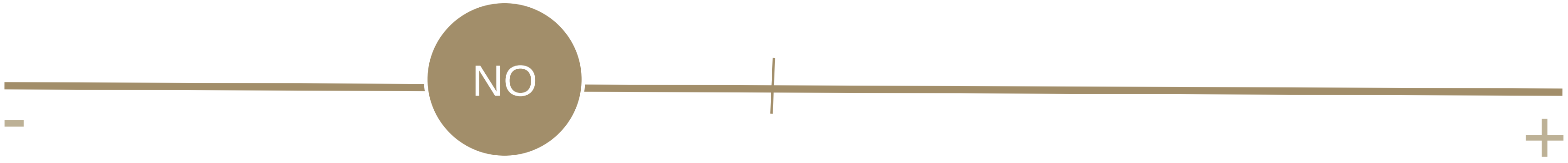
KAN DET VÆRE SÅ VANSKELIG?!

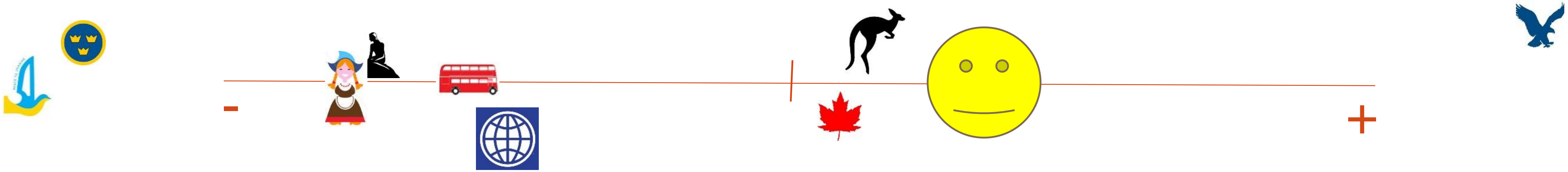
Sikkerhetsstyring i et mottakerperspektiv

UTFORDRING: FAGSYSTEMER



"Vi er dårlige"

Saksbeh.	Ute
Arkiv	Hjemme



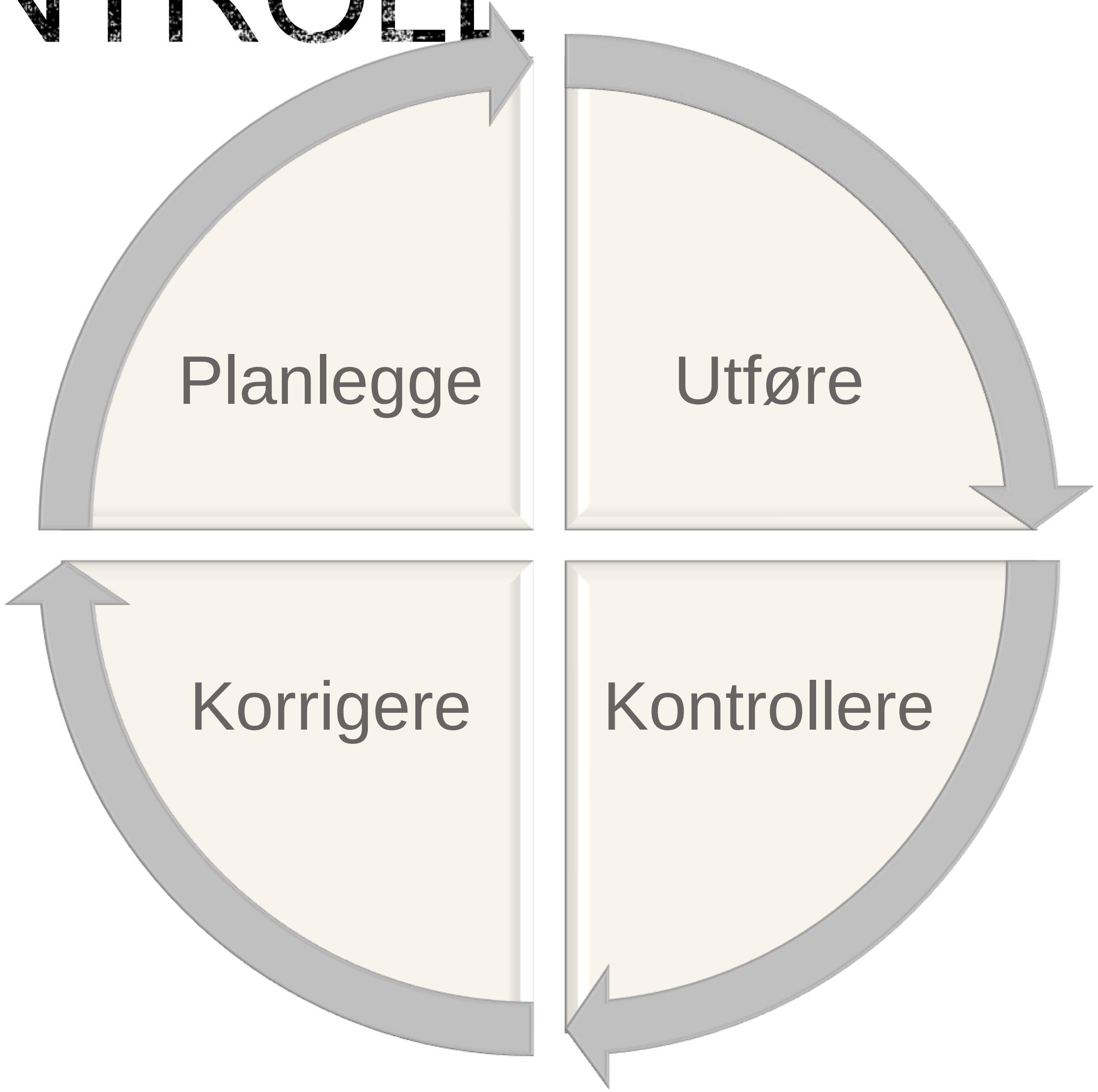
~~"Vi er dårlige"~~

Vi er ikke så dårlige.

…men graden av etterlevelse er ikke god nok.

HVORFOR ER DET SÅ VANSKELIG?

KONTROLL

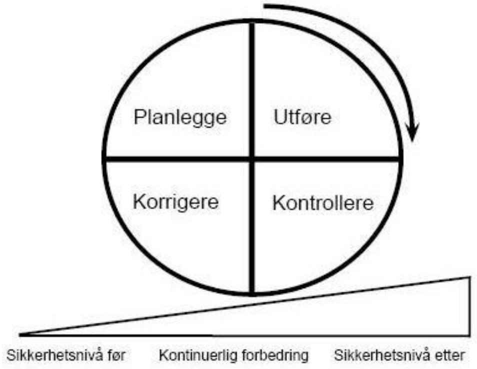


Planlegge

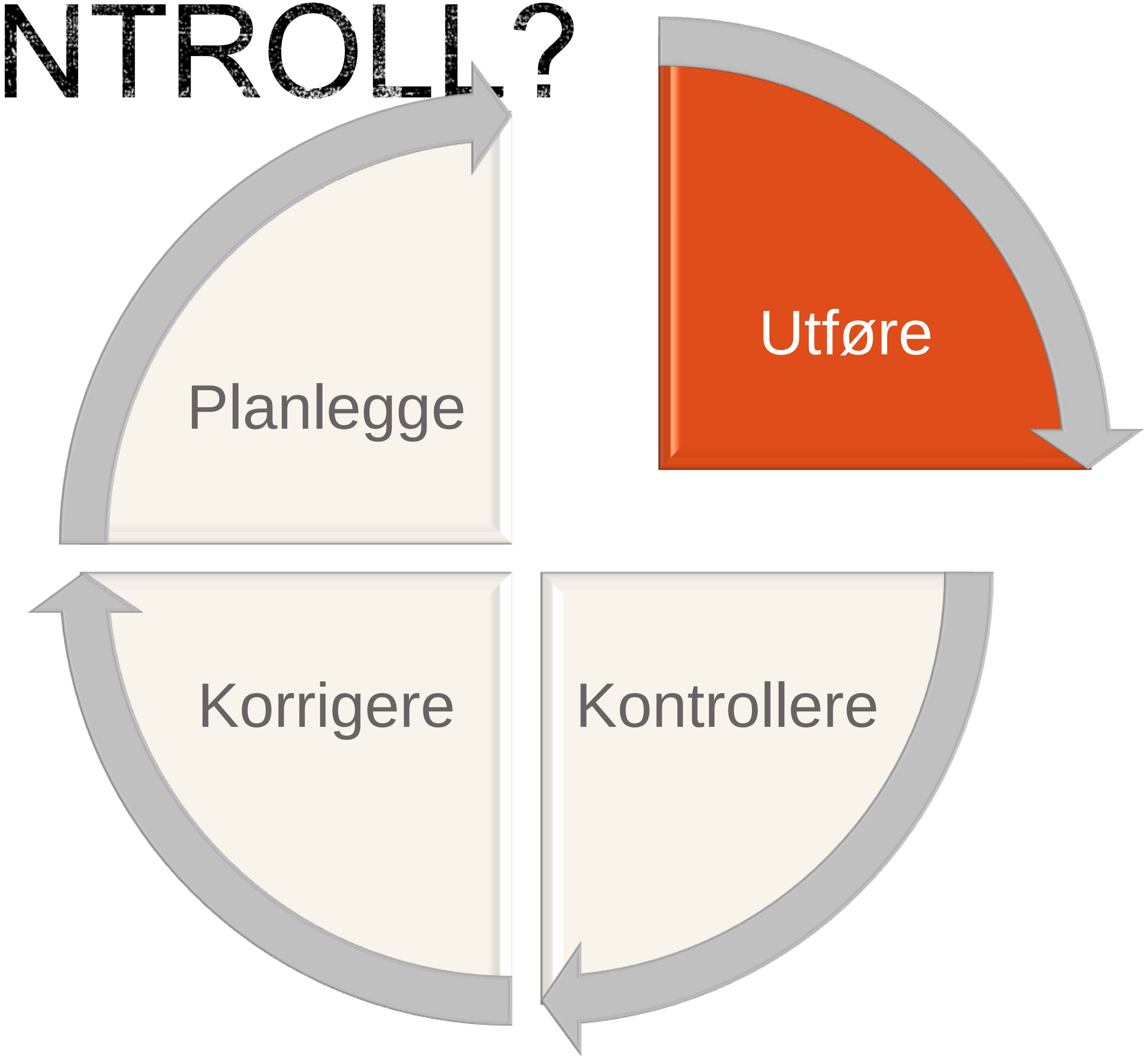
Utføre

Korrigere

Kontrollere



KONTROLL?

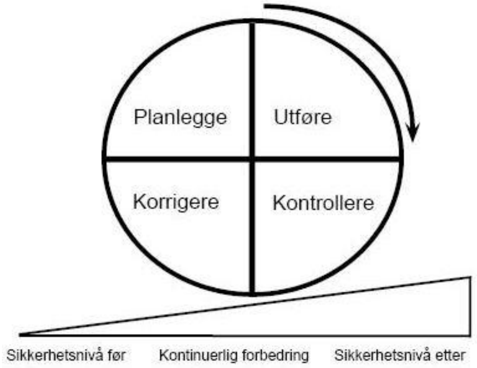


Planlegge

Utføre

Kontrollere

Korrigere



Planlegge

Utføre

Korrigere

Kontrollere

Sikkerhetsnivå før

Kontinuerlig forbedring

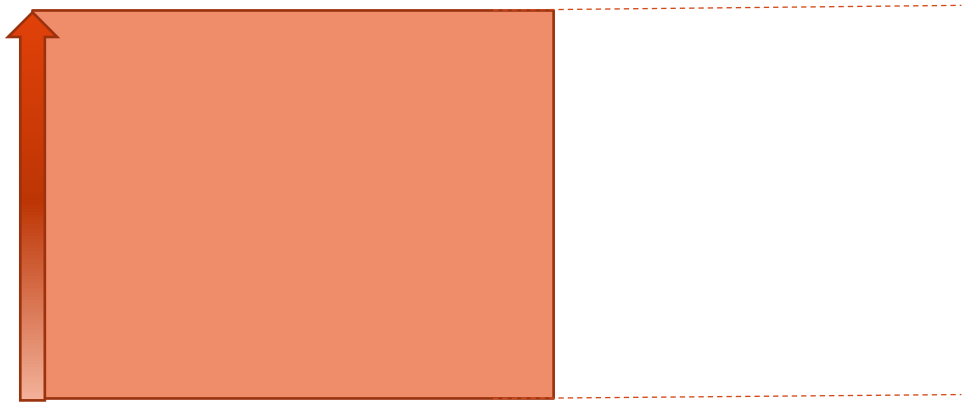
Sikkerhetsnivå etter

REAL MEN
DO IT IN ONE TRIP

("Olympics Rings")

HVA ER PROBLEMET? MERVERDIGAPET.

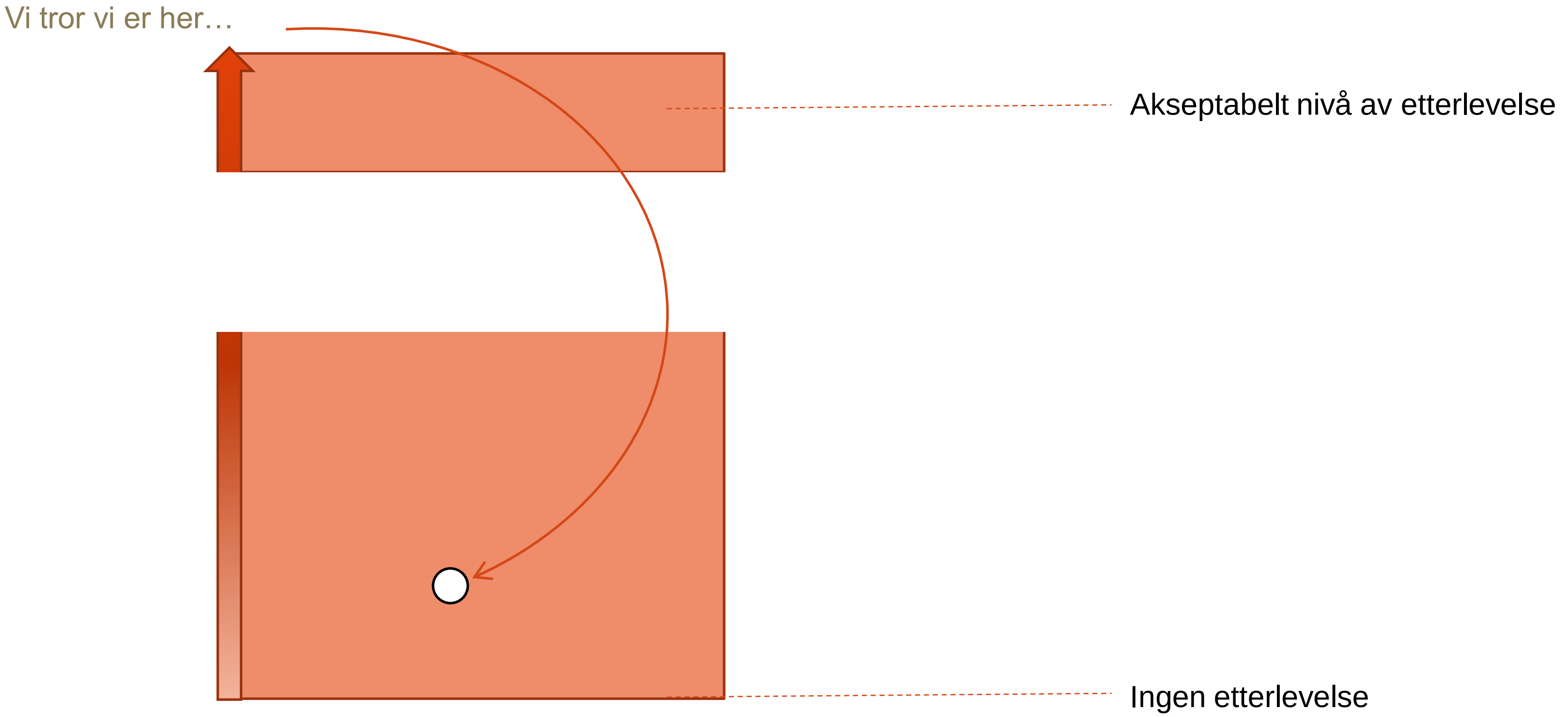
GRAFEN FOR GRAD AV ETTERLEVELSE



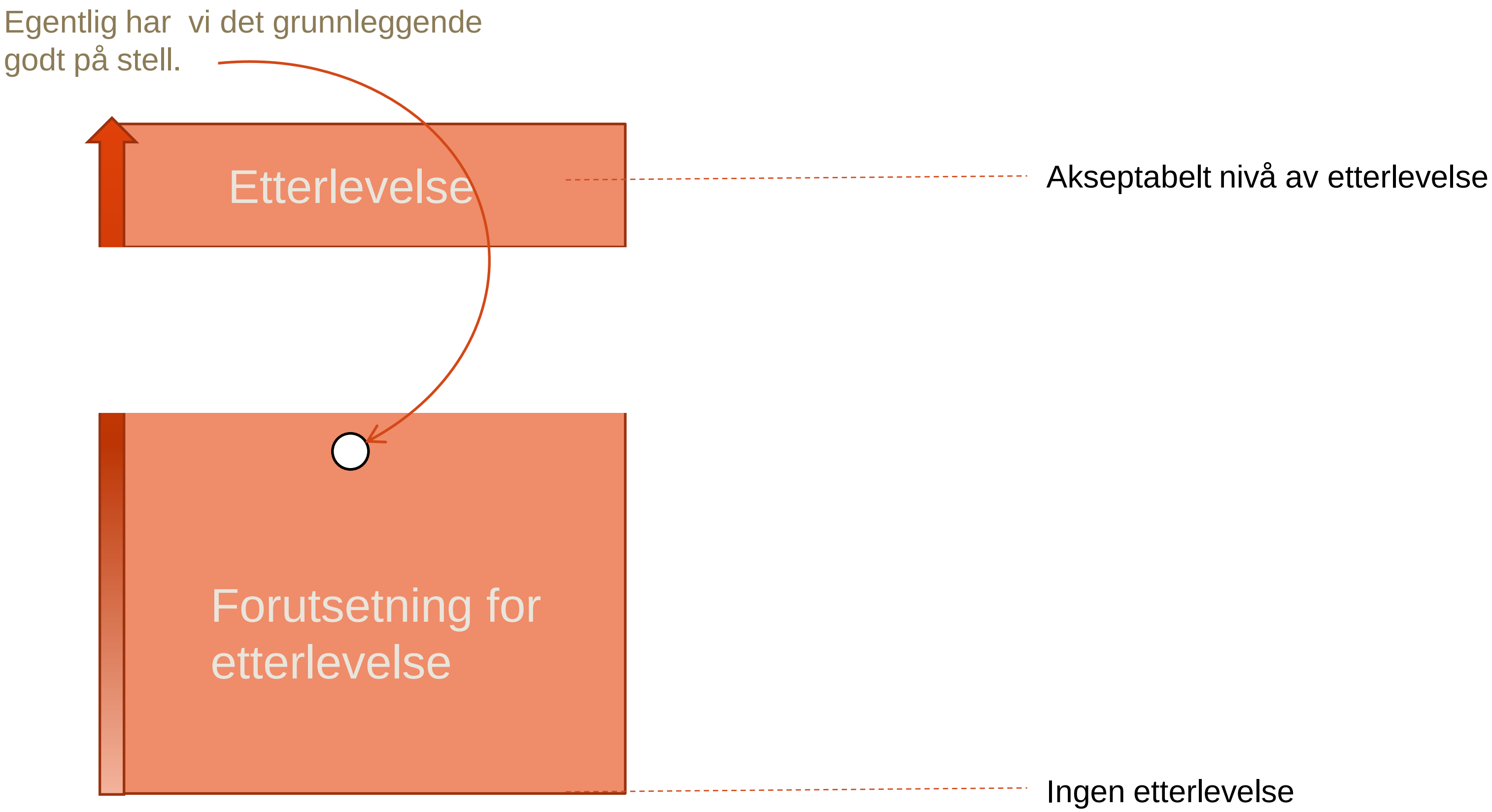
Akseptabelt nivå av etterlevelse

Ingen etterlevelse

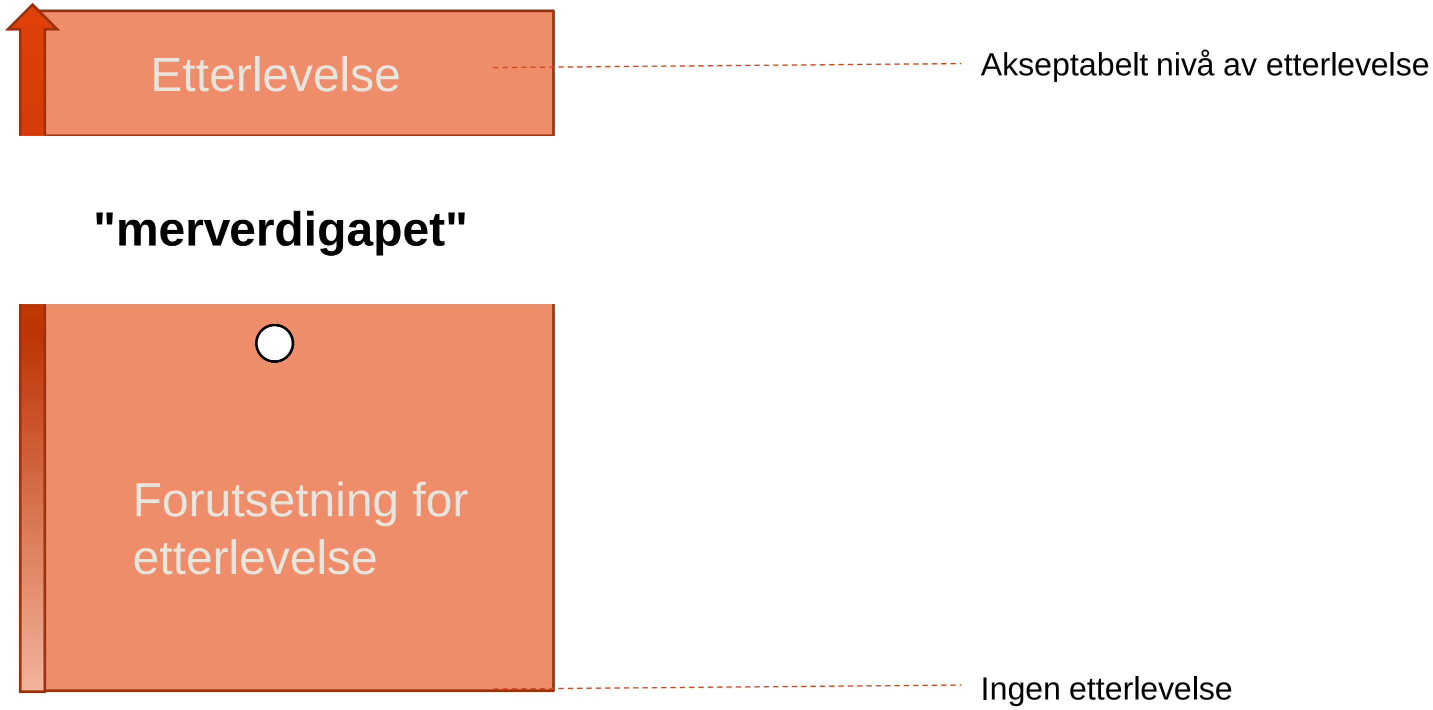
…ER HØYERE ENN VI TROR



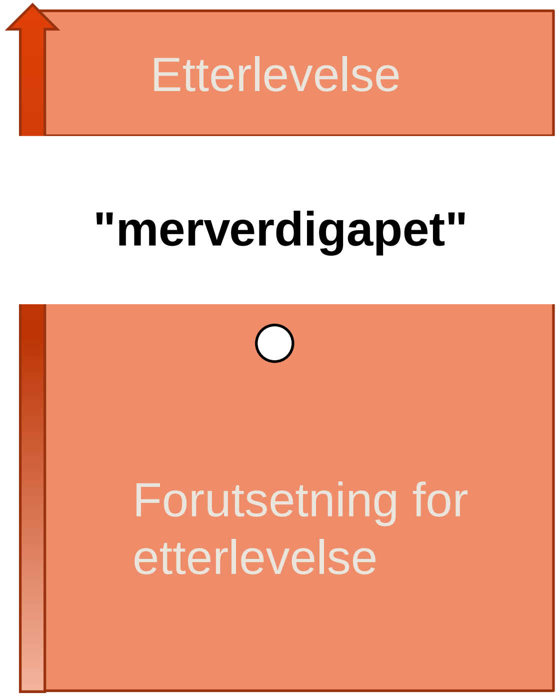
…ER HØYERE ENN VI TROR


Egentlig har vi det grunnleggende godt på stell.
Etterlevelse
Akseptabelt nivå av etterlevelse
Forutsetning for etterlevelse
Ingen etterlevelse

AVVIKET = MERVERDIGAPET

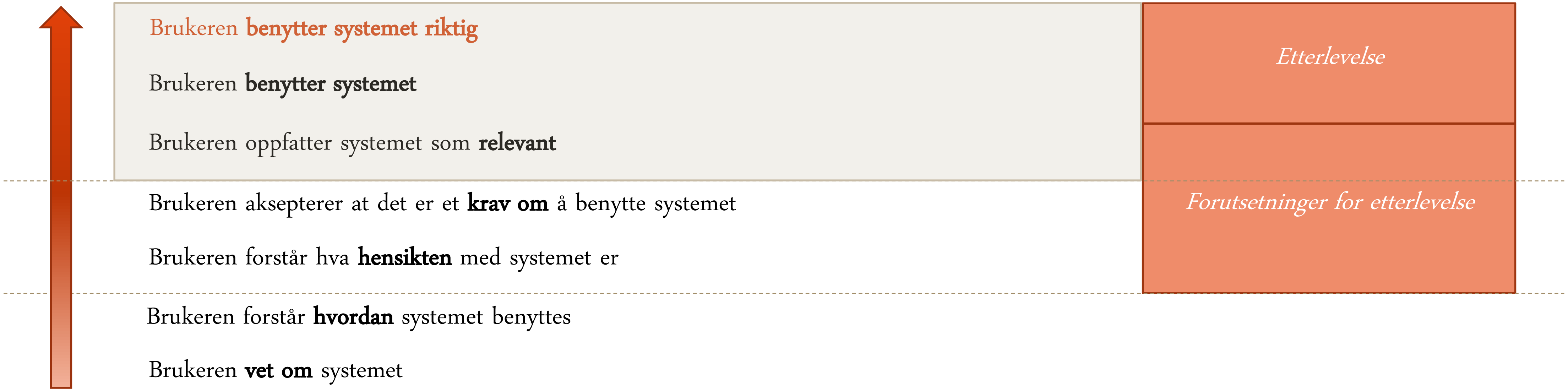

Etterlevelse
Akseptabelt nivå av etterlevelse
"merverdigapet"
Forutsetning for etterlevelse
Ingen etterlevelse

AVVIKET = MERVERDIGAPET



Når brukeren oppfatter systemet som relevant, og/eller ser gevinster ved å bruke systemet. Også kalt "insentiv".

Når alle krav er inkorporert i et system, rutiner beskrevet i dokumenter, og fagområdespesialisene (sikkerhet, risiko, arkiv, ikt) har kontroll.



Brukeren **benytter systemet riktig**

Brukeren **benytter systemet**

Brukeren oppfatter systemet som **relevant**

Brukeren aksepterer at det er et **krav om** å benytte systemet

Brukeren forstår hva **hensikten** med systemet er

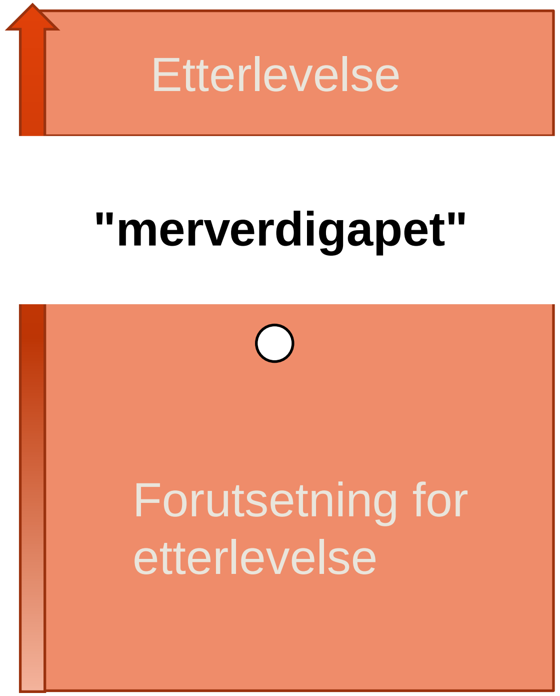
Brukeren forstår **hvordan** systemet benyttes

Brukeren **vet om** systemet

Etterlevelse

Forutsetninger for etterlevelse

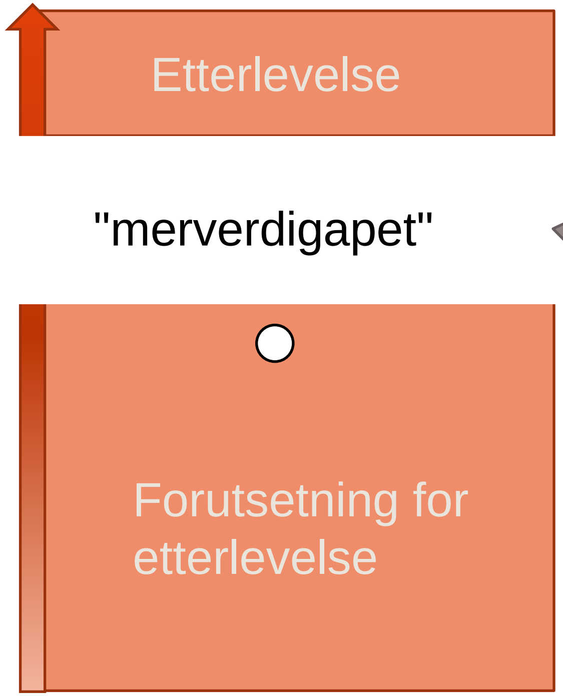
Krever du at brukeren skal ut av prosessen og inn i din fagverden, eller møter du ham/henne der de er i sin prosess?



Etterlevelse

"merverdigapet"

Forutsetning for etterlevelse


Etterlevelse

"merverdigapet"

Forutsetning for etterlevelse

Tilgjengelighet
Gjenfinning
Gjenbruk
Deling / samhandling
Statistikk / historikk
Oversikt
Effektivisering

DEN SISTE MILEN

Snakk med brukerne

Irritasjonsmomenter

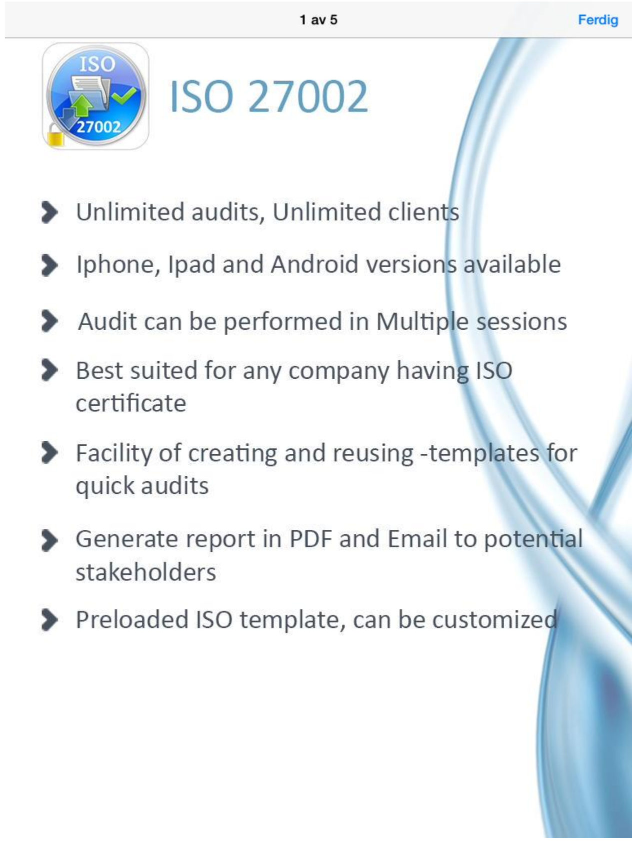
Omkringliggende behov

ETT SKRITT AV GANGEN

HVORDAN SER LØSNINGEN UT HOS DEG?

Hva er merverdien for dine brukere?

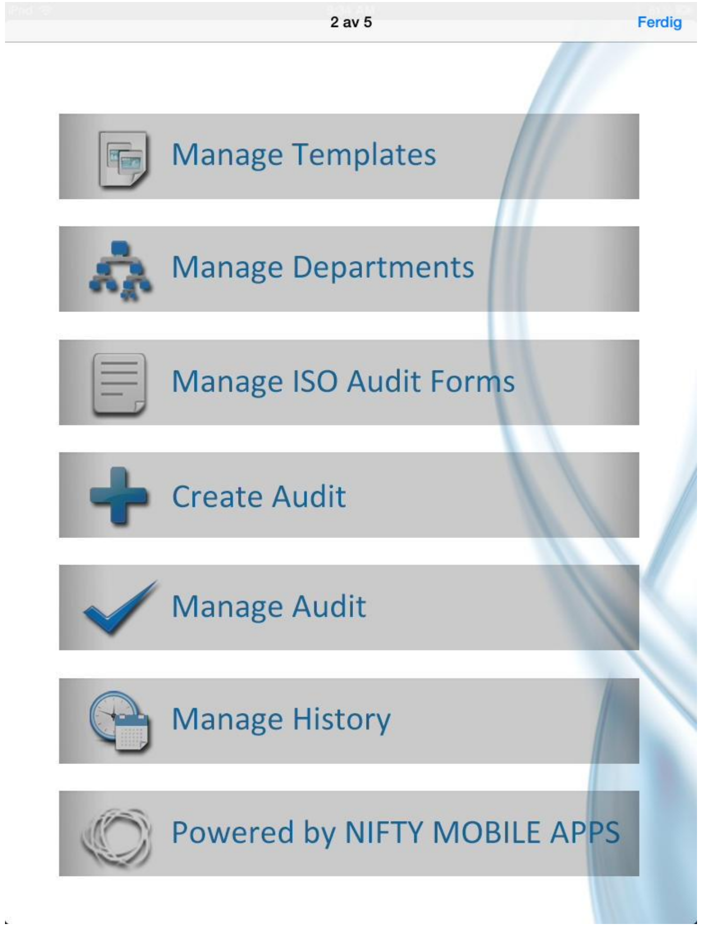
NOEN FORSØK



1 av 5 Ferdig

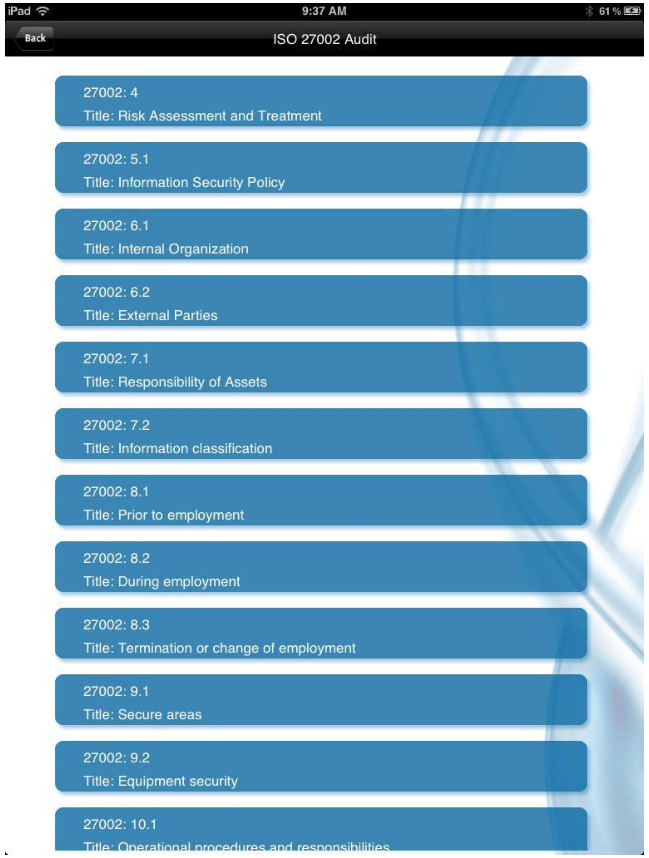
ISO 27002

- Unlimited audits, Unlimited clients
- Iphone, Ipad and Android versions available
- Audit can be performed in Multiple sessions
- Best suited for any company having ISO certificate
- Facility of creating and reusing -templates for quick audits
- Generate report in PDF and Email to potential stakeholders
- Preloaded ISO template, can be customized



2 av 5 Ferdig

- Manage Templates
- Manage Departments
- Manage ISO Audit Forms
- Create Audit
- Manage Audit
- Manage History
- Powered by NIFTY MOBILE APPS



iPad 9:37 AM 61 %

Back ISO 27002 Audit

27002: 4
Title: Risk Assessment and Treatment

27002: 5.1
Title: Information Security Policy

27002: 6.1
Title: Internal Organization

27002: 6.2
Title: External Parties

27002: 7.1
Title: Responsibility of Assets

27002: 7.2
Title: Information classification

27002: 8.1
Title: Prior to employment

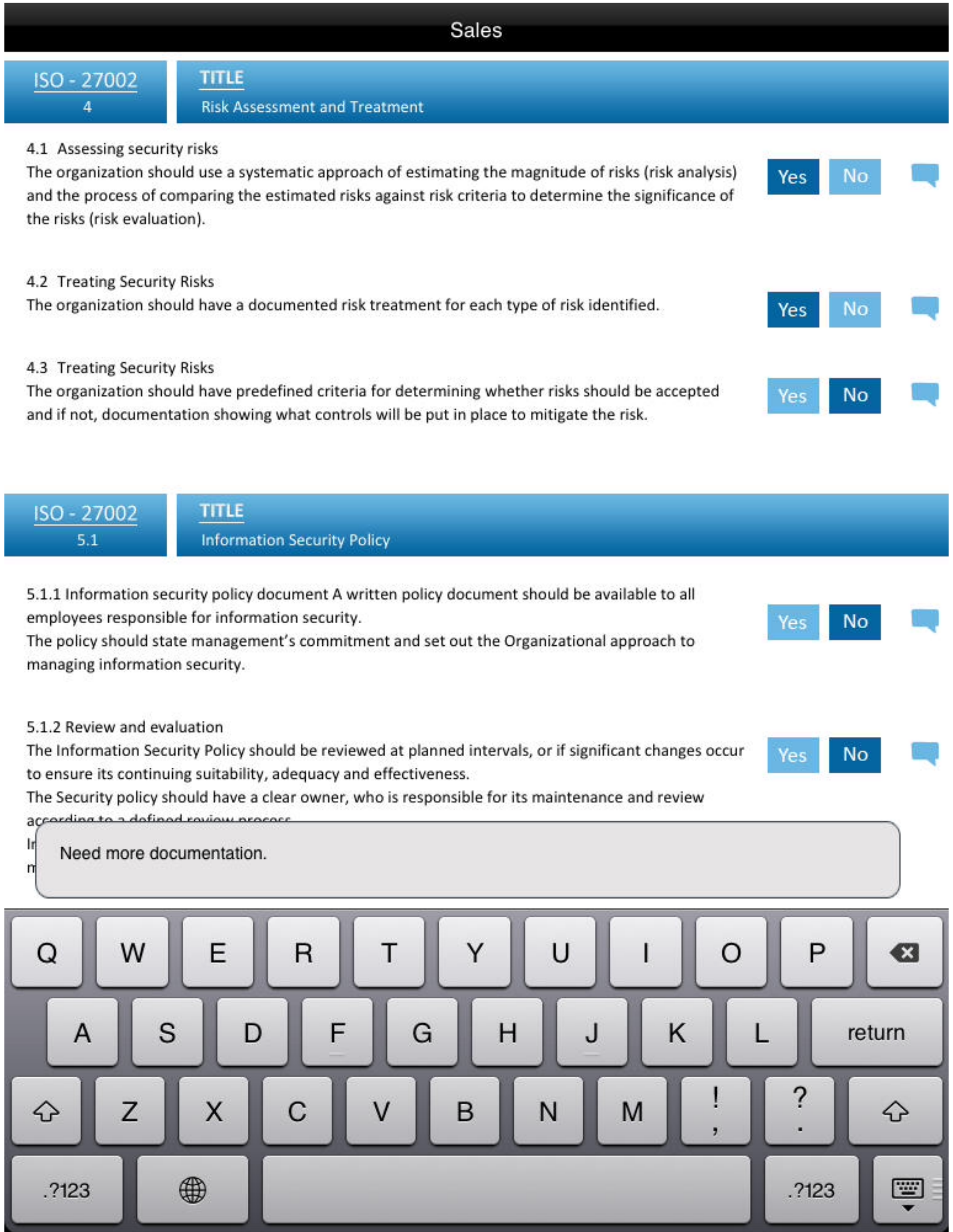
27002: 8.2
Title: During employment

27002: 8.3
Title: Termination or change of employment

27002: 9.1
Title: Secure areas

27002: 9.2
Title: Equipment security

27002: 10.1
Title: Operational procedures and responsibilities



Sales

ISO - 27002
4

TITLE
Risk Assessment and Treatment

4.1 Assessing security risks
The organization should use a systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation).

[✓ Yes] No

4.2 Treating Security Risks
The organization should have a documented risk treatment for each type of risk identified.

[✓ Yes] No

4.3 Treating Security Risks
The organization should have predefined criteria for determining whether risks should be accepted and if not, documentation showing what controls will be put in place to mitigate the risk.

Yes [✓ No]

ISO - 27002
5.1

TITLE
Information Security Policy

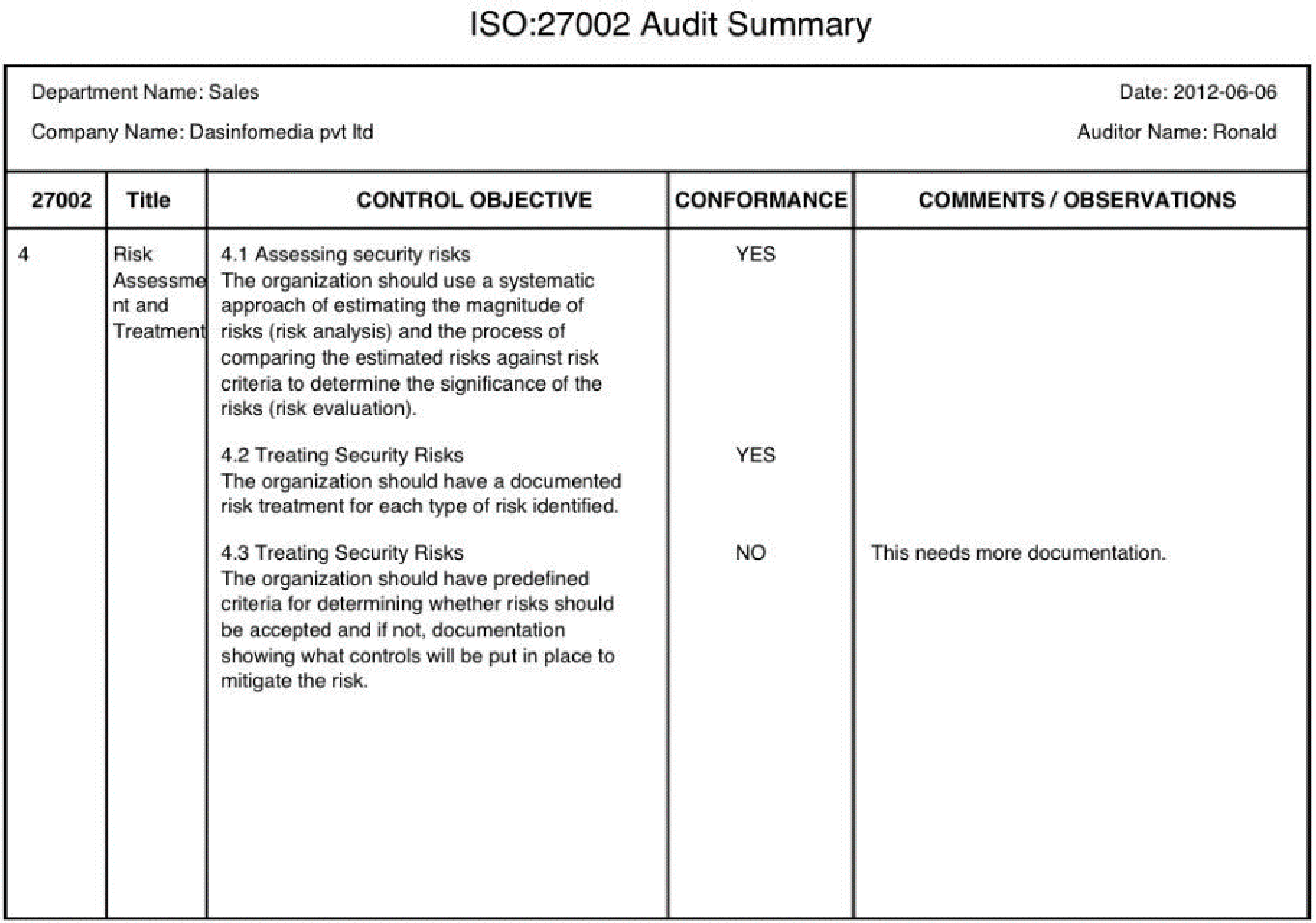
5.1.1 Information security policy document A written policy document should be available to all employees responsible for information security.
The policy should state management’s commitment and set out the Organizational approach to managing information security.

Yes [✓ No]

5.1.2 Review and evaluation
The Information Security Policy should be reviewed at planned intervals, or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness.
The Security policy should have a clear owner, who is responsible for its maintenance and review according to a defined review process.
In
m

Yes [✓ No]

Need more documentation.



ISO:27002 Audit Summary

Department Name: Sales

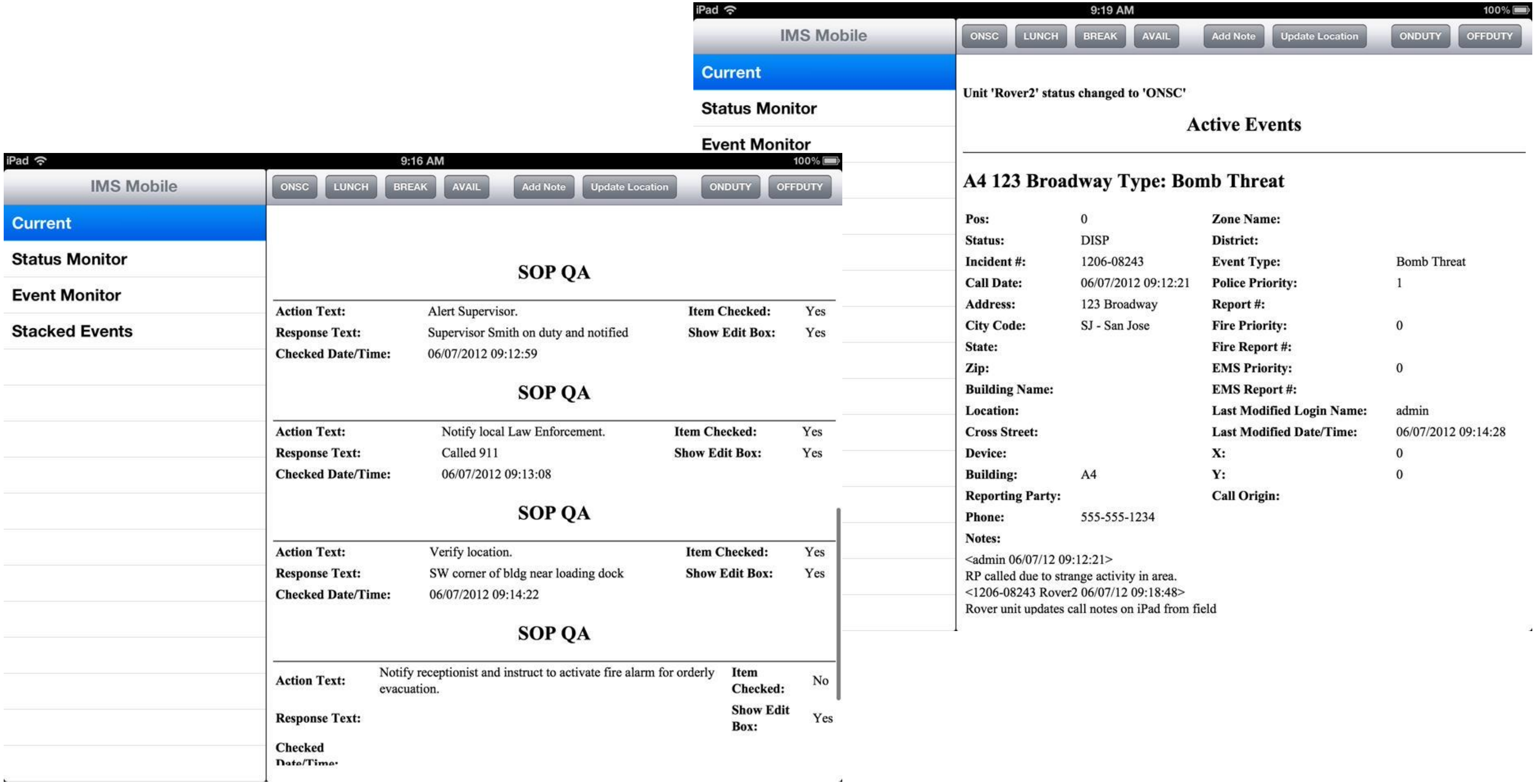
Date: 2012-06-06

Company Name: Dasinfomedia pvt ltd

Auditor Name: Ronald

27002	Title	CONTROL OBJECTIVE	CONFORMANCE	COMMENTS / OBSERVATIONS
4	Risk Assessment and Treatment	4.1 Assessing security risks The organization should use a systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation).	YES	
		4.2 Treating Security Risks The organization should have a documented risk treatment for each type of risk identified.	YES	
		4.3 Treating Security Risks The organization should have predefined criteria for determining whether risks should be accepted and if not, documentation showing what controls will be put in place to mitigate the risk.	NO	This needs more documentation.

VALOR IMS



Unit 'Rover2' status changed to 'ONSC'

Active Events

A4 123 Broadway Type: Bomb Threat

Pos:	0	**Zone Name:**	
Status:	DISP	**District:**	
Incident #:	1206-08243	**Event Type:**	Bomb Threat
Call Date:	06/07/2012 09:12:21	**Police Priority:**	1
Address:	123 Broadway	**Report #:**	
City Code:	SJ - San Jose	**Fire Priority:**	0
State:		**Fire Report #:**	
Zip:		**EMS Priority:**	0
Building Name:		**EMS Report #:**	
Location:		**Last Modified Login Name:**	admin
Cross Street:		**Last Modified Date/Time:**	06/07/2012 09:14:28
Device:		**X:**	0
Building:	A4	**Y:**	0
Reporting Party:		**Call Origin:**	
Phone:	555-555-1234		

Notes:

<admin 06/07/12 09:12:21>
RP called due to strange activity in area.
<1206-08243 Rover2 06/07/12 09:18:48>
Rover unit updates call notes on iPad from field

SOP QA

Action Text:	Alert Supervisor.	**Item Checked:**	Yes
Response Text:	Supervisor Smith on duty and notified	**Show Edit Box:**	Yes
Checked Date/Time:	06/07/2012 09:12:59		

SOP QA

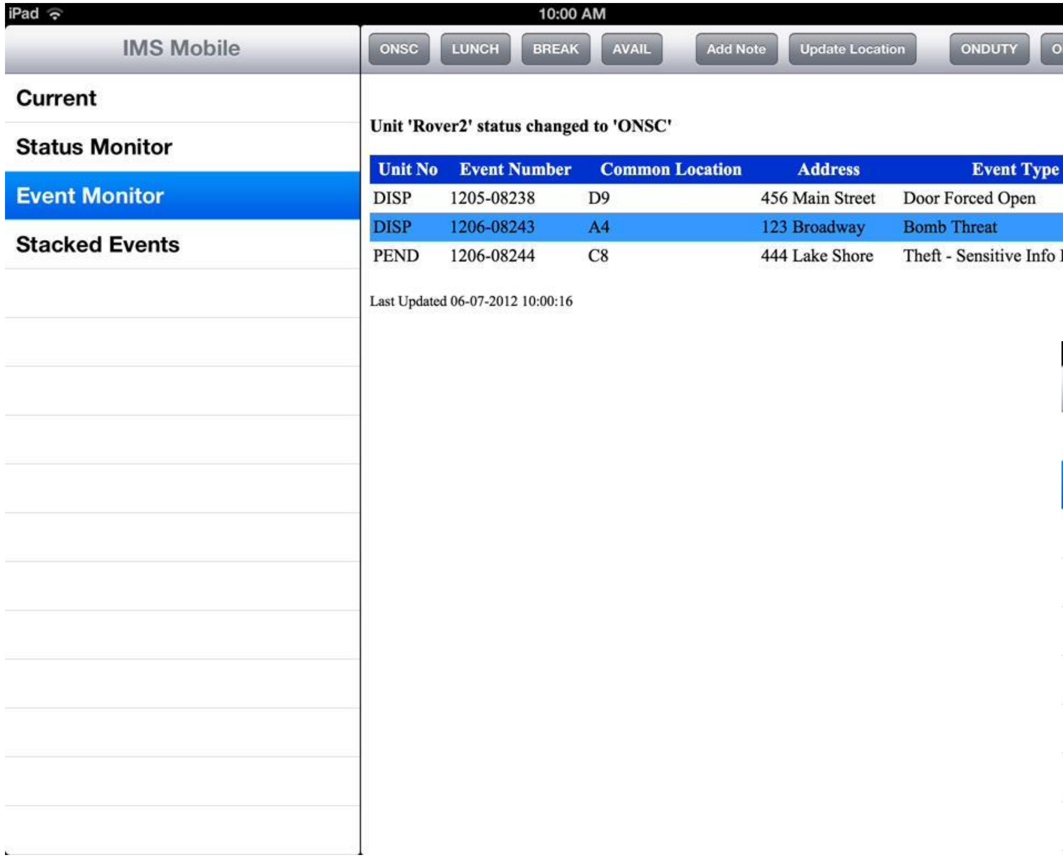
Action Text:	Notify local Law Enforcement.	**Item Checked:**	Yes
Response Text:	Called 911	**Show Edit Box:**	Yes
Checked Date/Time:	06/07/2012 09:13:08		

SOP QA

Action Text:	Verify location.	**Item Checked:**	Yes
Response Text:	SW corner of bldg near loading dock	**Show Edit Box:**	Yes
Checked Date/Time:	06/07/2012 09:14:22		

SOP QA

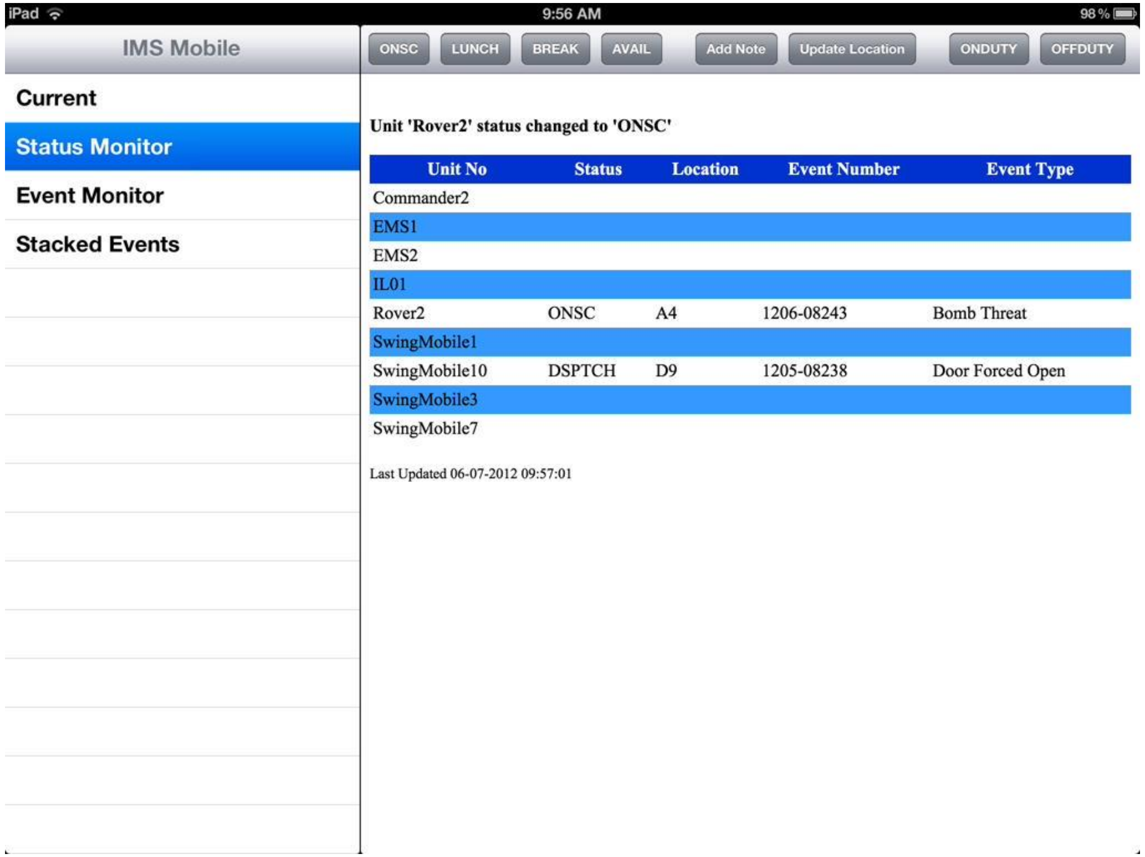
Action Text:	Notify receptionist and instruct to activate fire alarm for orderly evacuation.	**Item Checked:**	No
Response Text:		**Show Edit Box:**	Yes
Checked Date/Time:			



Unit 'Rover2' status changed to 'ONSC'

Unit No	Event Number	Common Location	Address	Event Type
DISP	1205-08238	D9	456 Main Street	Door Forced Open
DISP	1206-08243	A4	123 Broadway	Bomb Threat
PEND	1206-08244	C8	444 Lake Shore	Theft - Sensitive Info Loss

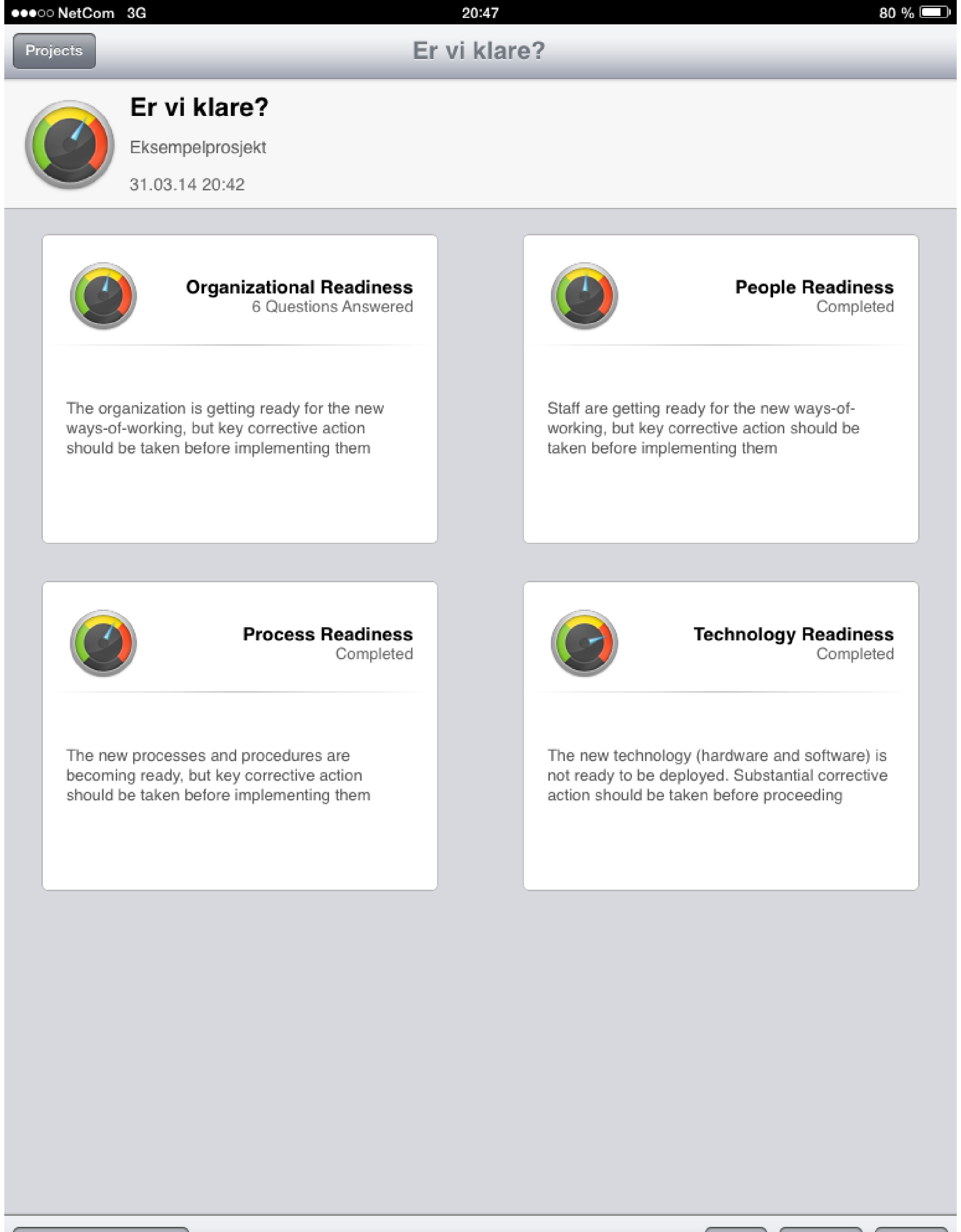
Last Updated 06-07-2012 10:00:16



Unit 'Rover2' status changed to 'ONSC'

Unit No	Status	Location	Event Number	Event Type
Commander2				
EMS1				
EMS2				
IL01				
Rover2	ONSC	A4	1206-08243	Bomb Threat
SwingMobile1				
SwingMobile10	DSPTCH	D9	1205-08238	Door Forced Open
SwingMobile3				
SwingMobile7				

Last Updated 06-07-2012 09:57:01



Er vi klare?

Er vi klare?

Eksempelprosjekt

31.03.14 20:42

Organizational Readiness
6 Questions Answered

The organization is getting ready for the new ways-of-working, but key corrective action should be taken before implementing them

People Readiness
Completed

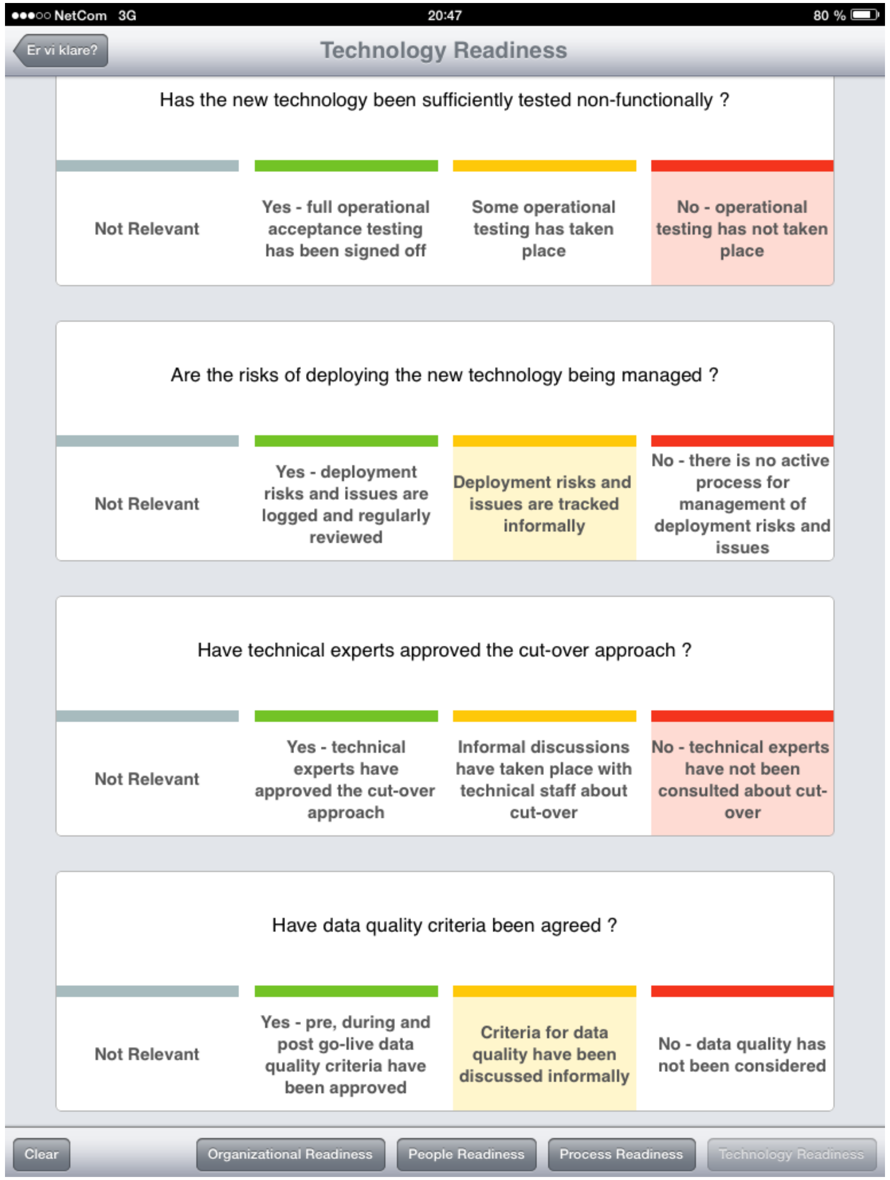
Staff are getting ready for the new ways-of-working, but key corrective action should be taken before implementing them

Process Readiness
Completed

The new processes and procedures are becoming ready, but key corrective action should be taken before implementing them

Technology Readiness
Completed

The new technology (hardware and software) is not ready to be deployed. Substantial corrective action should be taken before proceeding



Technology Readiness

Has the new technology been sufficiently tested non-functionally ?

Not Relevant	Yes - full operational acceptance testing has been signed off	Some operational testing has taken place	No - operational testing has not taken place

Are the risks of deploying the new technology being managed ?

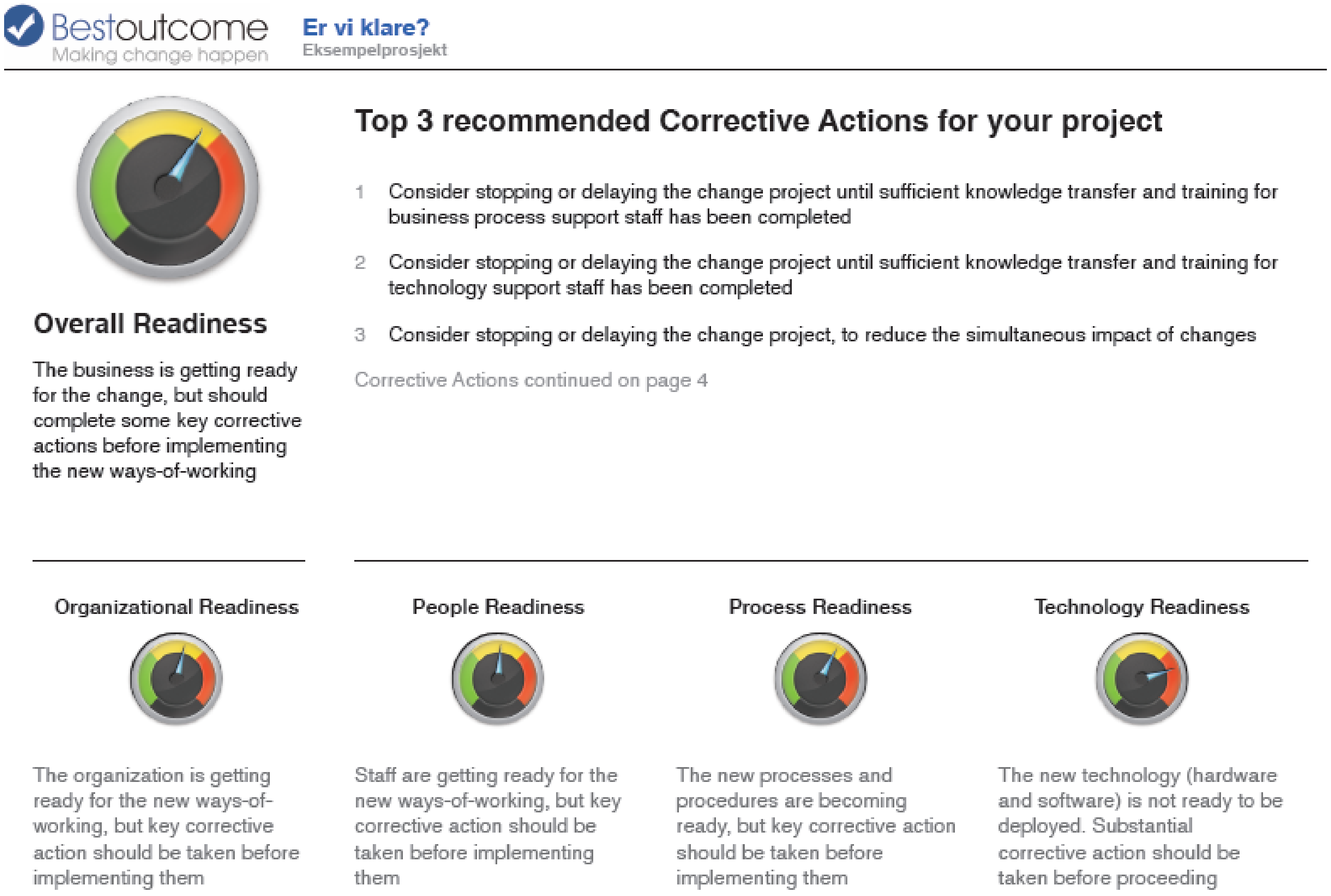
Not Relevant	Yes - deployment risks and issues are logged and regularly reviewed	Deployment risks and issues are tracked informally	No - there is no active process for management of deployment risks and issues

Have technical experts approved the cut-over approach ?

Not Relevant	Yes - technical experts have approved the cut-over approach	Informal discussions have taken place with technical staff about cut-over	No - technical experts have not been consulted about cut-over

Have data quality criteria been agreed ?

Not Relevant	Yes - pre, during and post go-live data quality criteria have been approved	Criteria for data quality have been discussed informally	No - data quality has not been considered



Bestoutcome
Making change happen

Er vi klare?
Eksempelprosjekt

Top 3 recommended Corrective Actions for your project

1 Consider stopping or delaying the change project until sufficient knowledge transfer and training for business process support staff has been completed

2 Consider stopping or delaying the change project until sufficient knowledge transfer and training for technology support staff has been completed

3 Consider stopping or delaying the change project, to reduce the simultaneous impact of changes

Corrective Actions continued on page 4

Overall Readiness

The business is getting ready for the change, but should complete some key corrective actions before implementing the new ways-of-working

Organizational Readiness

The organization is getting ready for the new ways-of-working, but key corrective action should be taken before implementing them

People Readiness

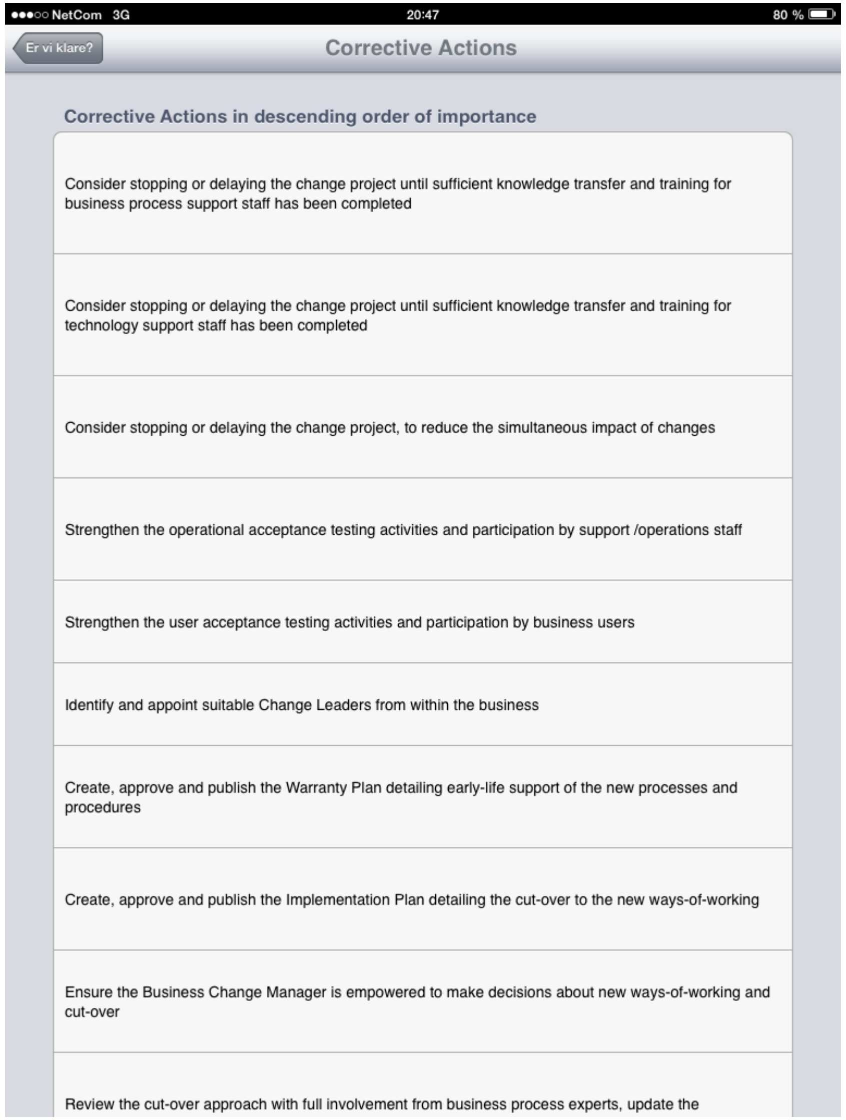
Staff are getting ready for the new ways-of-working, but key corrective action should be taken before implementing them

Process Readiness

The new processes and procedures are becoming ready, but key corrective action should be taken before implementing them

Technology Readiness

The new technology (hardware and software) is not ready to be deployed. Substantial corrective action should be taken before proceeding



Corrective Actions

Corrective Actions in descending order of importance

Consider stopping or delaying the change project until sufficient knowledge transfer and training for business process support staff has been completed

Consider stopping or delaying the change project until sufficient knowledge transfer and training for technology support staff has been completed

Consider stopping or delaying the change project, to reduce the simultaneous impact of changes

Strengthen the operational acceptance testing activities and participation by support /operations staff

Strengthen the user acceptance testing activities and participation by business users

Identify and appoint suitable Change Leaders from within the business

Create, approve and publish the Warranty Plan detailing early-life support of the new processes and procedures

Create, approve and publish the Implementation Plan detailing the cut-over to the new ways-of-working

Ensure the Business Change Manager is empowered to make decisions about new ways-of-working and cut-over

Review the cut-over approach with full involvement from business process experts, update the

KAN DET VÆRE SÅ VANSKELIG?

DET ER VANSKELIG

- Få føler de har lykkes
- Sjansen for at du er kommet lenger enn du tror er stor
- Samtidig er det lenger igjen til målet enn du tror
- Lykkes du å fylle **merverdigapet** vil graden av etterlevelse øke

- Husk at det er et maraton, ikke en spurt
- Våg å satse på ny teknologi / tenke nytt

"Brukervennlige løsninger gjør etterlevelse av regelverk lettere i en hverdag preget av tidspress.

Tungvinte, langsomme og lite tilgjengelige systemer øker risikoen for at snarveier benyttes."