



National Institute for Public Health
and the Environment
Ministry of Health, Welfare and Sport



Biosecurity self- assessment toolkit and vulnerability assay

Harold van den Berg
The Netherlands Biosecurity Office



The Netherlands Biosecurity Office

National biosecurity knowledge and information office, aimed at organisations working with high risk pathogens (BSL 3 and 4)

Several activities to create awareness for biosecurity:

- Target group: professionals (stakeholders)



Biosecurity Workshops



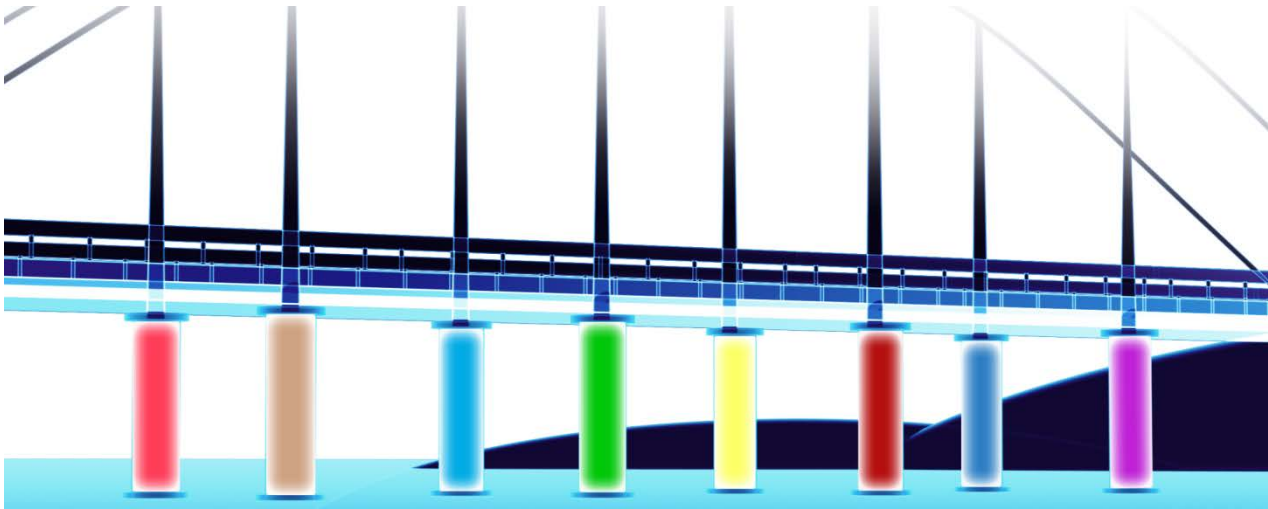
Biosecurity Movie



Biosecurity Toolkit



Biosecurity Movie





Biosecurity toolkit

Goal of the Biosecurity toolkit

- To indicate the current level of biosecurity in the organisation
- To identify potential gaps in the biosecurity regime inside an organization
- To provide related legal basis (rules and legislation) and a set of good practices to improve the level of biosecurity





Novel Dutch self-assessment Biosecurity Toolkit to identify biorisk gaps and to enhance biorisk awareness

Petra C. C. Sijnesael^{1,2}, Linda M. van den Berg¹, Diederik A. Bleijs^{1,3}, Paul Odinet⁴, Carin de Hoog¹, Mieke W. J. C. Jansen⁵, Evelien Kampert⁶, Saskia A. Rutjes^{1,7}, Martien Broekhuijsen⁸ and Sander Banus^{1*}

Biosecurity Self-scan toolkit

Web-based: <http://www.biosecuritytoolkit.com>
(Anonymous and freely available)



Biosecurity Self-scan Toolkit

Version 1.6-RELEASE © 2012-2015 RIVM

[Home](#) [Awareness](#) [Personnel reliability](#) [Transport security](#) [Information security](#) [Accountability for materials](#) [Response](#) [Management](#) [Physical measures](#) [Results](#) [Contact](#)

Biosecurity Self-scan Toolkit

Welcome to the biosecurity self-scan toolkit of the [Biosecurity Office](#). The toolkit is in the form of a questionnaire covering the eight pillars of biosecurity that is designed to give you an indication of the current level of biosecurity in your organisation.

You can start the toolkit at the first pillar, 'Awareness' and then work your way through all the pillars, or you can start at a pillar of your choice and answer the questions on that particular subject first. If a question does not apply to your organisation, it will not be counted in the results.

You can view the interim results at any time, but bear in mind that the more questions you have answered, the more accurate a picture you will get of the current state of affairs in your organisation and what still needs to be done. On the results page you can click on each pillar to access specific tips and good practices (implementation examples) which may help you to improve biosecurity in your organisation. The results can be printed out for discussion purposes.

For more information or if you have any questions, please e-mail us at: biosecurity@rivm.nl

[Start the questionnaire](#)

Print



Self-scan toolkit

- Background information
- Several questions on all themes (8 pillars)



012-2015 RIVM

Information security Accountability for materials Response Management **Physical measures** Results Contact

Physical measures

Are all biological agents stored in sealed and secure locations?
This falls under responsible conduct. Yes No N.A.

Is access to the storage locations being checked?
The organisation has a record of which personnel have access to which locations. Yes No N.A.

Is the entrance to the storage location secured by a combination of at least two methods?
These methods may consist of: Something you have (key), something you know (PIN code), something you are (biometrics) Yes No N.A.

Are these locations under guard and can all storage points be locked?
Access routes to locations that contain high-risk materials are being monitored, and these locations are not accessible to the public. Yes No N.A.



Results of Self-scan toolkit

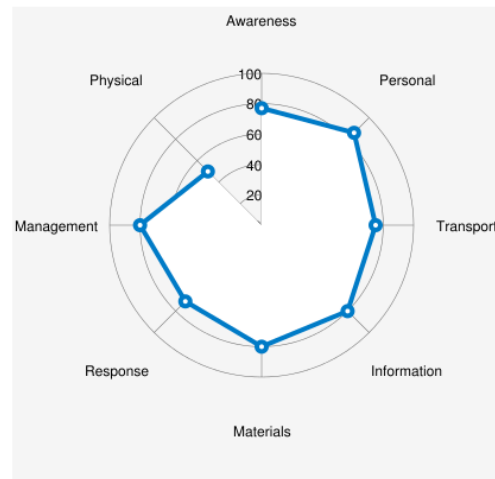
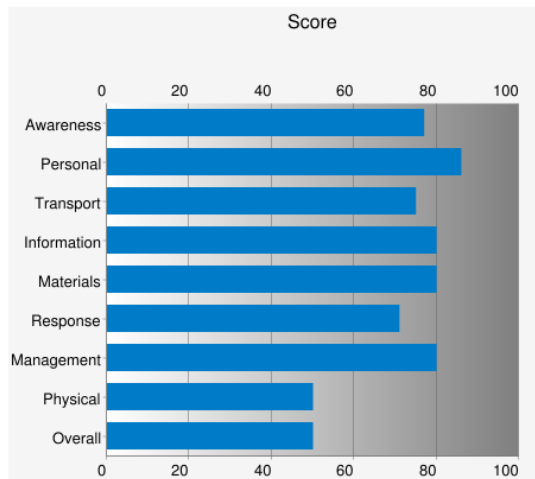
Results

Clicking on the pillar will take you to another tab on the Biosecurity Office website where you will find specific tips and good practices for this pillar.

Category	Yes	No	N.A.	Score (%)
Awareness ^{L2}	5	2	1	77
Personnel reliability ^{L2}	6	1	0	86
Transport security ^{L2}	7	2	0	75
Information security ^{L2}	8	2	0	80
Accountability for materials ^{L2}	8	2	0	80
Response ^{L2}	5	2	0	71
Management ^{L2}	8	2	0	80
Physical measures ^{L2}	2	2	0	50
Biosecurity overall score				50

Focussing on gaps:

- To improve overall score, attention should be given to lowest score
- Increases awareness



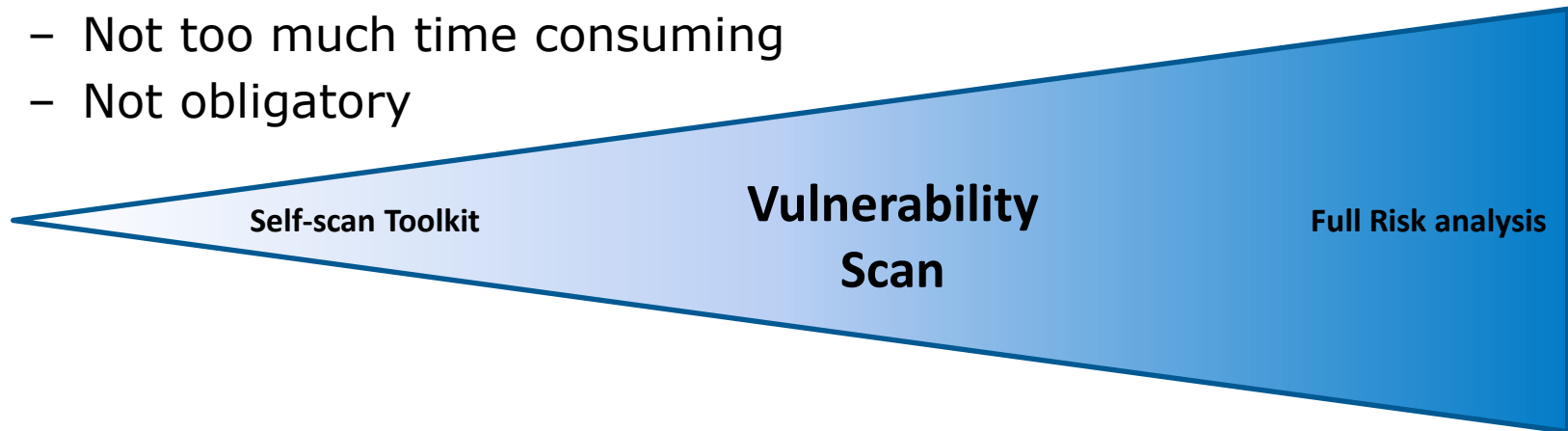


Improvement of the Biosecurity Toolkit

- Input from professionals (workshop and meetings)
 - Less abstract
 - More options per question, not only yes or no
 - More practical tool
 - > more good practices, including practical examples

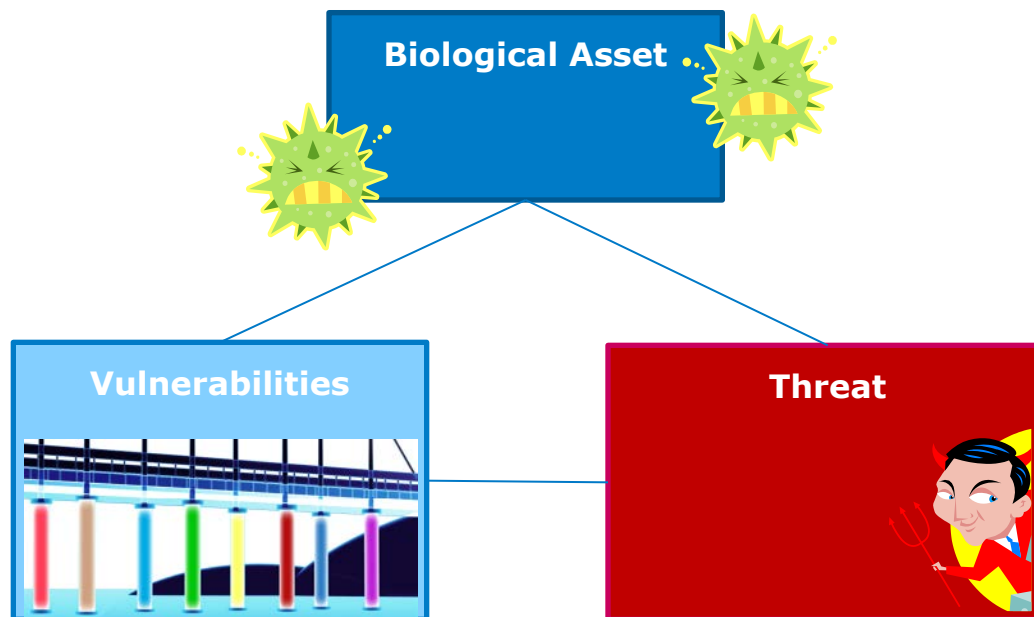
But:

- Not too detailed
- Not too much time consuming
- Not obligatory





Vulnerability scan \neq Biosecurity Risk Analysis





Vulnerability scan

Together with professionals (expert group) Bureau Biosecurity is developing this more practical tool

Bureau Biosecurity

Home Quick Scan Vulnerability Scan

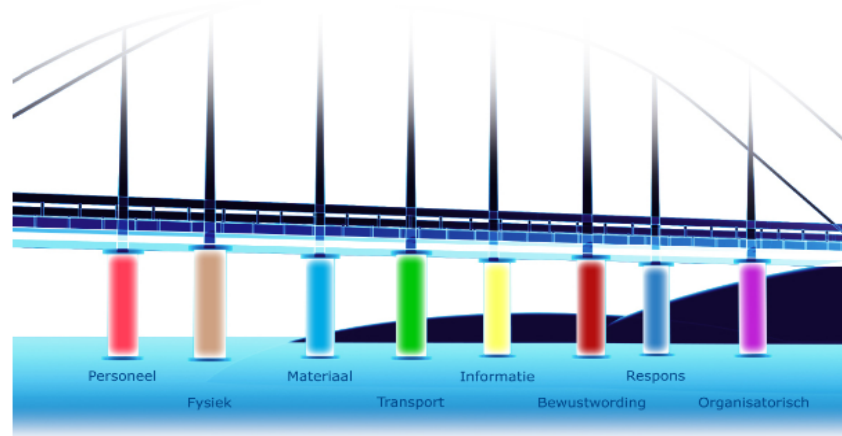
zoek

Sitemap Uitgebreid zoeken

[Home](#) Biosecurity - Vulnerability Scan

Biosecurity - Vulnerability Scan

Klik op een pijler om hiermee verder te gaan.



Extra uitleg indien nodig

Meer informatie:

[KNAW gedragscode voor biosecurity \(pdf\)](#)

[Laboratory biorisk management standard \(CWA 15793\)\(pdf\)](#)

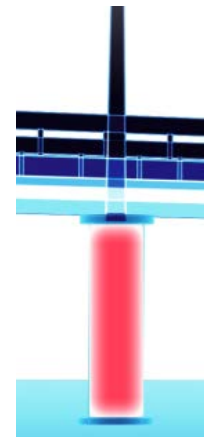
[Biosecurity Toolkit](#)



Selection of one pillar

General information

- The importance of this pillar for biosecurity
- The contribution of the pillar to biosecurity
- The content of the pillar
- Choice between Questionnaire and Scenarios





Selection of one pillar



Fysieke beveiliging

Uw voortgang in de vragenlijst:

Inleiding tot de vragen

Bij beveiliging denkt men vaak het eerste aan sloten, toegangspoorten, portiers, beveiligingspersoneel en camera's. Deze vormen van beveiligen vallen onder fysieke beveiliging en barrières en verschillende maatregelen versterkt de fysieke beveiliging, waardoor het voor onbevoegden lastiger wordt om toegang te krijgen tot het hoogrisico materiaal. Het is hierbij van belang. Fysieke beveiliging bestaat dus uit barrières, maatregelen en autorisatie & controle van de toegang. Hier worden in deze pijler vragen over gesteld.



Foto: paslezer met vingerafdruk

In deze pijler krijgt u meer inzicht in:

- Gelaagde of gefragmenteerde beveiliging (vraag 1 en scenario 3, 4 en 6);
- Verschillende fysieke maatregelen (vraag 2 en scenario 2, 3 en 4);
- Verschillende beveiligingsystemen (vraag 3 en scenario 4);
- Autorisatie & controle van de toegang (vraag 4 en scenario 1, 2, 3 en 5);
- Het belang van de bewustwording en alertheid van medewerkers (vraag 5 en 6 en scenario 1, 3, 5 en 6).

Hier kunt u de keuze maken om verder te gaan met de **vragen** of **scenario's**.

Door middel van het beantwoorden van de vragen worden de belangrijkste elementen van fysieke beveiliging binnen uw organisatie doorgenomen. Met de scenario's worden aan de hand van reële situaties kwetsbaarheden zichtbaar gemaakt. Wanneer de scenario's worden doorlopen, wordt een inzicht verkregen hoe uw organisatie omgaat met deze kwetsbaarheden.

Vragen



Scenario's





Questionnaire and scenarios

Questionnaire

- More detail into the pillar by specific questions
- Multiple answers provides direct information for improvement (if possible)

Scenarios

- Show important vulnerabilities by recognizable situations, based on experiences from the field
- Motivate to invest if this situation can occur at the organisation
- Motivate to address measurements for improvement

Direct feedback per answer/scenario

- Provide relevant and practical feedback per answer
- Provide relevant references
- Link questions and scenarios

Report

Overview of all answers and scenarios with

- relevant and practical feedback
- relevant references



Example of a question



Fysieke beveiliging

Uw voortgang in de vragenlijst:

1. Is de beveiliging van biologisch materiaal opgebouwd uit meerdere beveiligingslagen?

Een beveiligingslaag is een barrière die voorkomt dat onbevoegde personen toegang hebben tot een gebied, gebouw of ruimte. Voorbeelden van barrières zijn een toe van het soort barrière, andere kennis vereist (klimmen over hek, deur openen, sleutel nodig voor opslag). Wanneer de beveiliging van een organisatie bestaat uit één onbevoegd persoon overal toegang tot heeft. Door de beveiliging van de organisatie te fragmenteren ofwel het aanbrengen van meerdere beveiligingslagen wordt voor heeft tot de hoogrisico ruimte en/of materiaal (zie figuur 1).

- A. De fysieke beveiliging van hoog risico materiaal is opgebouwd uit vier of meer beveiligingslagen.
- B. De fysieke beveiliging van hoog risico materiaal is opgebouwd uit drie beveiligingslagen.
- C. De fysieke beveiliging van hoog risico materiaal is opgebouwd uit twee beveiligingslagen.
- D. De fysieke beveiliging van hoog risico materiaal is opgebouwd uit een beveiligingslaag.
- E. Er is geen beveiligingslaag voor hoog risico materiaal (denk bijvoorbeeld aan veldwerk).

Vraag 1

Vraag 2

Vraag 3

Vraag 4

Vraag 5

Vraag 6



Example of a question



Fysieke beveiliging

Uw voortgang in de vragenlijst:

1. Is de beveiliging van biologisch materiaal opgebouwd uit meerdere beveiligingslagen?

Een beveiligingslaag is een barrière die voorkomt dat onbevoegde personen toegang hebben tot een gebied, gebouw of ruimte. Voorbeelden van barrières zijn een to van het soort barrière, andere kennis vereist (klimmen over hek, deur openen, sleutel nodig voor opslag). Wanneer de beveiliging van een organisatie bestaat uit één onbevoegd persoon overal toegang tot heeft. Door de beveiliging van de organisatie te fragmenteren ofwel het aanbrenge van meerdere beveiligingslagen wordt vo heeft tot de hoogrisico ruimte en/of materiaal (zie figuur 1).

- A. De fysieke beveiliging van hoog risico materiaal is opgebouwd uit vier of meer beveiligingslagen.
- B. De fysieke beveiliging van hoog risico materiaal is opgebouwd uit drie beveiligingslagen.
- C. De fysieke beveiliging van hoog risico materiaal is opgebouwd uit twee beveiligingslagen.
- D. De fysieke beveiliging van hoog risico materiaal is opgebouwd uit een beveiligingslaag.
- E. Er is geen beveiligingslaag voor hoog risico materiaal (denk bijvoorbeeld aan veldwerk).

B. Meerdere barrières in toegangsbeveiliging (gelaagdheid) voorkomt dat onbevoegden zomaar toegang hebben tot alle gebouwen en dus materiaal. Wanneer men door één barrière is gekomen, zijn er nog andere barrières om de onbevoegden tegen te houden. Hierbij is de aanbeveling dat de barrières andere fysieke maatregelen hebben (bv receptie voor terrein, paslezers voor gebouwen).

Bij gelaagdheid die bestaat uit 3 lagen zijn het materiaal, en minimaal 2 van de volgende gebieden beveiligd: het vitaal gebied, het beveiligd gebied of het observatiegebied. Er worden ook mensen bewust door een laag toegelaten, bijvoorbeeld in geval van een open instelling of een bezoek van een monteur. Hierbij moet minimaal het materiaal beveiligd zijn, een geautoriseerd persoon aanwezig zijn of een andere aanvullende veiligheidsmaatregel worden genomen.

Vraag 1

Vraag 2

Vraag 3

Vraag 4

Vraag 5

Vraag 6



Results and report

- Under construction
- Combination of all questions and scenarios filled in
 - Good practices
 - References
- Discussion with expert group:
 - Biosafety officers of university medical centres, knowledge institute, university laboratory
 - Regional hospitals
 - Royal Netherlands Academy of Arts and Sciences



Multiple use of the Vulnerability Scan

- Demonstrate the current biosecurity situation in the organization
- Demonstrate the gaps in biosecurity
- The results can be used for improving biosecurity
- Results can be used to convince management
- Both scenarios and questionnaires can be used to increase biosecurity awareness for employees



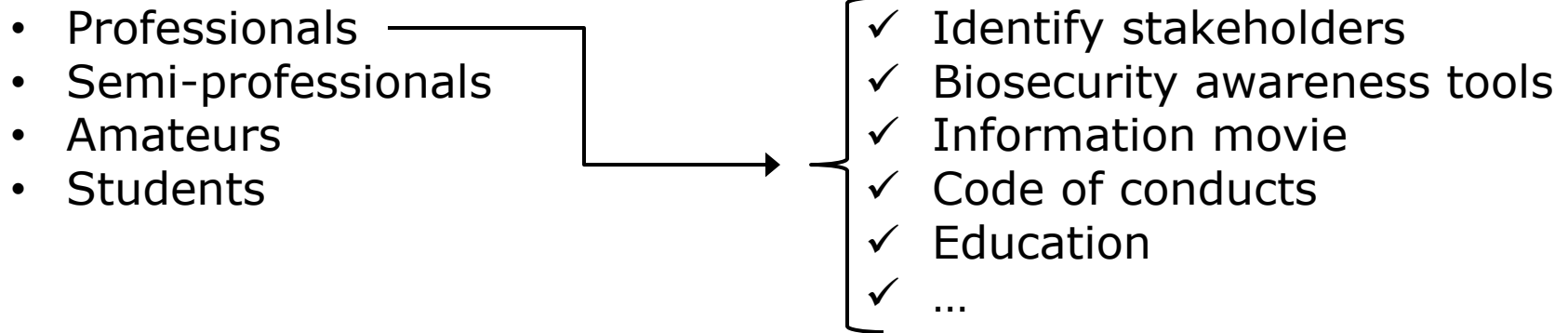
Conclusions

- Professionals showed interest in the tools:
 - Biosecurity movie
 - Self-scan toolkit
- There is need for a more practical tool (e.g. Vulnerability Scan)
- The biosecurity movie and biosecurity tools are developed to increase awareness for professionals
- To increase awareness for iGEM or DIY biology these tools need to be adapted for better connection to their situation and activities





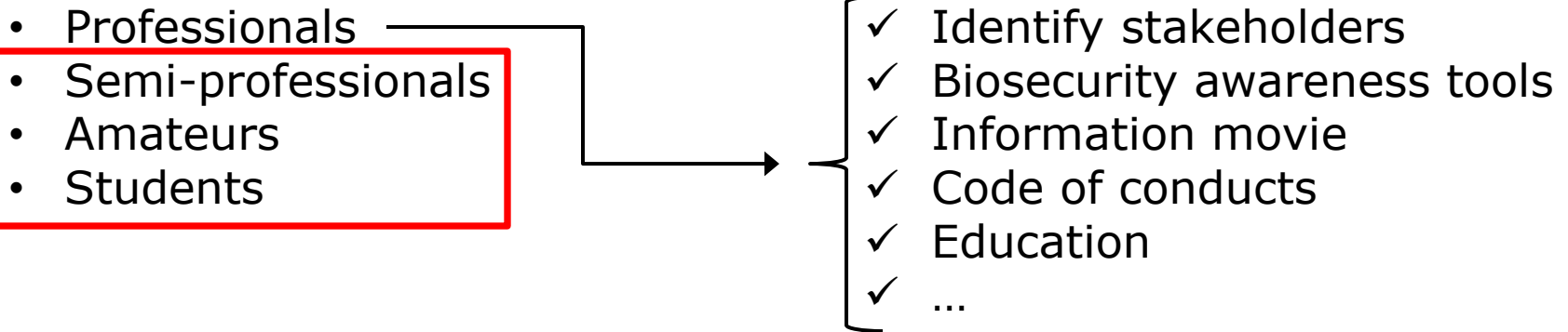
Conclusions



Biosecurity awareness raising not only important for professionals, but also for semi-professionals, DIY biology and iGEM community, students and other interested amateurs



Discussion



- How to identify your stakeholders?
- How to reach your stakeholders?
- How to increase biosecurity awareness?
- Do we need to develop code of conducts?
- Are the tools developed by Biosecurity Office useful?
- Are other tools needed to increase awareness?



Contact & Questions

www.bureaubiosecurity.nl
www.biosecuritytoolkit.com

biosecurity@rivm.nl

 @B_Biosecurity

