# Programme
# Fortify Digital Security

Liedewij Lamers

8th of September 2017



# PROGRAMME MANAGEMENT



# What do you expect as a member?

- Your personal data is safe
- What I read is my business only
- E-books just ‘work’
- Downloads can be trusted
- Data in catalogue is accurate
- Websites and portals work and are safe





# The future of the KB

Transformation

Physical collections → Fully digital library

- Full speed digital
- Enhance use of collections
- Strengthen our international position

# Digital Security increasingly important



- Keep the trust
  - Of our members
  - Of our partners
  - Of the copyright holders
  - Of our financiers
- Continuity of our organisation

# Trust is built on strong foundations

What are the foundations for digital security within the KB?



# The six foundations

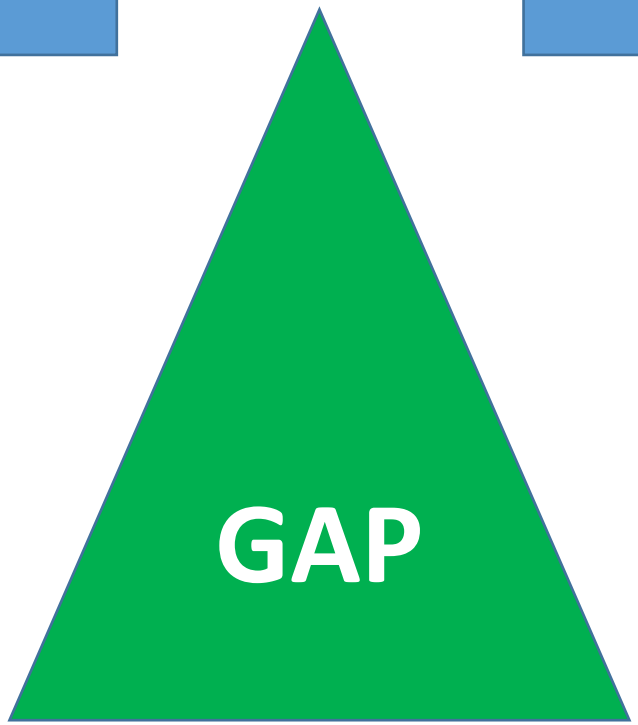
- ✓ Roles and funding are available
- ✓ Laws and regulations form basic level
- ✓ Prepared for incidents and limits impacts
- ✓ Perdurable storage and availability is our priority
- ✓ Guarantee content, catalogue and service of national digital library
- ✓ Accomplish digital security in close co-operation with our partners



# What is the quality of these foundations?

CURRENT STATE

TARGET STATE



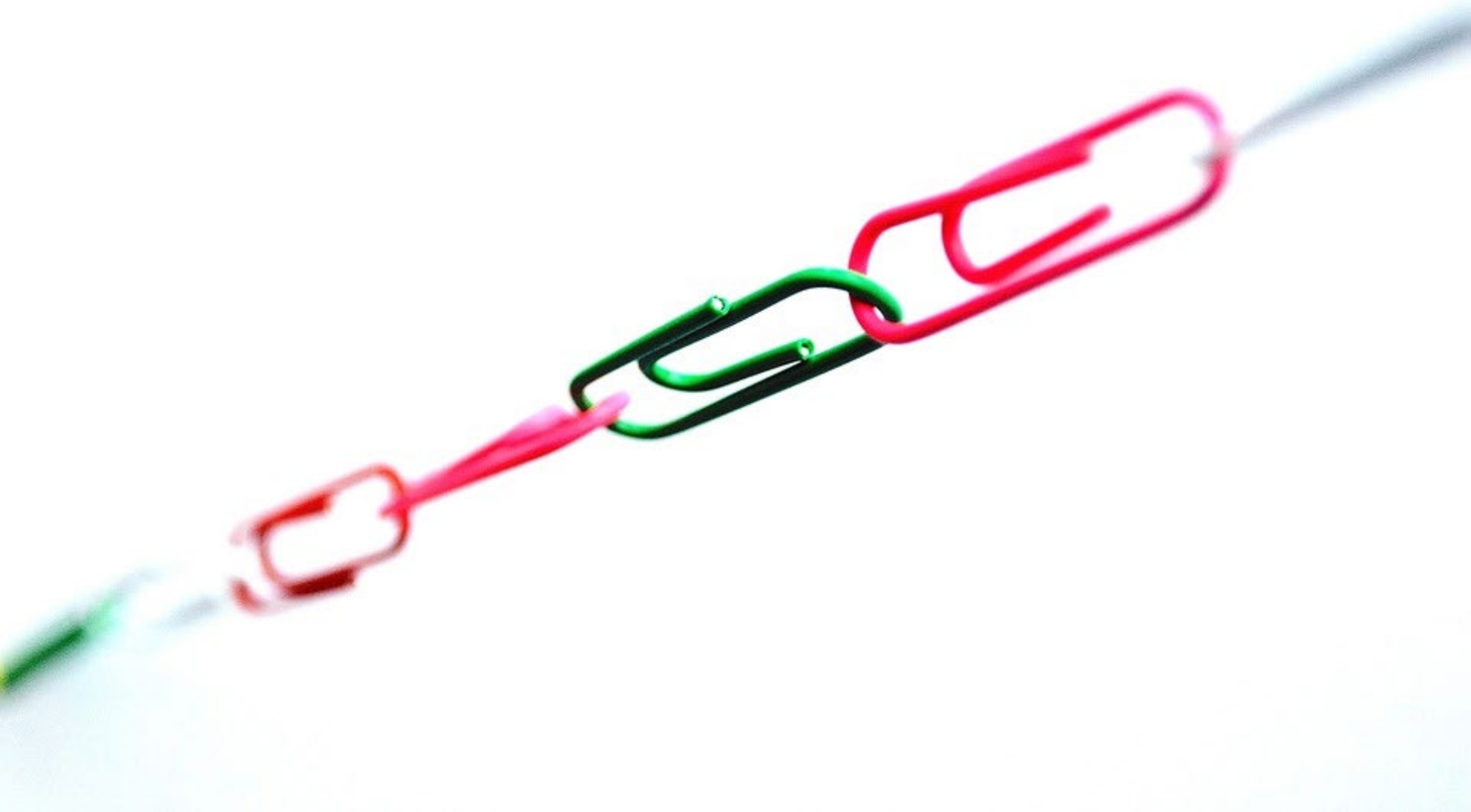
KB Koninklijke Bibliotheek
Nationale bibliotheek van Nederland



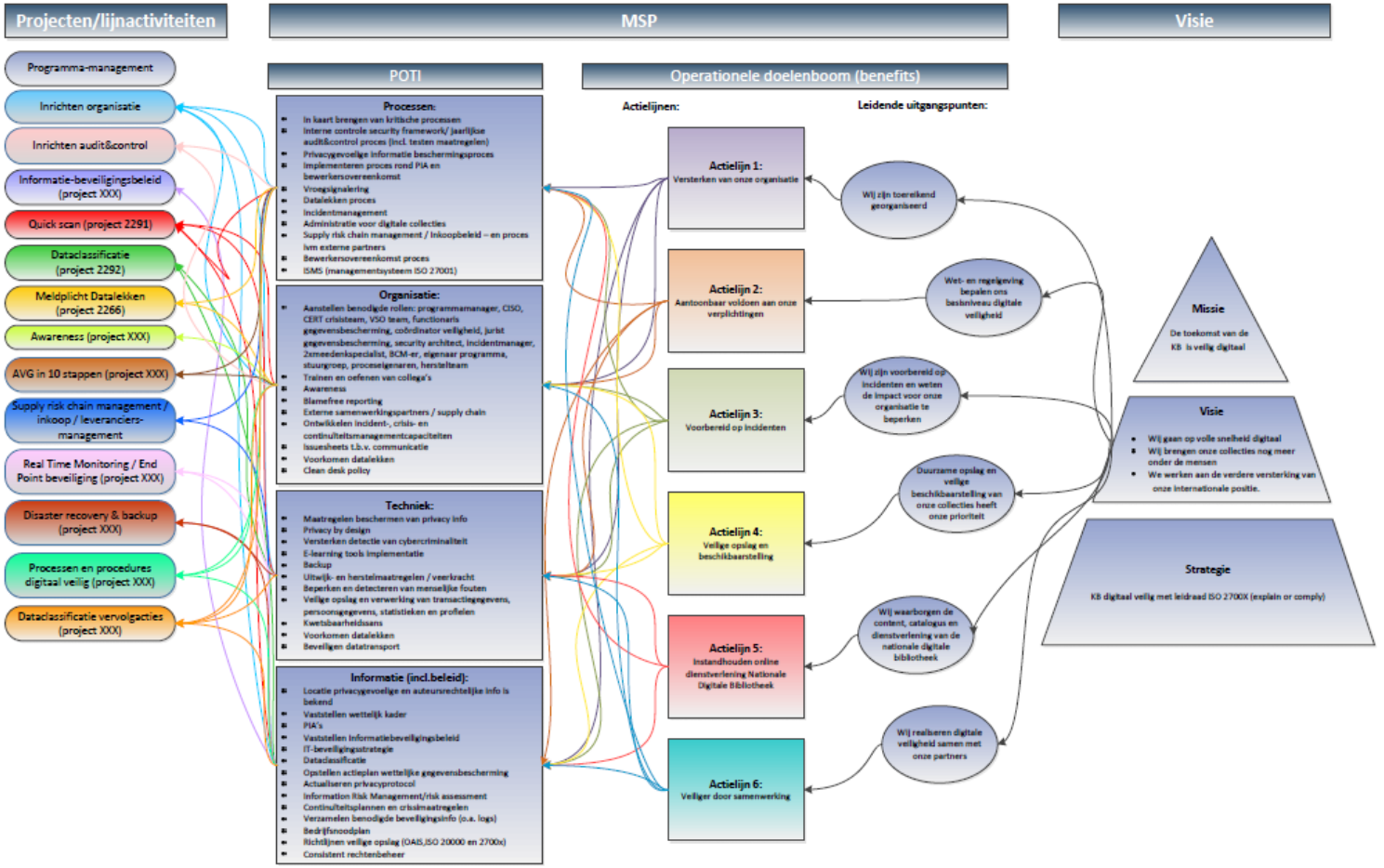
# What are those paths to take?




1. Strengthen our organisation
2. Prove we can fullfill our obligations
3. Be prepared for incidents and impact management
4. Secure storage and accesibility of collections
5. Continuity of the national digital library online service
6. Security in the full chain (close co-operation with our partners)

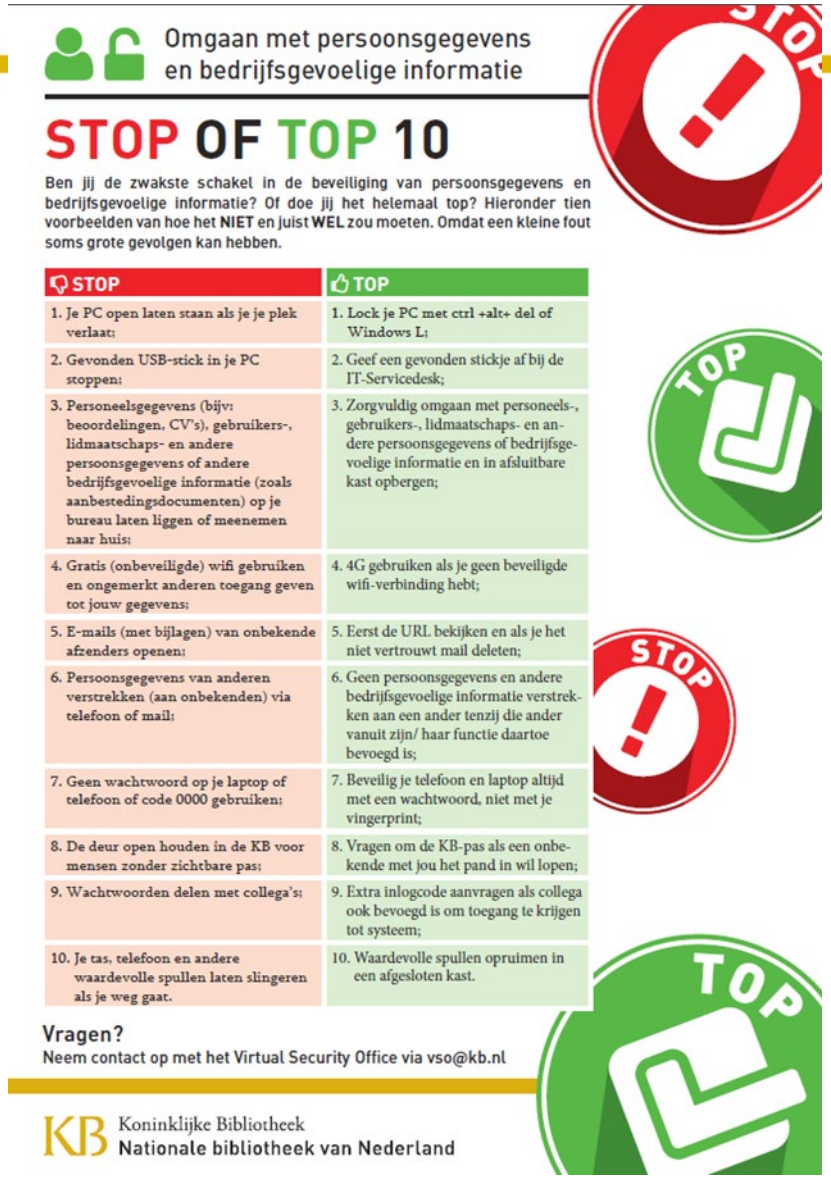


# Programme map



# Accomplishments

- Organisation is stronger
- Monitoring ‘early warning’ has been improved
- Increased awareness among staff
- Developed processes and procedures regarding digital security
- Scan by expert company on to determine strenghts and weaknesses in more detail



Omgaan met persoonsgegevens en bedrijfsgevoelige informatie

## STOP OF TOP 10

Ben jij de zwakste schakel in de beveiliging van persoonsgegevens en bedrijfsgevoelige informatie? Of doe jij het helemaal top? Hieronder tien voorbeelden van hoe het **NIET** en juist **WEL** zou moeten. Omdat een kleine fout soms grote gevolgen kan hebben.

| STOP | TOP |
|---|---|
| 1. Je PC open laten staan als je je plek verlaat; | 1. Lock je PC met ctrl +alt+ del of Windows L; |
| 2. Gevonden USB-stick in je PC stoppen; | 2. Geef een gevonden stickje af bij de IT-Servicedesk; |
| 3. Personeelsgegevens (bijv: beoordelingen, CV’s), gebruikers-, lidmaatschaps- en andere persoonsgegevens of andere bedrijfsgevoelige informatie (zoals aanbestedingsdocumenten) op je bureau laten liggen of meenemen naar huis; | 3. Zorgvuldig omgaan met personeels-, gebruikers-, lidmaatschaps- en andere persoonsgegevens of bedrijfsgevoelige informatie en in afsluitbare kast opbergen; |
| 4. Gratis (onbeveiligde) wifi gebruiken en ongemerkt anderen toegang geven tot jouw gegevens; | 4. 4G gebruiken als je geen beveiligde wifi-verbinding hebt; |
| 5. E-mails (met bijlagen) van onbekende afzenders openen; | 5. Eerst de URL bekijken en als je het niet vertrouwt mail deleten; |
| 6. Persoonsgegevens van anderen verstrekken (aan onbekenden) via telefoon of mail; | 6. Geen persoonsgegevens en andere bedrijfsgevoelige informatie verstrekken aan een ander tenzij die ander vanuit zijn/ haar functie daartoe bevoegd is; |
| 7. Geen wachtwoord op je laptop of telefoon of code 0000 gebruiken; | 7. Beveilig je telefoon en laptop altijd met een wachtwoord, niet met je vingerprint; |
| 8. De deur open houden in de KB voor mensen zonder zichtbare pas; | 8. Vragen om de KB-pas als een onbekende met jou het pand in wil lopen; |
| 9. Wachtwoorden delen met collega’s; | 9. Extra inlogcode aanvragen als collega ook bevoegd is om toegang te krijgen tot systeem; |
| 10. Je tas, telefoon en andere waardevolle spullen laten slingeren als je weg gaat. | 10. Waardevolle spullen opruimen in een afgesloten kast. |

**Vragen?**
Neem contact op met het Virtual Security Office via vso@kb.nl

Koninklijke Bibliotheek
Nationale bibliotheek van Nederland

# Goals 2017

1. Data classification
2. Continuous focus on awareness
3. Start implementation EU General Data Protection Regulation (GDPR)
4. Defining proper actions resulting the quick scan



# Overall plan for 2018

- Strong focus on strenghtening awareness
- Rerun data classification
- Compliancy to GDPR
- Implement actions from scan and rerun scan (yearly)



# Questions?

