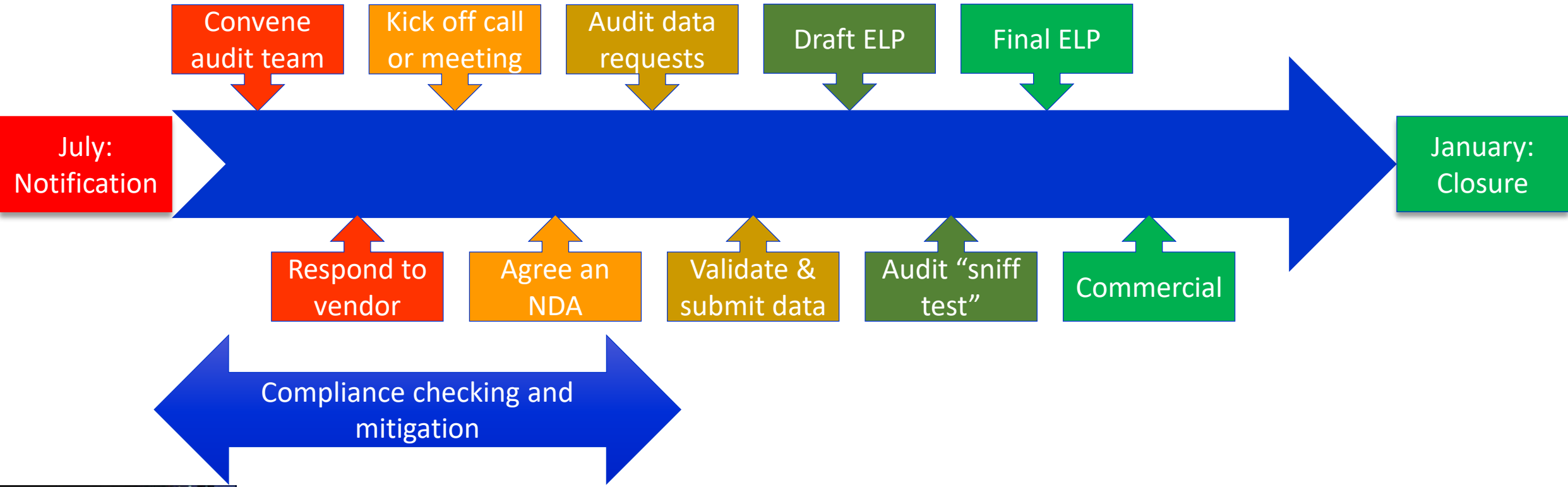


# IBM Issues We Found



- Risk Management
  - Should be minimal non-compliance
  - 2 x PVU licensed products non-compliance = c£185k
  - Removed £3.8m of risk pre-data submission...
  - ...but some audits yield surprising results
- Bonus Auditor Findings
  - Sterling B2B Integrator
    - Licensed on PVUs and Connections
    - Auditor claimed 613 connection licences shortfall = c£125k
  - Tealeaf CX and cxReveal
    - Licensed on Authorised Users and RVUs (MMI)
    - Auditor claimed 31 user licences shortfall = c£190k
  - Cognos Disclosure Management Administrator
    - Licensed on Authorised Users
    - Auditor claimed 13 licences shortfall

# The Audit Timeline



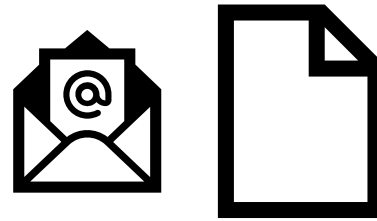
# Have a Negotiation Plan...Early



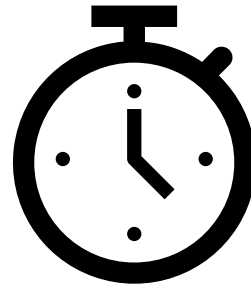
- What's your plan?
  - What does the vendor want?
  - What do you want?
  - Where is the compromise?
  - What can you leverage?
- What can you use?
  - How was the audit process conducted?
  - Has there been any lack of openness?
  - Has the vendor done anything to contribute to your compliance issues?
  - Is the vendor keen to sell you something you're thinking about anyway?
- Be firm but try to avoid aggressive positions

# End Result

Please see attached the script output. Let me know when you've completed your ELP.



At last! We'll be in touch.



2 weeks later



We did try and tell you that last March but you insisted on auditing.

Erm...we're going to cancel the audit. You don't appear to be using our software.

# Questions or Comments?





# Thank You for Coming

[barry.pilling@cortexconsulting.co.uk](mailto:barry.pilling@cortexconsulting.co.uk)

[@Baron ITAM](#)

[www.linkedin.com/in/barrypilling](http://www.linkedin.com/in/barrypilling)

[www.cortexconsulting.co.uk](http://www.cortexconsulting.co.uk)

[@cortexllp](#)

[www.linkedin.com/company/cortex-consulting-llp-uk](http://www.linkedin.com/company/cortex-consulting-llp-uk)