

YOUR  
LOGO  
HERE

# eftsure inside Dynamics 365 FO

## Kickoff meeting

eftsure

# KICKOFF AGENDA

Introduction (15min)

- meet your new team
- what's the background?
- why are we doing this?

Project (45min)

- what are we doing?
- who is doing what?
- how are we going to work together?

Role (10min)

- Ownership

Q&A

YOUR  
LOGO  
HERE

## eftsure Team

Kim Lalor

Customer Success Manager

[kiml@eftsure.com.au](mailto:kiml@eftsure.com.au)

Greg Peignoux

D365 Product Manager

[gregp@eftsure.com.au](mailto:gregp@eftsure.com.au)

Berengere Villey

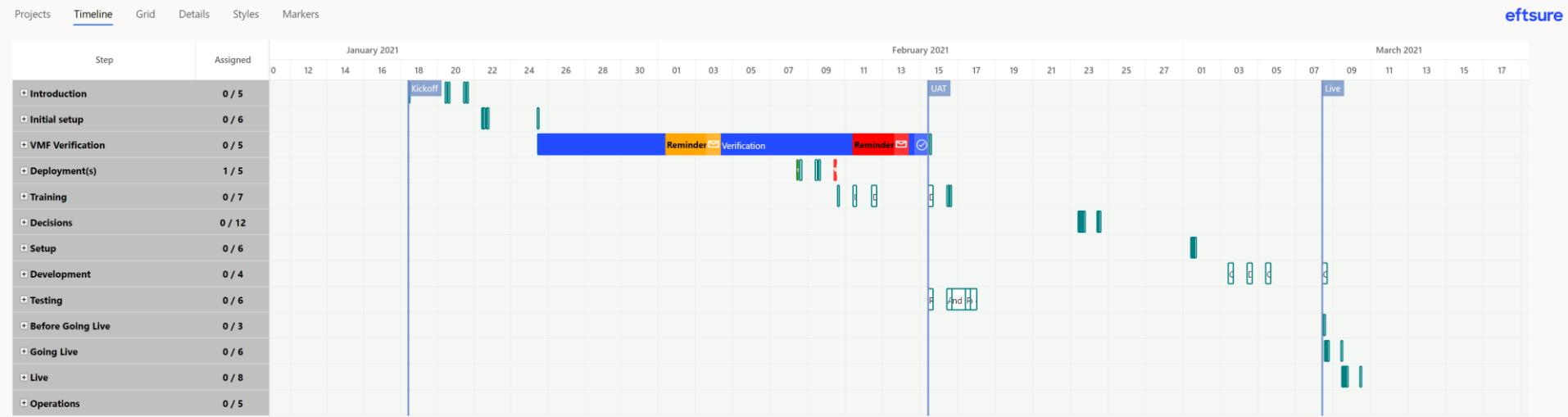
D365 Finance Expert

[berengerep@eftsure.com.au](mailto:berengerep@eftsure.com.au)

eftsure

YOUR  
LOGO  
HERE

# Project Plan



eftsure

# Adoption

- Plan strategy to improve user adoption  
Get your teams excited about the change
- Have all employees stop work and attend the event in person and via video conference
- Invite company leaders to share how the new tech will impact people in their department
- Show employees real-life examples of how the new tech makes their life better
- Continually remind employees of the benefits of the new tech
- Create a poster campaign that highlights key events in the adoption process, from the launch and ongoing training, to helpful how-tos and usage success stories
- Invite employees to give feedback about the new tech via a weekly email, text or Intranet poll
- Host lunch-n-learns and/or ice-cream socials that provide employees with top user tips and a relaxed atmosphere for a Q&A session
- Provide ongoing training opportunities

YOUR  
LOGO  
HERE

# Promote awareness

Make sure everyone understands the goals, fraud methods and risks

Many security experts around the world have studied fraudulent payments and data breaches, they delivered the following non-exhaustive advices to promote awareness in organizations and help prevent the cybercrime issues solved by eftsure and eftsure inside D365FO.

On top of deploying our solution in your organization, it's always a great idea to further promote awareness of the issues to all employees:

- Have a security-first mindset and be suspicious about everything around you. Also, consider investing in your team's education and learn as much as possible about cyber security
- Be vigilant about requests to change suppliers' details, particularly bank account details. Call the requester back to confirm. Speak to who you normally speak to. Never accept an online request to change supplier details.
- Build some rules/policies/procedures around changing supplier details in your accounting software (i.e. each request must be supported by legitimate evidence and phone verification).
- Be insured – request a quote from your local broker for cyber-crime and fraud insurance. It is surprisingly inexpensive.
- Check the amounts being paid to suppliers – does it match your expectations?
- Check your financials against budget/expectations (if you're over budgeted expenditure without explanation, there may be a fraud).
- Has there been a sudden improved change in lifestyle of your administration employees/bookkeeper?
- Do not provide sensitive data over unsecured channels.
- Do not allow strangers to remotely access your computer and/or install software.
- Have a general awareness over what the normal activities of your finance team are and know their well-being. Do they have gambling issues or financial stress? Are they disgruntled? Are they behaving unusually? Do they have a suspected addiction? Is someone in their family ill and need funds to support their rehabilitation?

General awareness will benefit your employees both in their professional and personal life, on top of the added security of this module.

eftsure

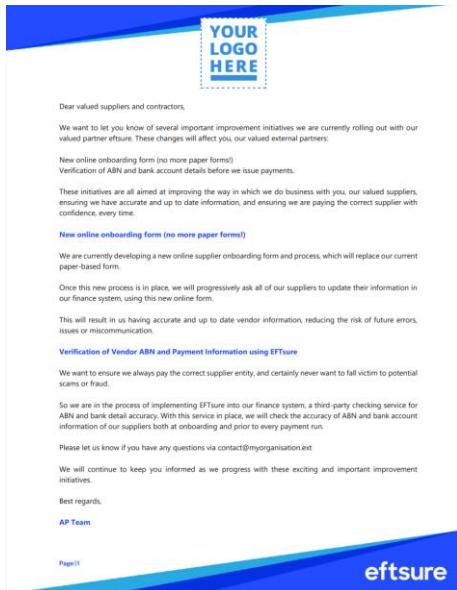
YOUR  
LOGO  
HERE

# External communication

Warn your suppliers early that change is coming

Communicating with your suppliers early is key to a smooth integration into your processes.

Reuse the External Communication Sample email to spread the word on the upcoming changes for your organization.



**Microsoft Word  
Document**

**eftsure**