
27th ANNUAL
FIRST
CONFERENCE
BERLIN
14-19 JUNE 2015
UNIFIED SECURITY:
IMPROVING THE FUTURE

Yet another story on information sharing...

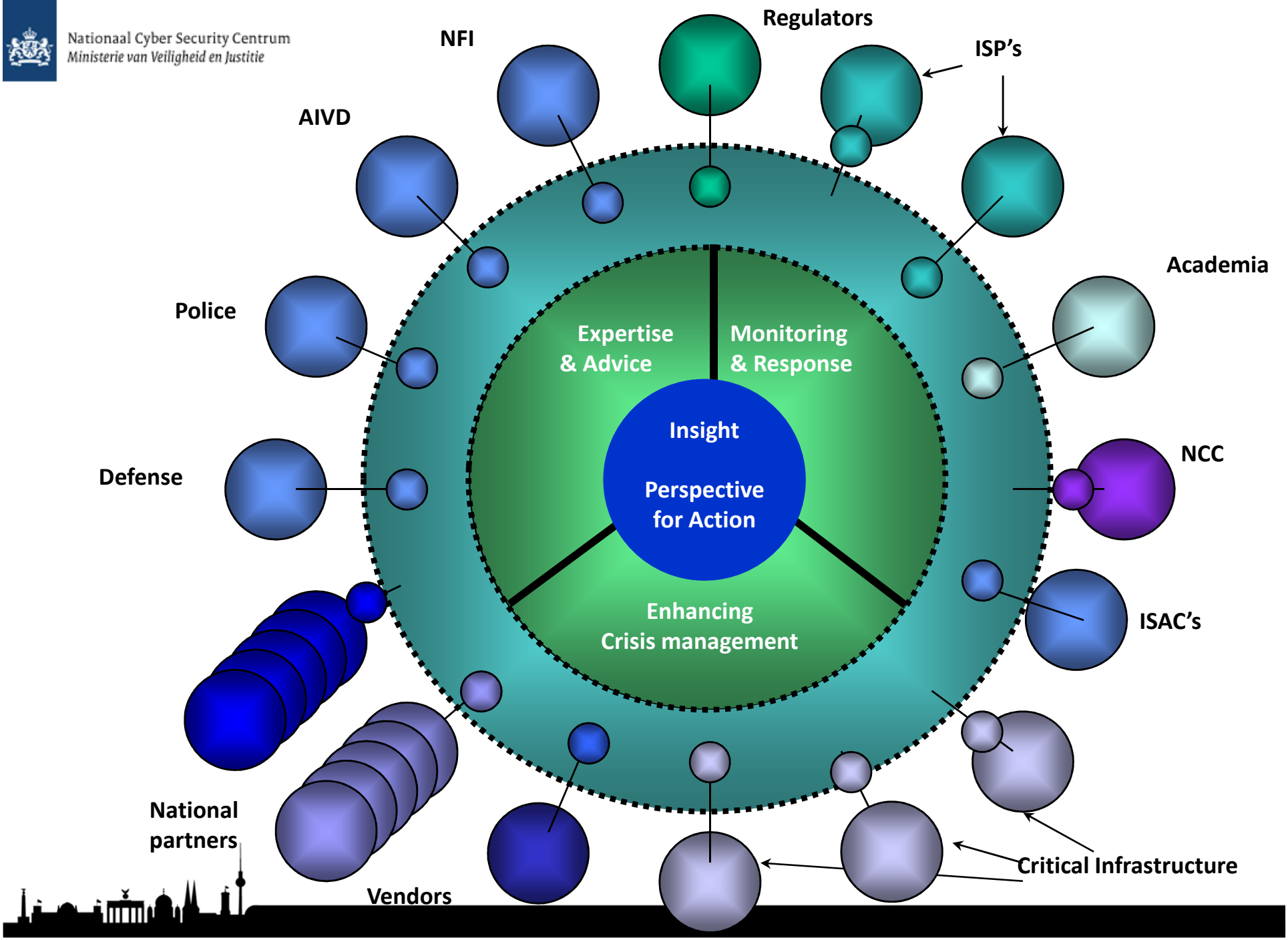
- NATO *Malware Information Sharing Platform*
- Panel discussion *Threat information sharing: Strategies and threat Scenario's*
- George Mason University *Barriers and pathways to improving effectiveness of cybersecurity Information Sharing Among Public and Private Sectors*
- *…*

Case study on improving shared situational awareness by focusing on community building

- ✓ Situational Awareness as is
- ✓ Why we saw cause for action
- ✓ The NDN initiative
- ✓ Steps in community building

michael.meijerink@NCSC..nl

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie



NCSC-NL situational awareness

Tactical	• News analysis • ***Daily weather report***	• Tactical analysis • Monthly monitor • Guidelines • Factsheets • White papers • Media analysis • Policy briefings	• One conference • Trend report • End of year
Operational	• Advisories	• Malware analysis • End of week • Ad hoc • ***Observables and context***	• One conference
	Daily		***Yearly***

2012 Dorifel

August 8th

- We receive first calls
- Requests for advice
- Municipality of Weert
- Malware sample
- Indicators sharing
- Actionability

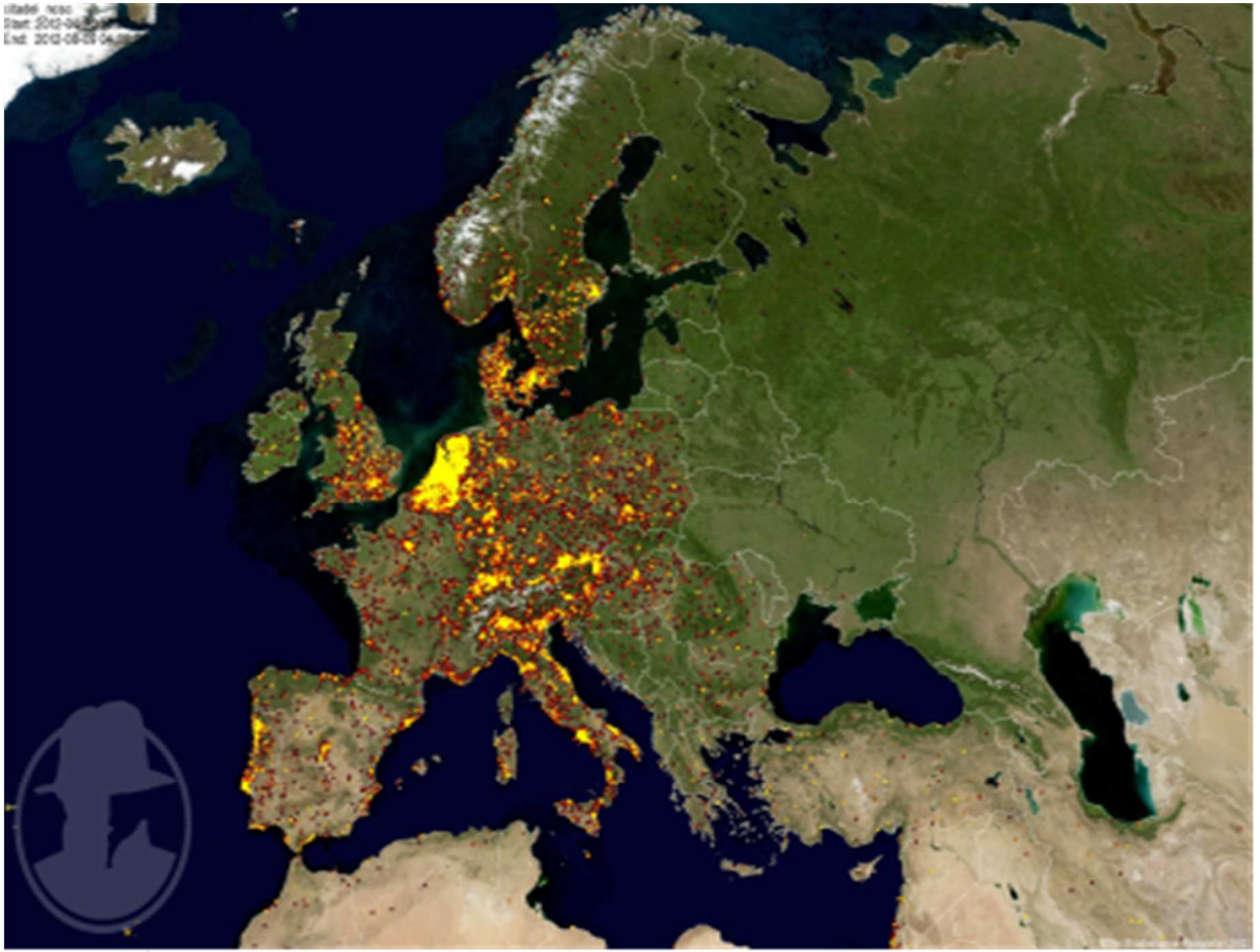
2012 Dorifel

August 9th

- New reported infections
- Notice and Takedowns
- ‘Release me of a botnet’

August 10th

- Total of 30 public and private organizations
- Scaled down
- Clean up still ongoing



https://www.shadowserver.org

2012 Dorifel Evaluation

Shortcomings

- No early warning
- No access to the networks
- No use of standards
- No feedback on indicators
- No community driven approach
- And thus ...no actual shared situational awareness

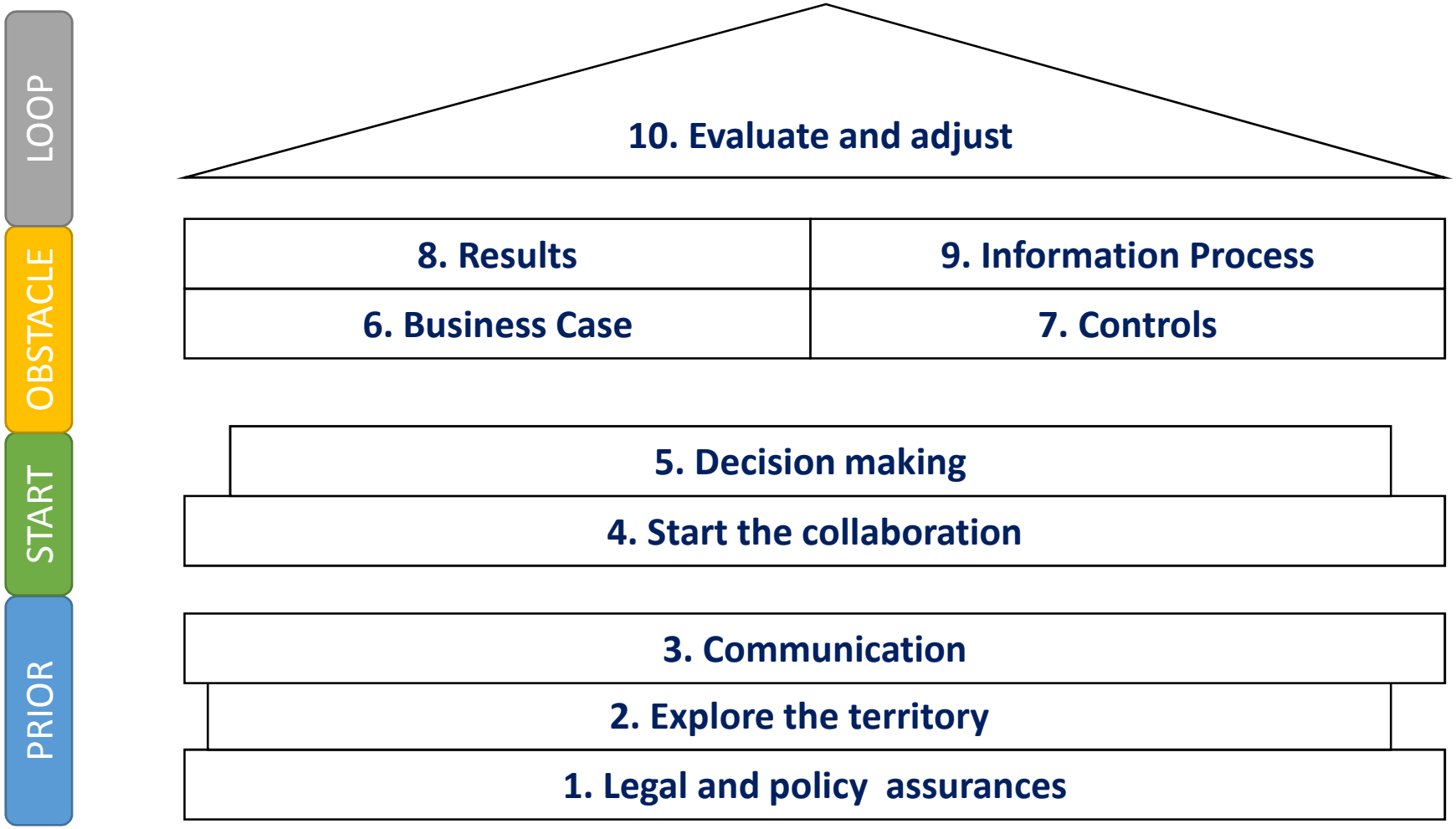
2015: National Detection Network

NDN offers

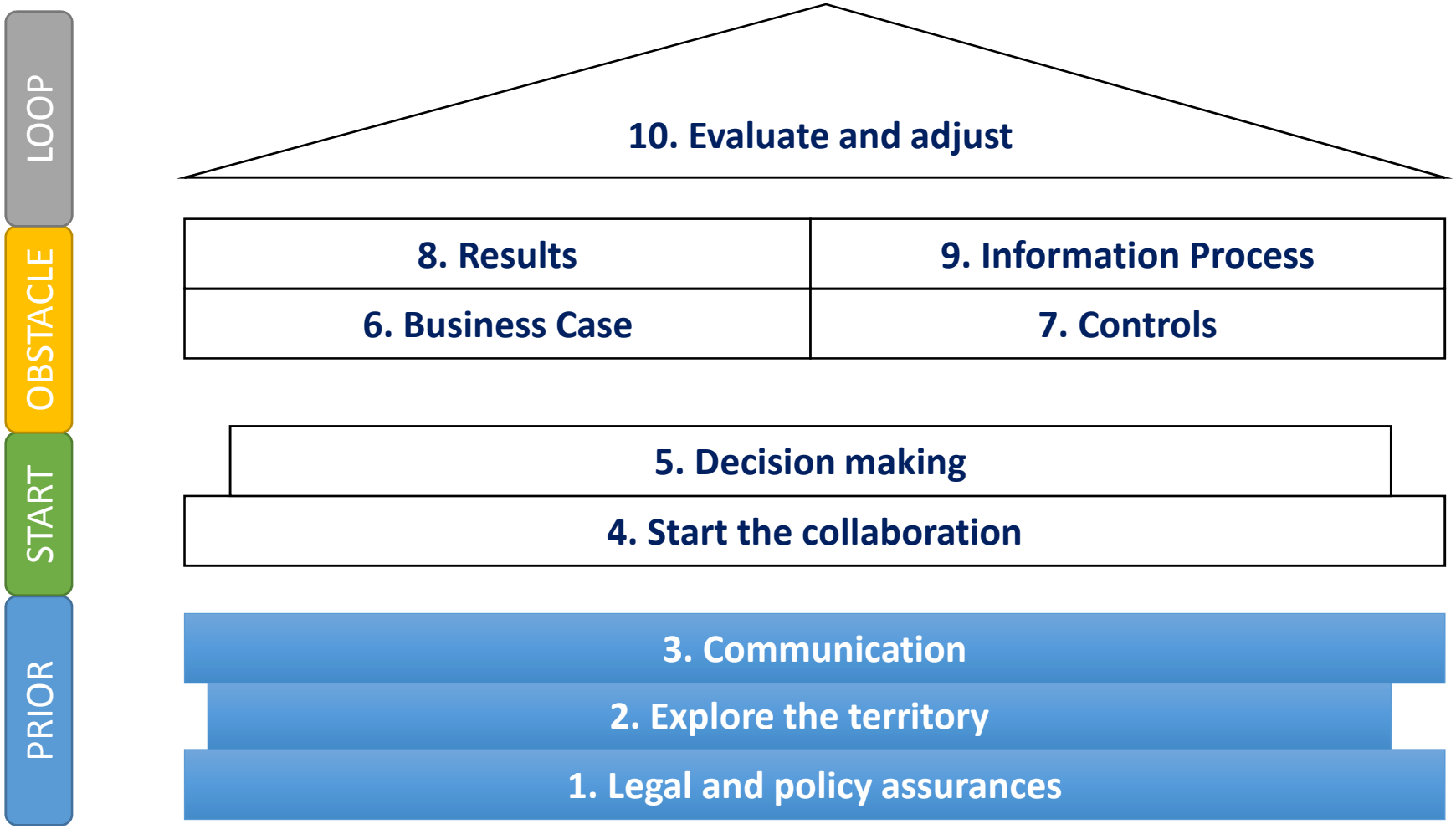
1. An IDS for government organisations
2. Threat intel data not (yet) widely available
3. Targeted at NL, high impact, high likelihood
4. Platform for private sectors in critical infrastructure
5. Use of standards and open source
6. Based on voluntary sharing with NCSC-NL
7. Available to all of our constituency

Topics dealt with

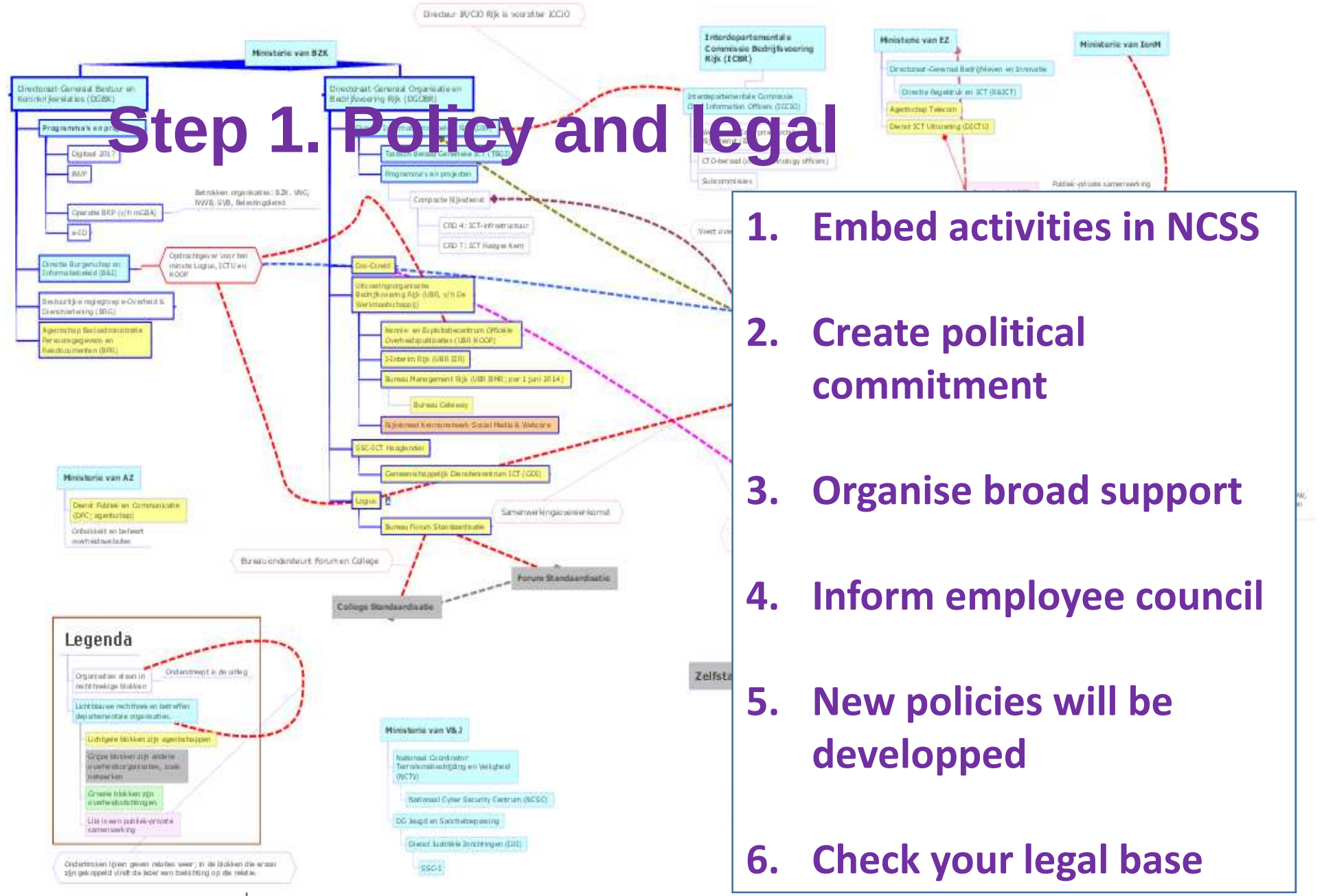
10 Steps in community building



Steps in community building



Step 1. Policy and legal



1. Embed activities in NCSS
2. Create political commitment
3. Organise broad support
4. Inform employee council
5. New policies will be developped
6. Check your legal base

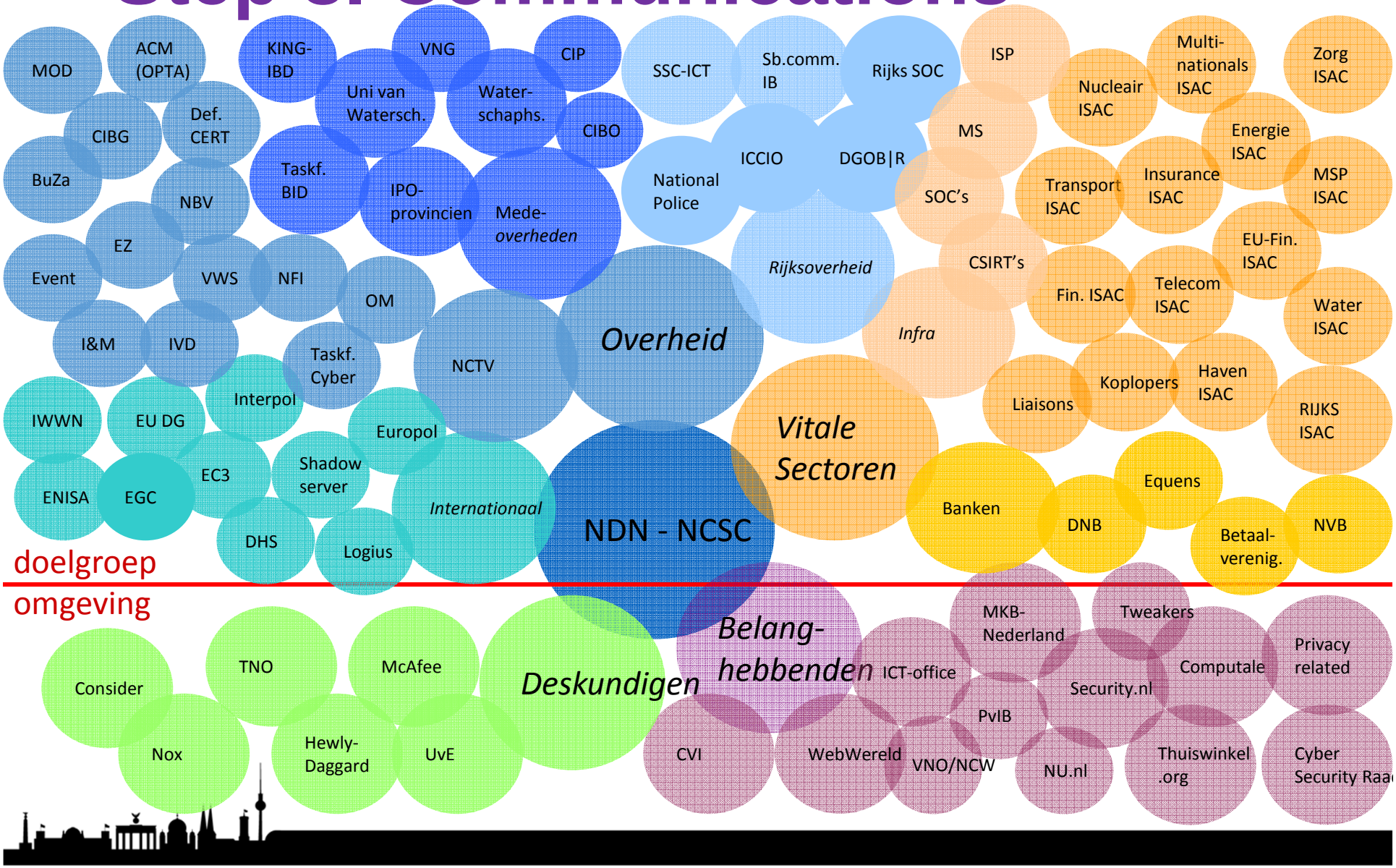
Step 2. Exploring the teritory

- Information
- Trust level
- Volume
- Sharing molde
- Benefit
- Authority
- Exchange base
- Size
- Lenght
- Connectednes
- Diversity
- ...

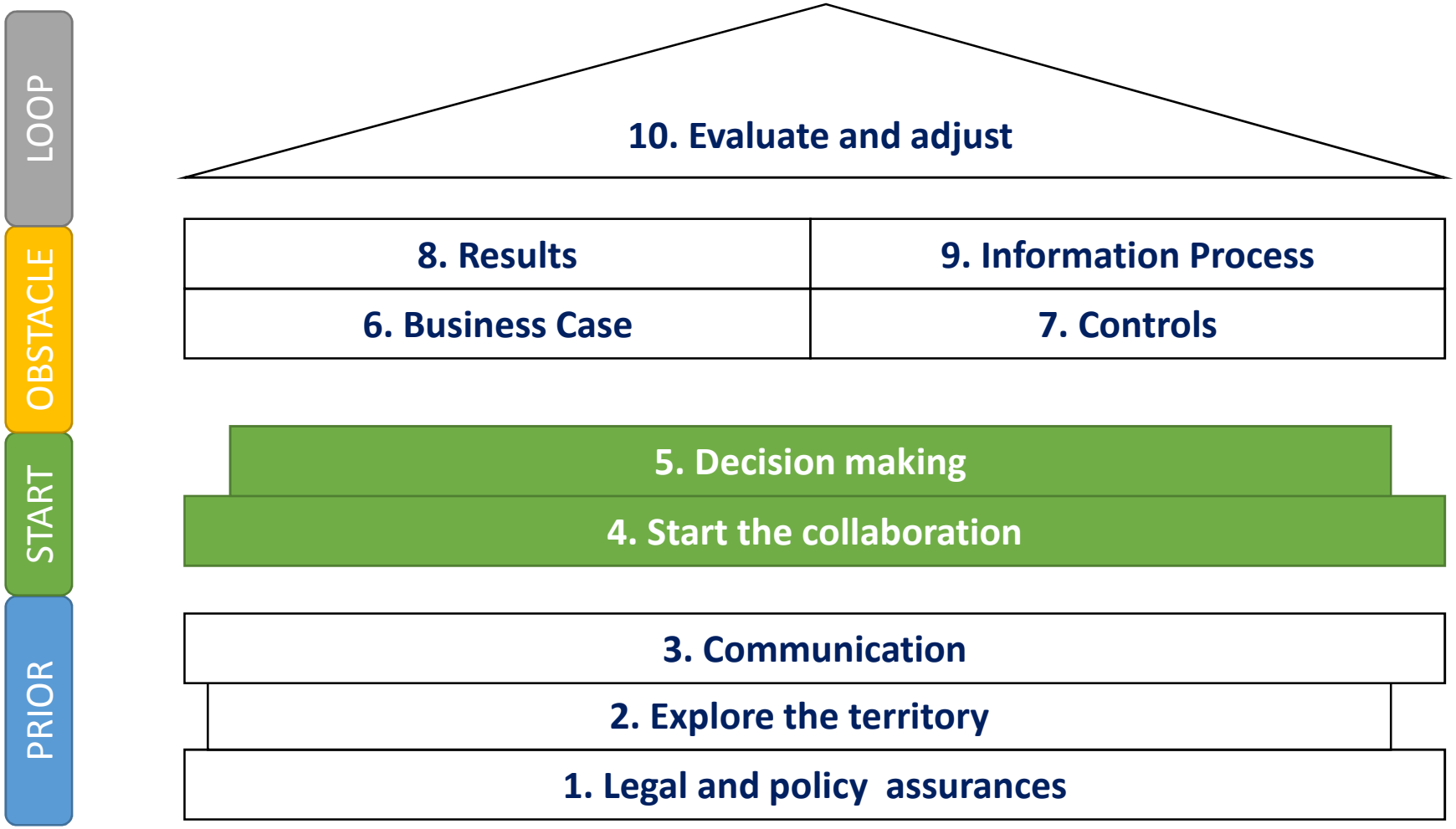
Step 2. Exploring the teritory

information	open	closed	
trust level	not present	informal	formal
volume	low	medium	high
sharing model	hub-spoke	peer-peer	hybrid
benefit	low	medium	high
authority	public	private	supervisory
exchange base	voluntary	mandatory	
size	limited	medium	large
lenght	ad hoc	long term	
connectedness	weak	strong	bridging
diversity	low	medium	high

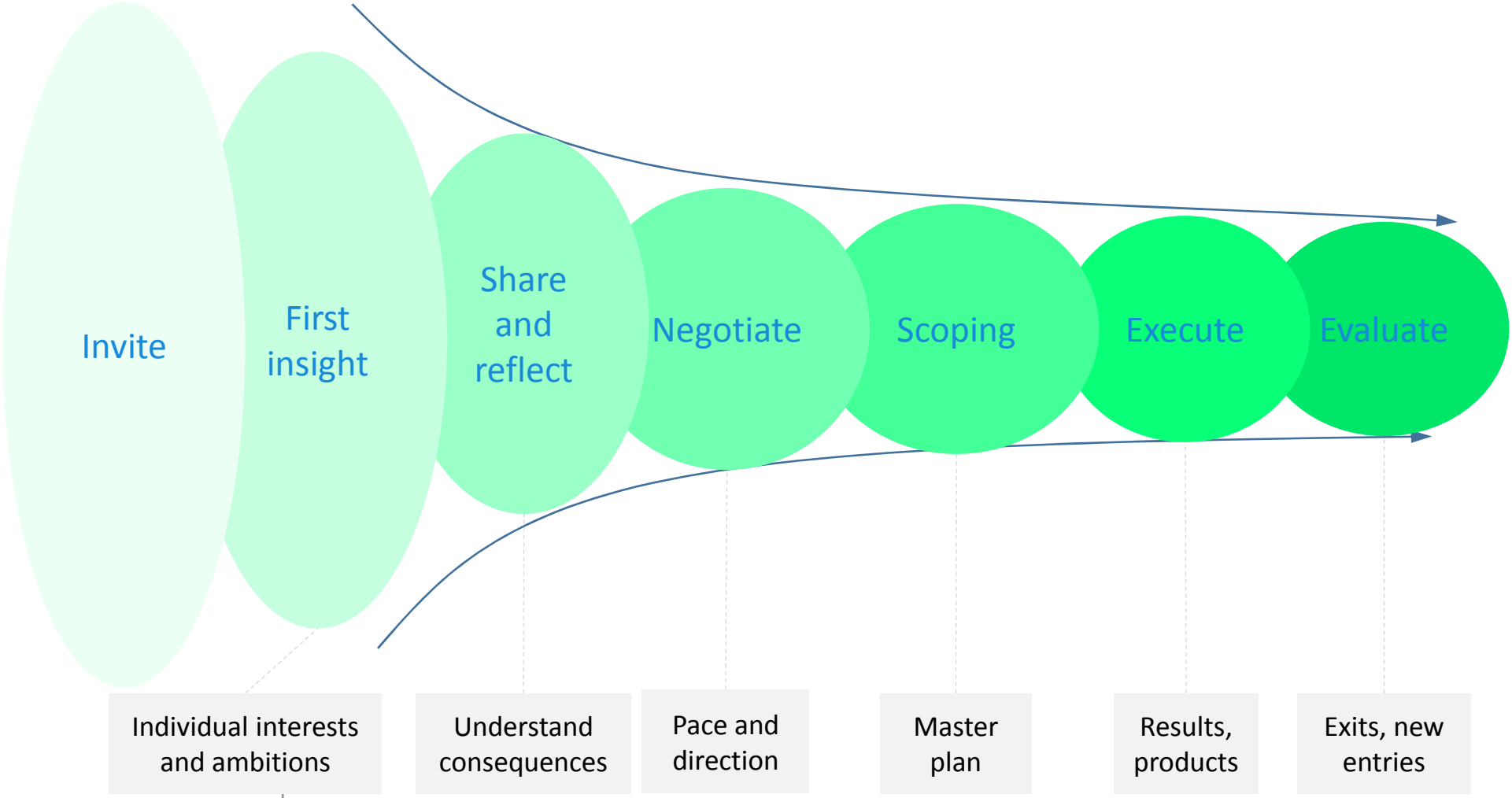
Step 3. Communications



Steps in community building



Step 4. Collaboration process



Leren samenwerken tussen organisaties, allianties netwerken ketens partnerships, Kaats, Pheij, 2013

Stages	Period	Activities
1 Invite	May-Nov ’13	- Representative organizations - Delegates
2 First insight	Dec ’13	- Round table sessions - Introductions - Proposition: benefits, challenges
3 Share and reflect	Feb ’14	- Interests made explicit - Implicit a group was made
4 Negotiate	Mar, Jun ’14	- Agenda - Roles, responsibilities
5 Scoping	Jun-Nov ’14	- Process, organization, information, infrastructure, legal, policy, communication
6 Execute	Dec ’14	- Start pilot: infrastructure, sharing
7 Evaluate	Jun-Sep ’15	- Roadmap, growth scenario, sharing proces

Private sectors only

Step 5. Decision making

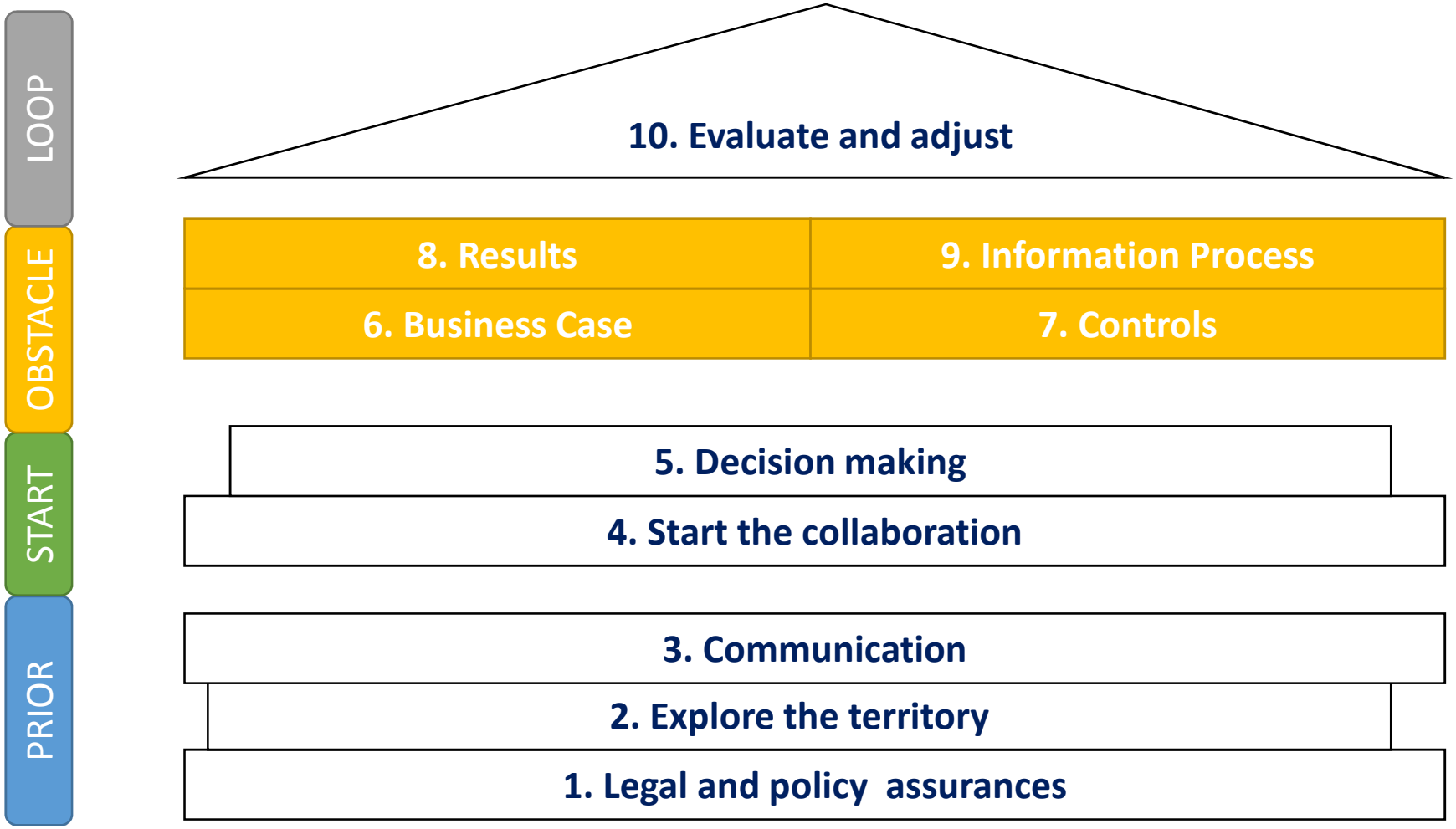
Stakeholders
- 150 corporate organizations
- 20 public organizations
- 3 founding partners
- ? Managed service providers

Structure
- 1 steering group, 2-monthly
- Senior management
- Sounding board
- Round table

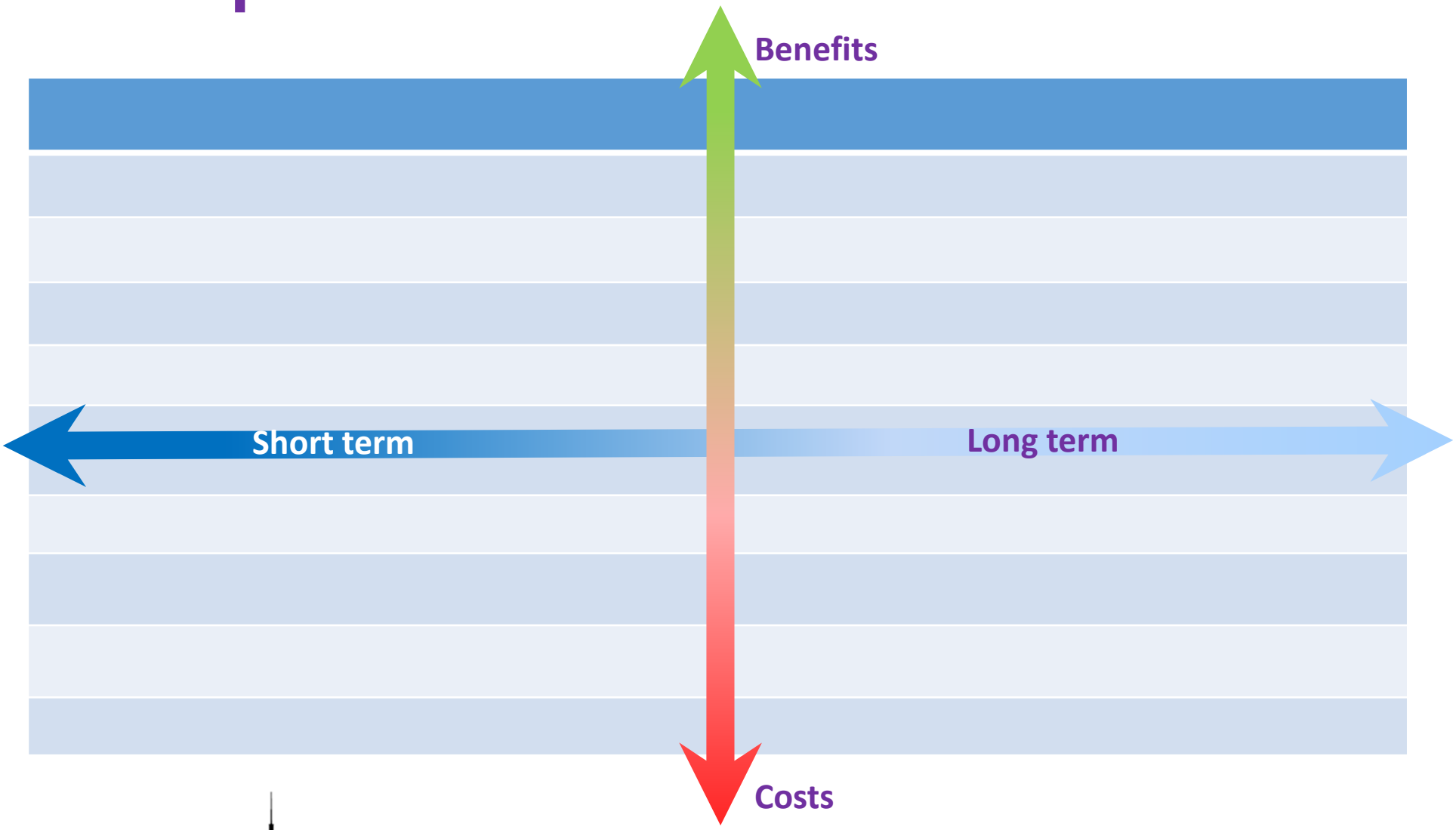
Topics
- Project and pilots
- Policy, legal and politics
- Finance and resources
- Communication

Results
- Consensus
- Political support
- Stakeholder collaboration
- Autonomy untouched
- Missing: MSSP, researchers, interest groups, ...

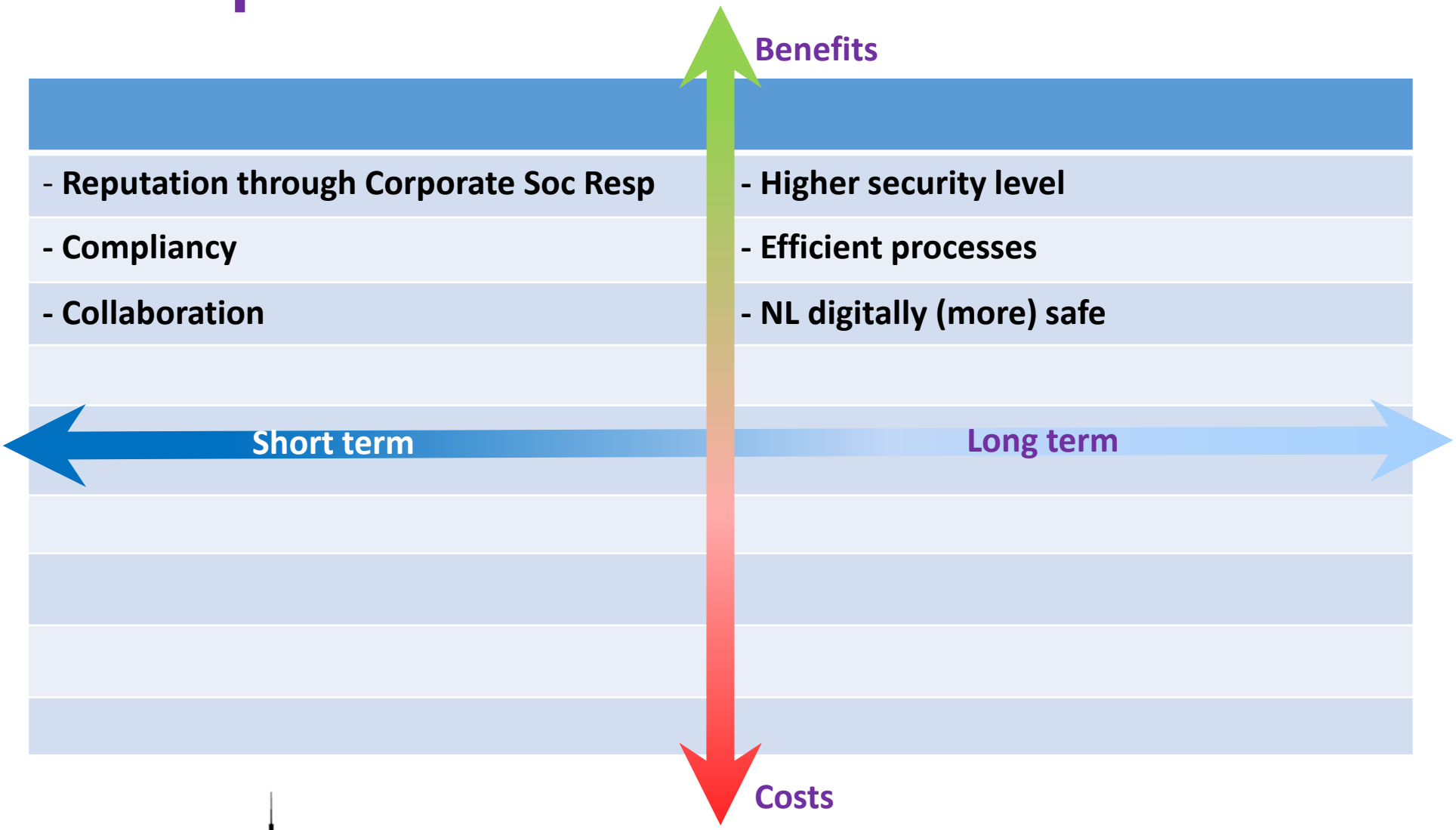
Steps in community building



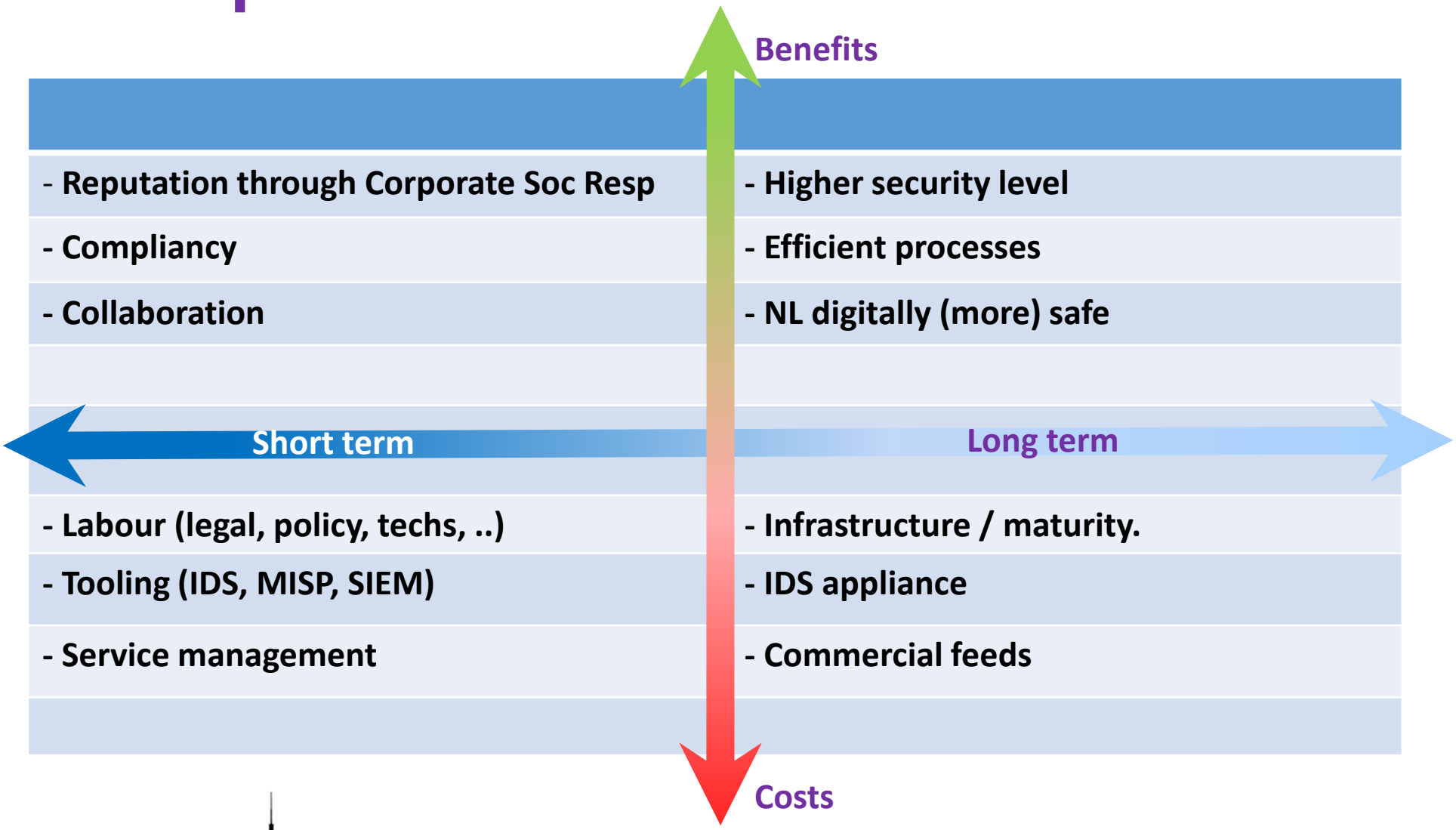
Step 6. Costs and benefits



Step 6. Costs and benefits



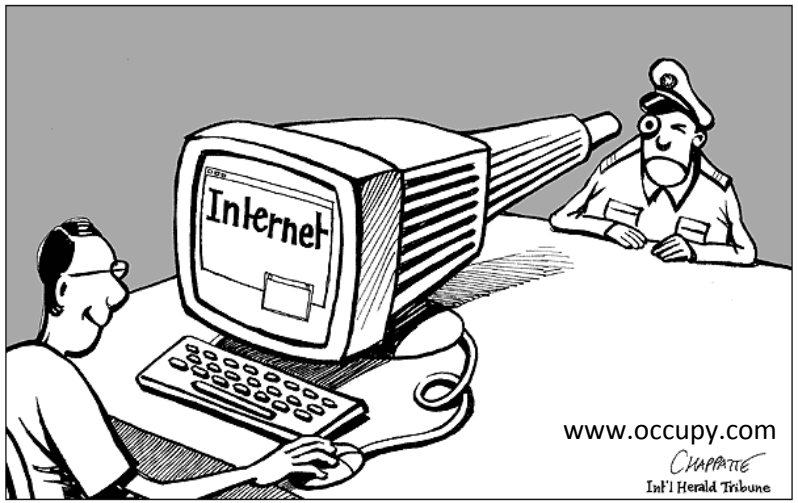
Step 6. Costs and benefits



Step 7. Information controls

Privacy controls (public IDS)

- Raw data only locally
- No IoC's on personal identifable information
- IP addresses hashed and salted
- Retention time <30 days
- Hits after 30 minute delay
- White box solution
- No remote management



Step 7. Information controls

Privacy controls in process and organization

- Describe the working process
- Protocols in place that describe how to handle
- Perform a privacy impact assessment
- Processes are externaly audited
- Keep checking on compliancy with legislation and policies
- Only screened personnel handle data

Step 7. Information controls

Sharing controls (private sector)

Public access and access from supervising authorities to government information

- Describe the working process
- Retention times on IoC's, sightings,...
- Policy statement, law amendment

TLP Amber, confidential or secret

- MSSP's, international branches
- Research e.g. Blooming filter
- Transparency in processing, (NDA's)

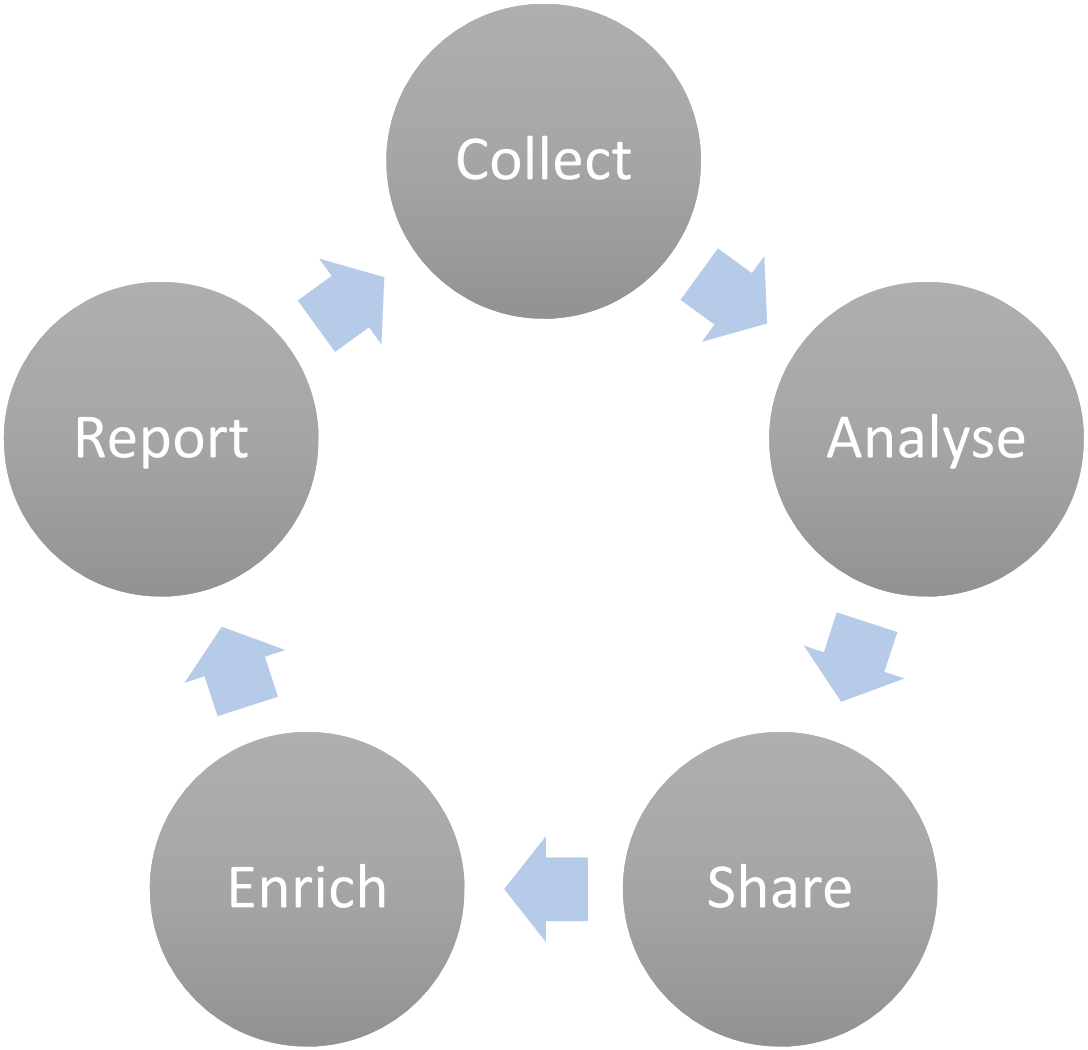
Step 8. Results

- Span, location, availability
- Bandwidth, performance
- Skill level
- Contextual information
- (Too) high expectations
- Remote access
- New friends

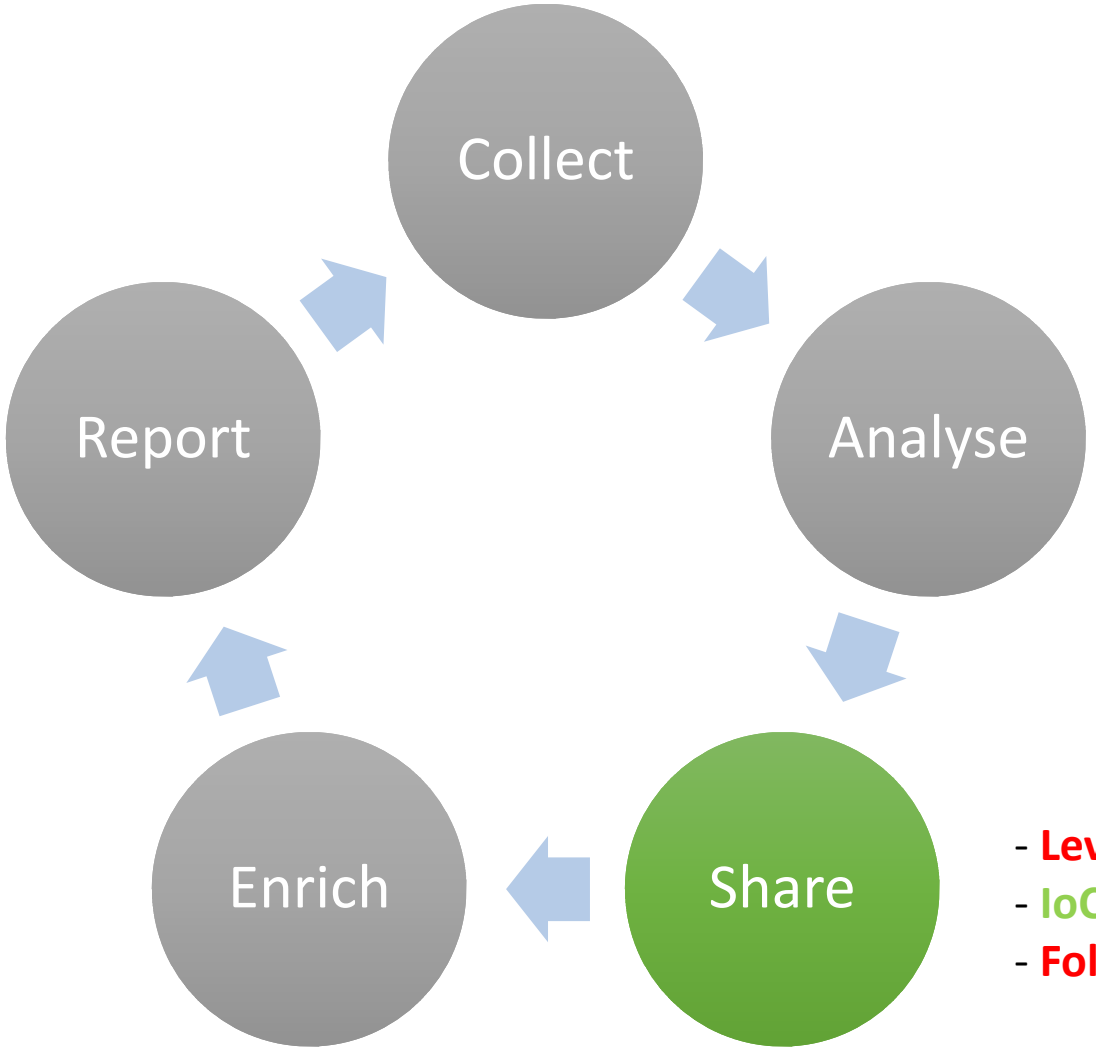
- MISP Forum
- MISP community driven
- MISP STIX
- MISP groups
- Government syndrom
- Data retention
- New friends

various pics via www.google.com

Step 9. Collect & share

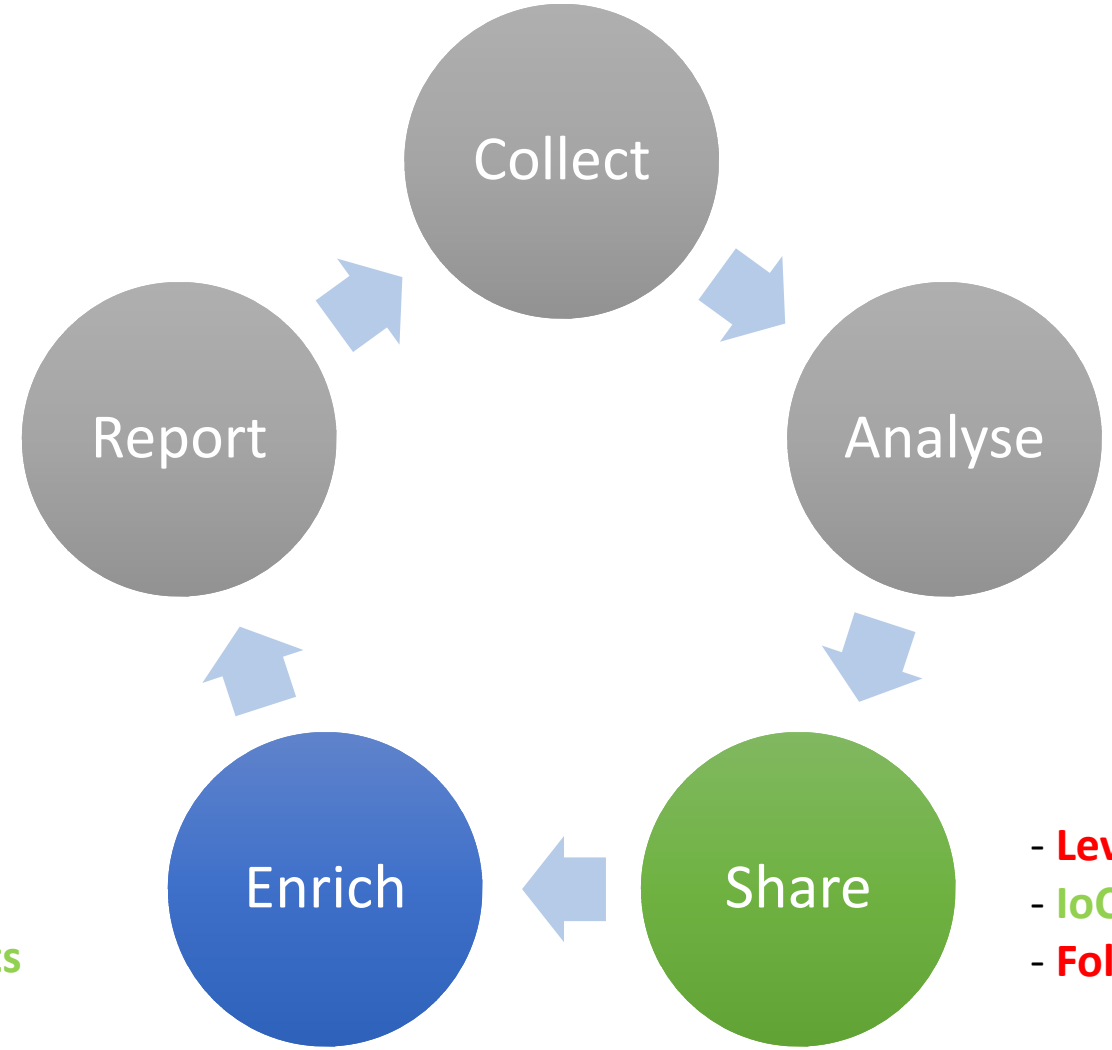


Step 9. Collect & share



- **Levels of sharing**
- **IoC's received**
- **Follow up**

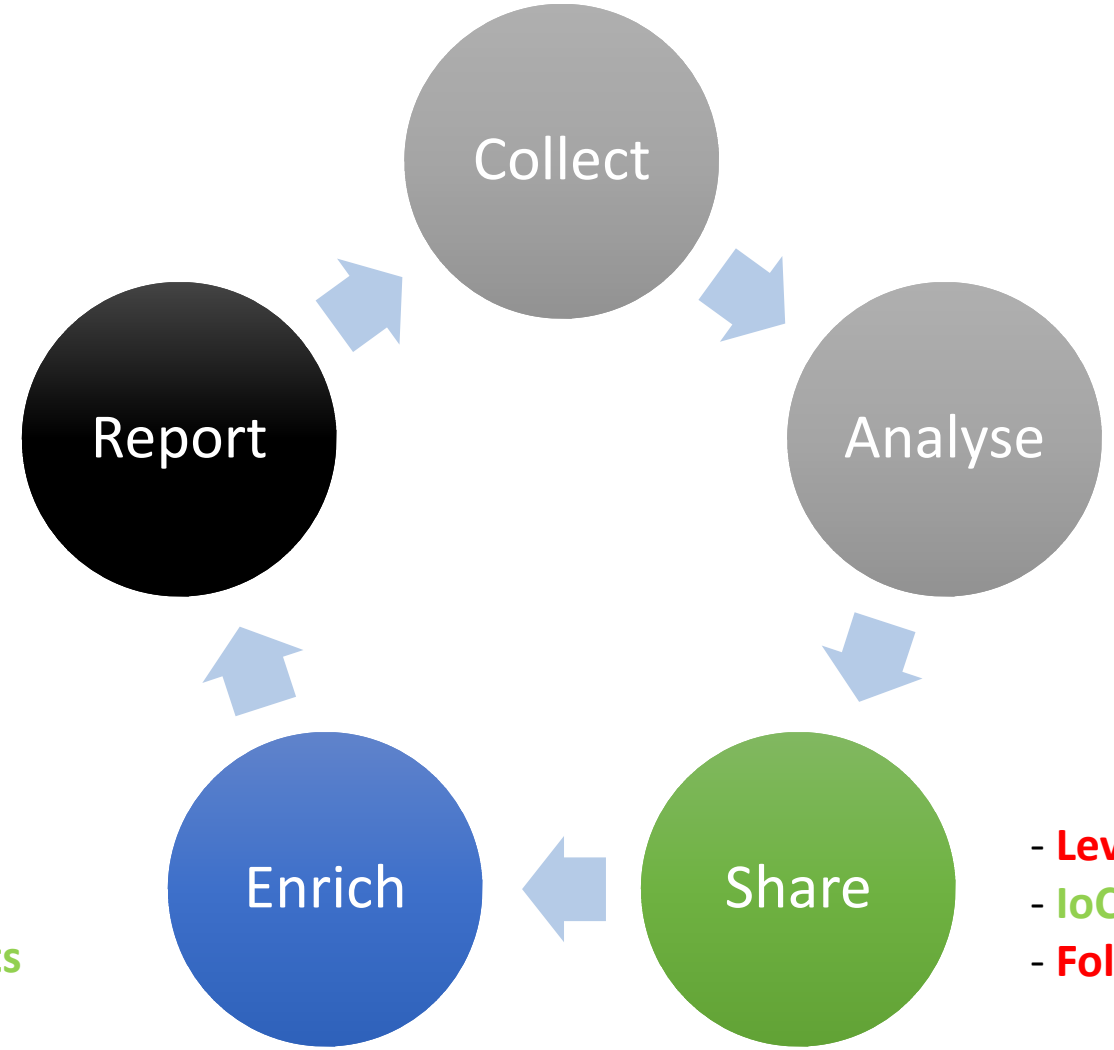
Step 9. Collect & share



- **Sightings**
- **Statistics**
- **Comments**

- **Levels of sharing**
- **IoC's received**
- **Follow up**

Step 9. Collect & share

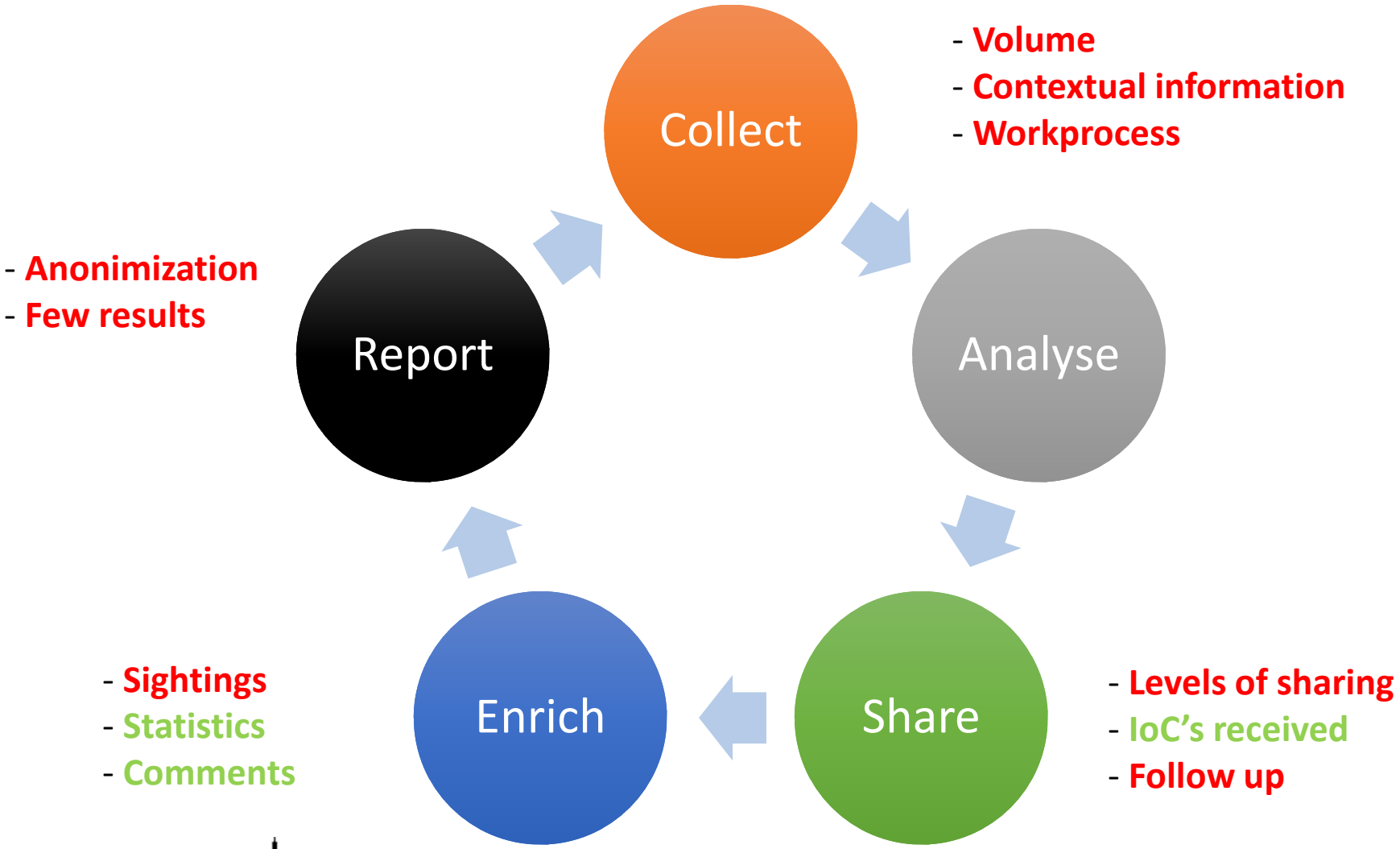


- **Anonimization**
- **Few results**

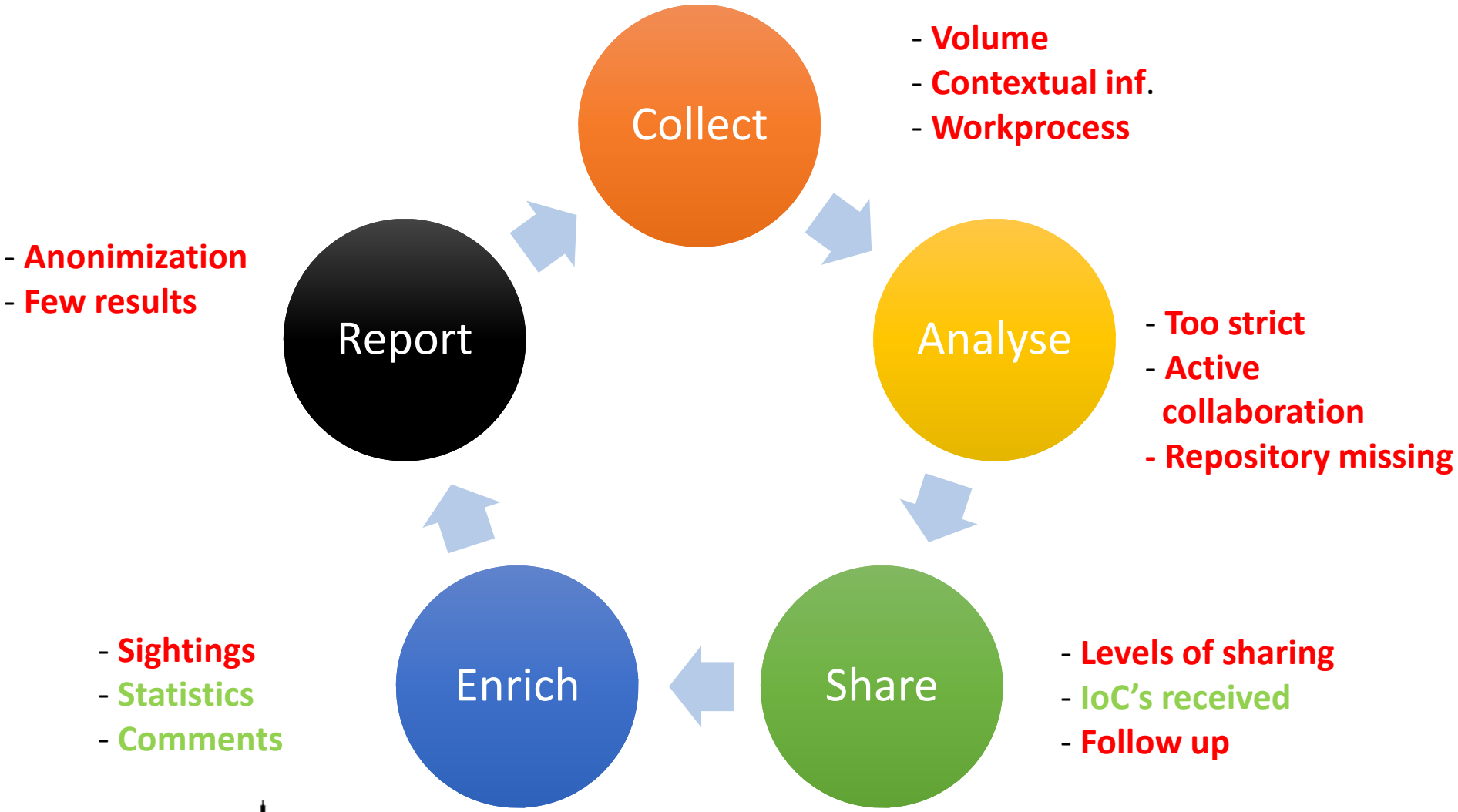
- **Sightings**
- **Statistics**
- **Comments**

- **Levels of sharing**
- **IoC's received**
- **Follow up**

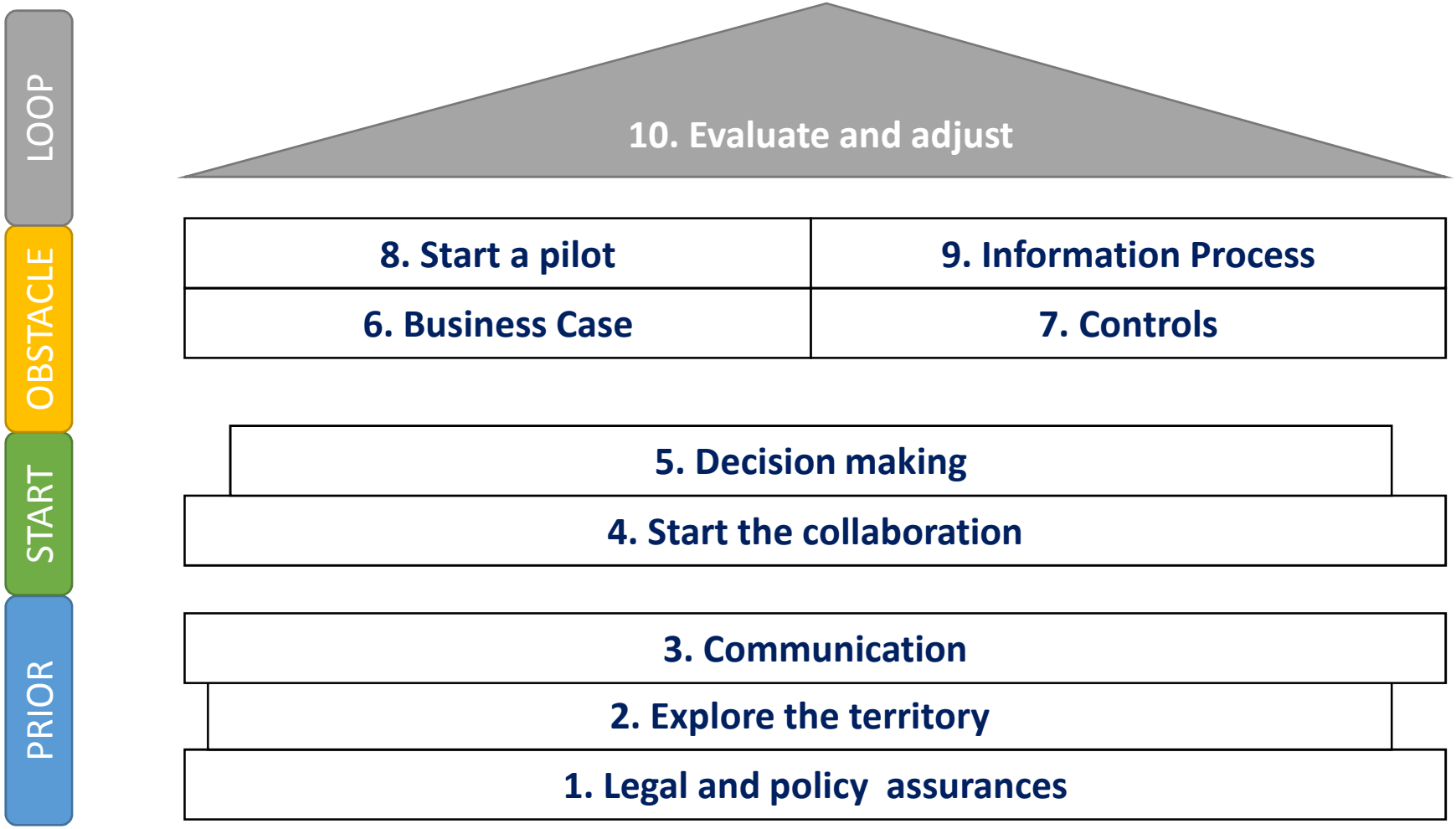
Step 9. Collect & share



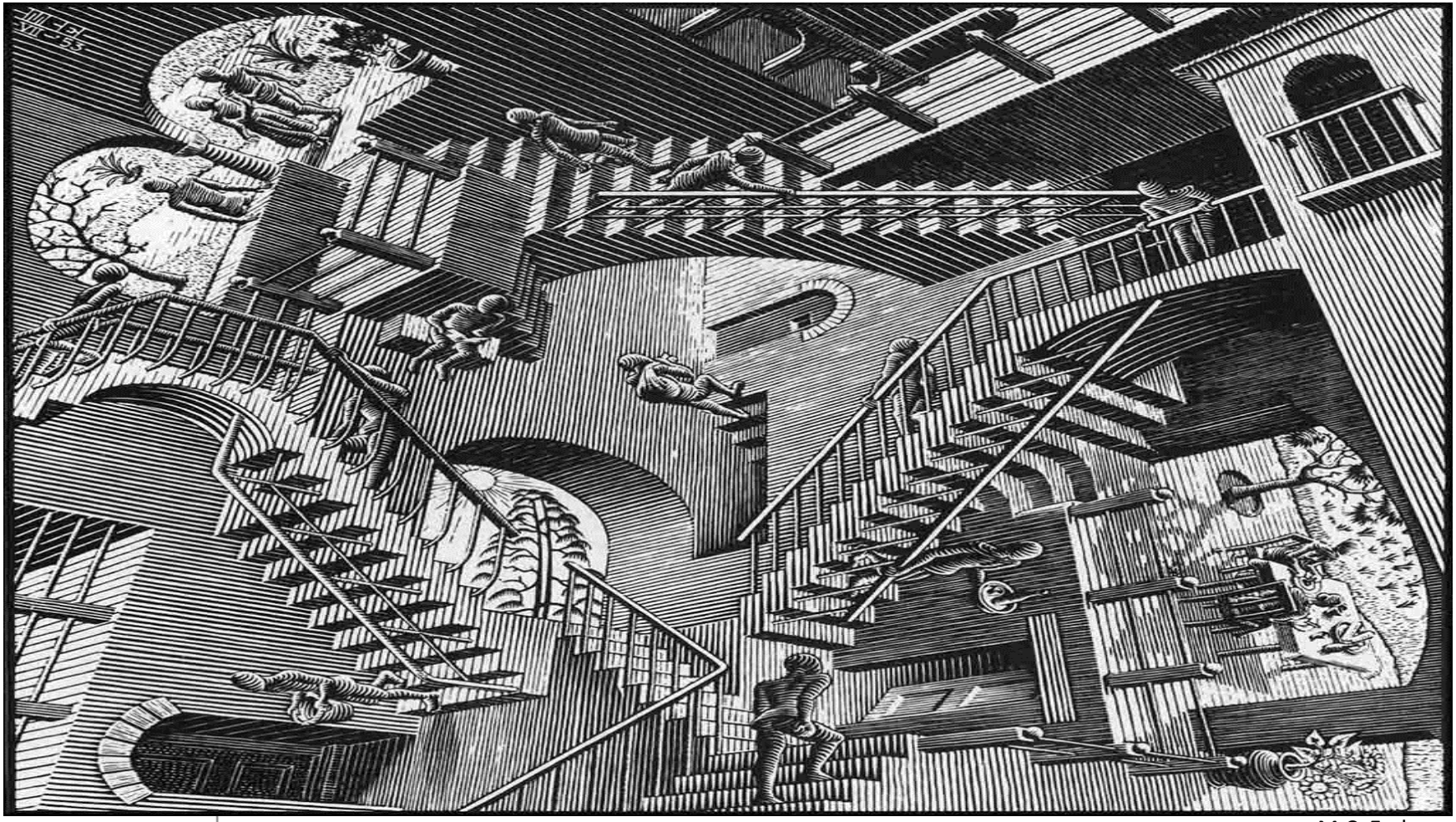
Step 9. Collect & share



Steps in community building



10. Continuous improvement



M.C. Escher

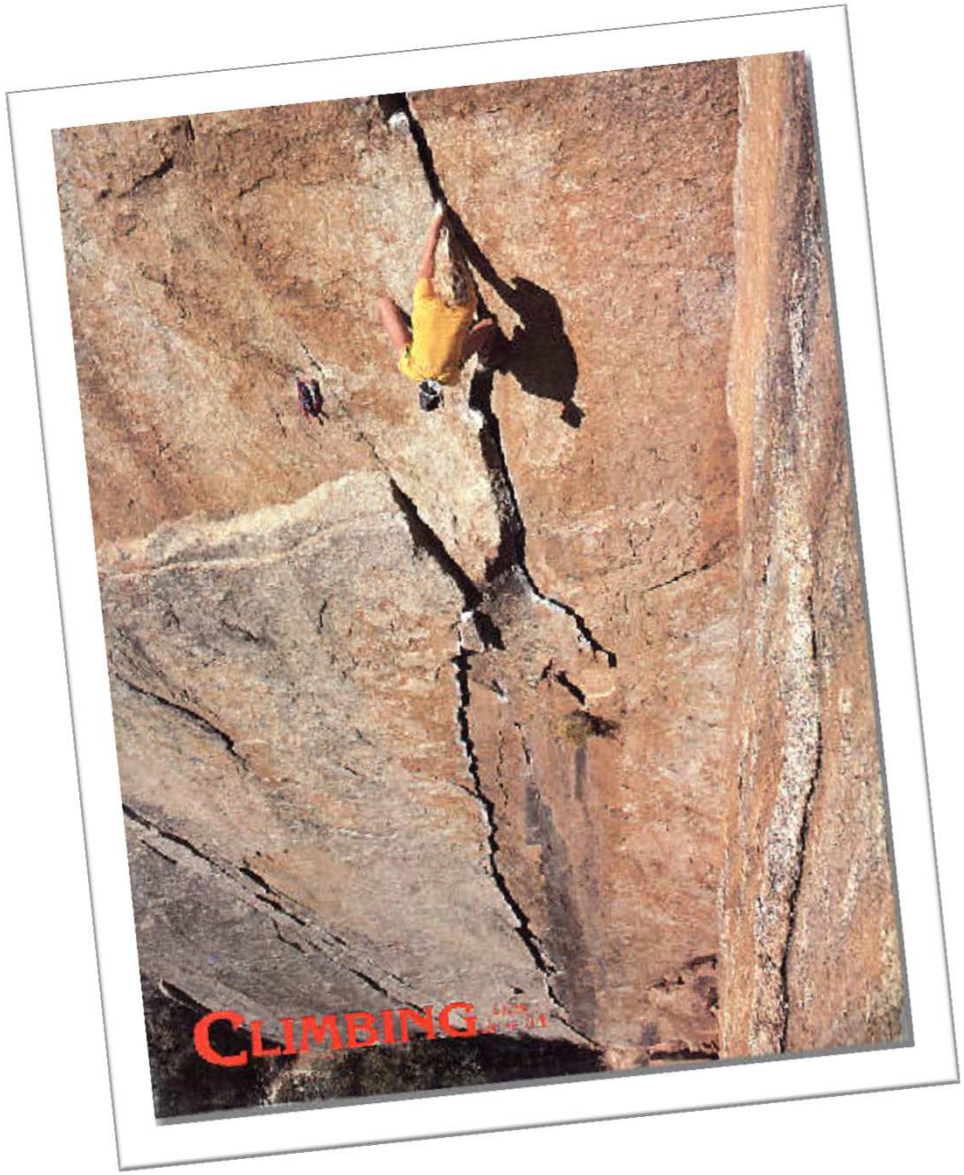
To conclude

Preparations

- Results
- Involvement

Collaboration

- Takes endurance
- Very intensive
- Trust issues reduced



http://www.tortoiseknowsbest.com/john-bachar-%E2%80%93-a-true-slow-hero/

To conclude

Obstacles

- Controls: transparency sources/ncsc/private
- Process: make a good inventory
- ROI: first insights, hard to put $/€/¥/£ to it
- Results: start small, make it work

Improvement

- Other practices, tooling, disciplines, industries

maps.google.com

This presentation is based on our own experiences as well as others:

- Electrotechnik und informationstechnik, Cyber security information exchange to gain insight into the effects, 2015
- http://link.springer.com/article/10.1007%2Fs00502-015-0289-2
- NCSC, Ahead of the threat, enhancing cyber intelligence communities, 2015
- https://www.ncsc.nl/actueel/nieuwsberichten/ncsc-levert-bijdrage-aan-european-cyber-security-perspectives-2015.html
- Microsoft, a framework for cyber security information sharing and risk reduction, 2015
- http://www.microsoft.com/en-us/download/details.aspx?id=45516
- Nist, Guide to Cyber Threat Information Sharing, 2014
- http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf
- EP, Mass surveillance, part 2, 2015
- http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527410/EPRS_STU%282015%29527410_REV1_EN.pdf
- EP, Network and Information Security (NIS) Directive, 2015
- http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive
- MISP, main developers Belgian Defence and Nato
- https://github.com/MISP/MISP