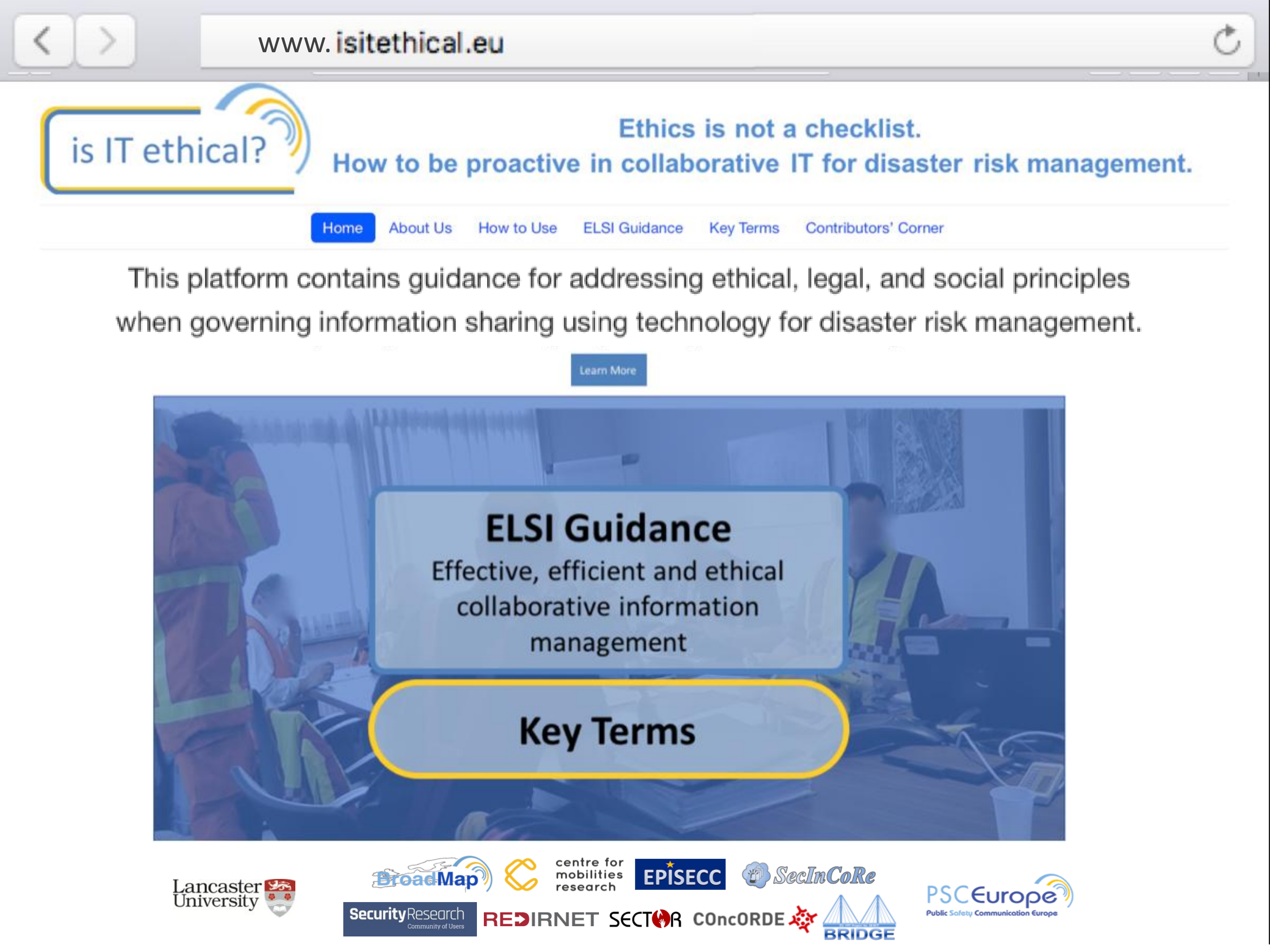


Ethics is not a checklist.

How to be proactive in collaborative IT for disaster risk management.

This platform contains guidance for addressing ethical, legal, and social principles when governing information sharing using technology for disaster risk management.

ELSI Guidance

Effective, efficient and ethical collaborative information management is IT ethical?

www.isITethical.eu

Motivation
Overview
Invitation

enisa

European Network and Information Security Agency

Emergency Communications Stocktaking

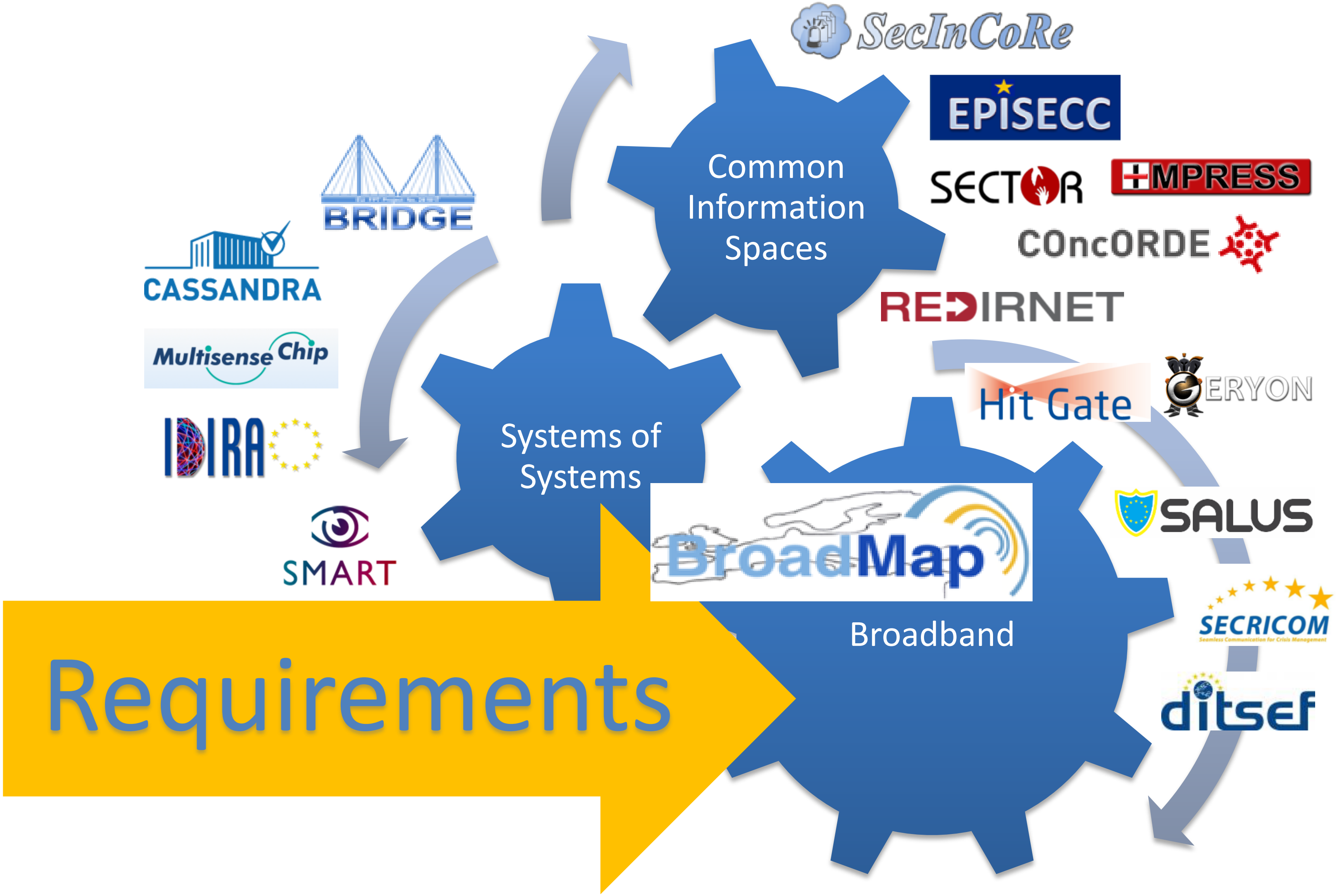
A study into Emergency Communications Procedures

https://www.enisa.europa.eu/publications/emergency-communications-stocktaking

Lack of interoperability between first responders and communication problems are the most common findings in post-crisis lessons learned exercises. ENISA 2012

PA

It was apparent that in some parts of the emergency response, the requirements of the Data Protection Act 1998 were either misinterpreted or over-zealously applied. … the London experience in this respect is not unique. (Hilary Armstrong, UK Cabinet Minister for Social Exclusion, after the London 7/7 bombings in 2005, Armstrong, Ashton & Thomas, 2007)

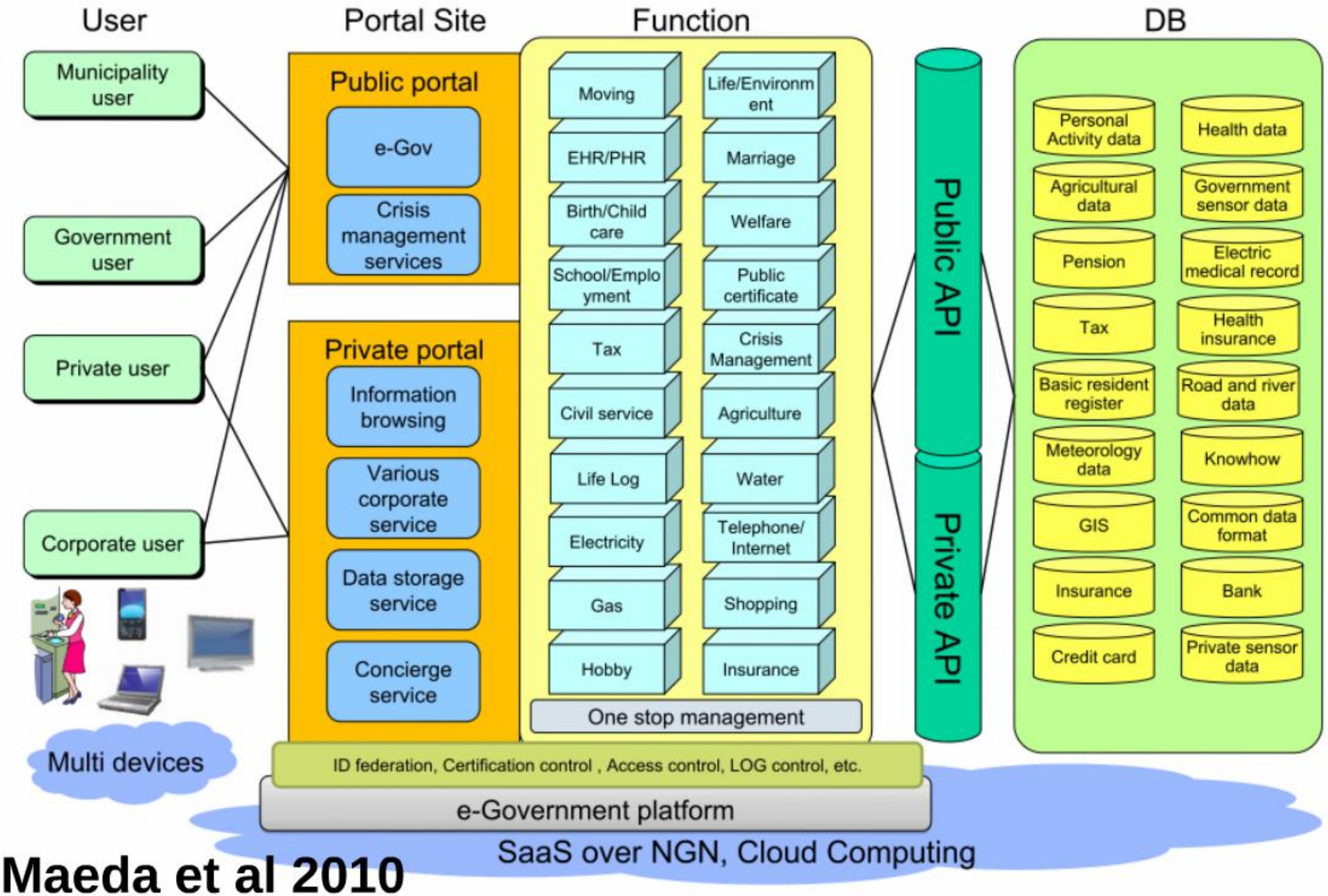


Common Information Spaces

Systems of Systems

Broadband

Requirements



Maeda et al 2010

Fig. 5. Realization image of resilient society by ICT systems.

Society and European Values

- Effects of not sharing
- Not just more sharing, but *better* sharing
- Exceptions – When? Start/stop? Who has access? Whose data?
- New Partnerships
- Trust
- Translation
- Civil liberties

Social Contract

BODY-WORN VIDEO

A report by Greater Manchester's
Independent Police Ethics Committee

- What impact would continuous use have on police officers? Would it be an intrusion and additional pressure? Does it support them against allegations, reduce likelihood of allegations?
- What impact does BWV have on police behaviour?
- What impact does it have on relations with the public? Could it create a barrier?

is IT ethical?

Resources

ICRC

‘Managing sensitive protection information’ of Professional standards for Protection Work (2013)

General Data Protection Regulation

Association for Computing Machinery
Advancing Computing as a Science & Profession

Code of Ethics and Professional Conduct

International Federation
of Red Cross and Red Crescent Societies

EUR-OPA
EUR-OPA MAJOR HAZARDS AGREEMENT
ACCORD EUR-OPA RISQUES MAJEURS

SATORI

EDPS

HM Government

Data Protection and Sharing Guidance for Emergency Planners and Responders

- **Practice**
- **Scholarship – observations & literature review**
- **Ethical Impact Assessment**

cen CENELEC

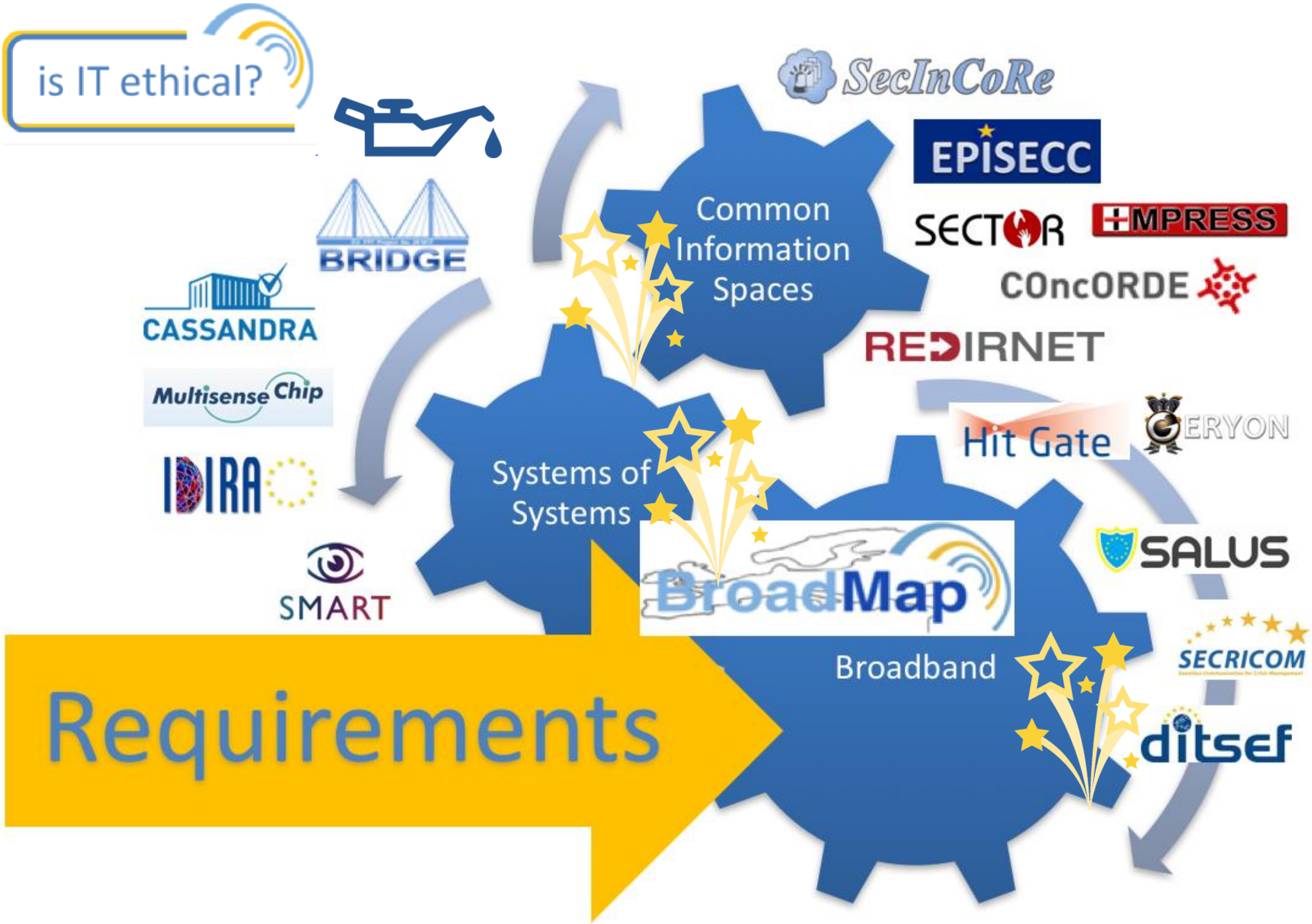
ETSI
World Class Standards

3GPP
A GLOBAL INITIATIVE

the law needs to catch up with technological innovation (Expert at BSSAR 2015)

Data protection legislation … provides a framework where personal data can be used with confidence that individuals' privacy rights are respected (Armstrong et al 2007)

… when I am designing my CIS …, I would read the entire Guidance and cross check what I have in my head and check if I am missing something. (Toni Staykova, ConCORDE)



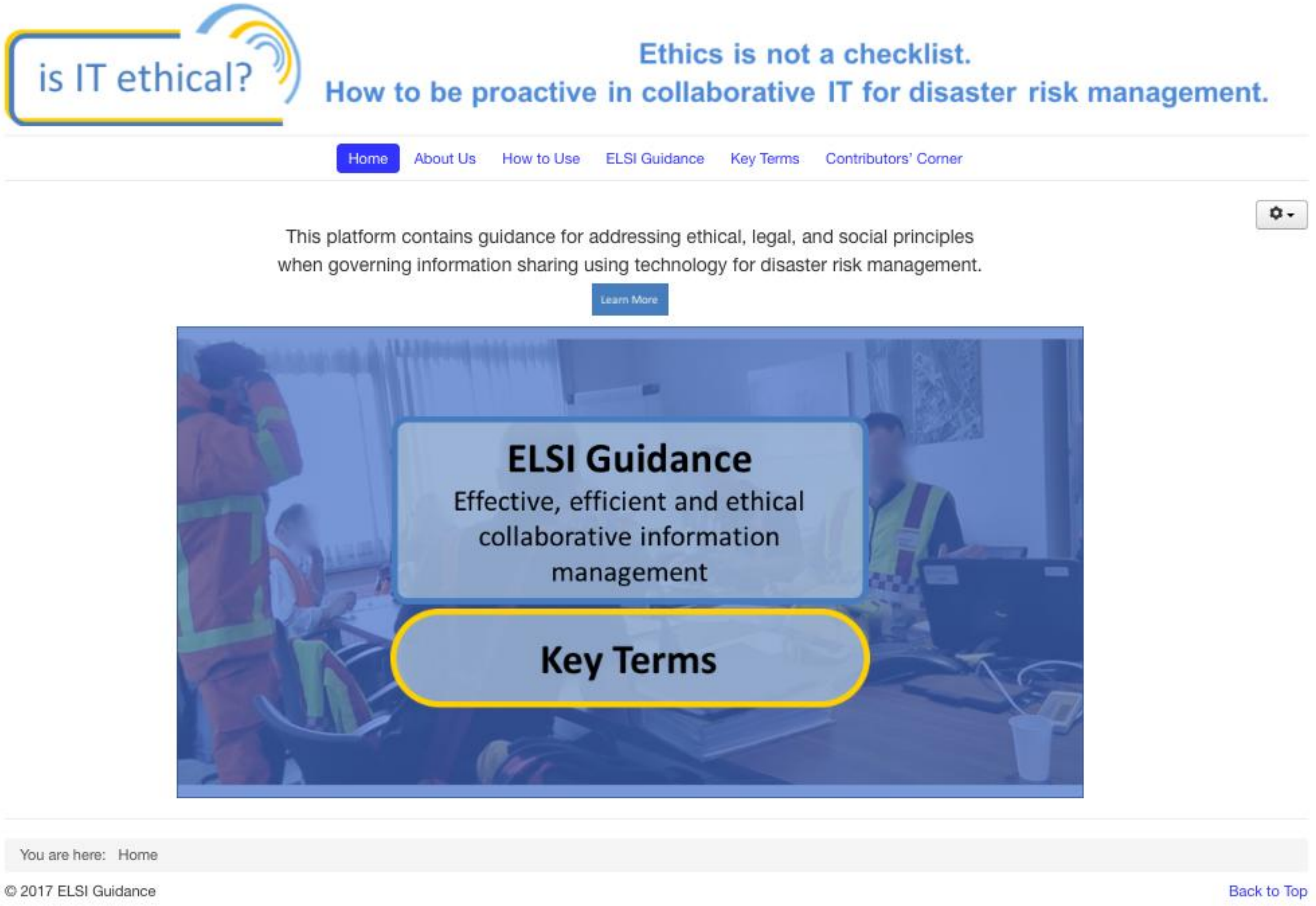
is IT ethical?

Common Information Spaces

Systems of Systems

Broadband

Requirements



Ethics is not a checklist.
How to be proactive in collaborative IT for disaster risk management.

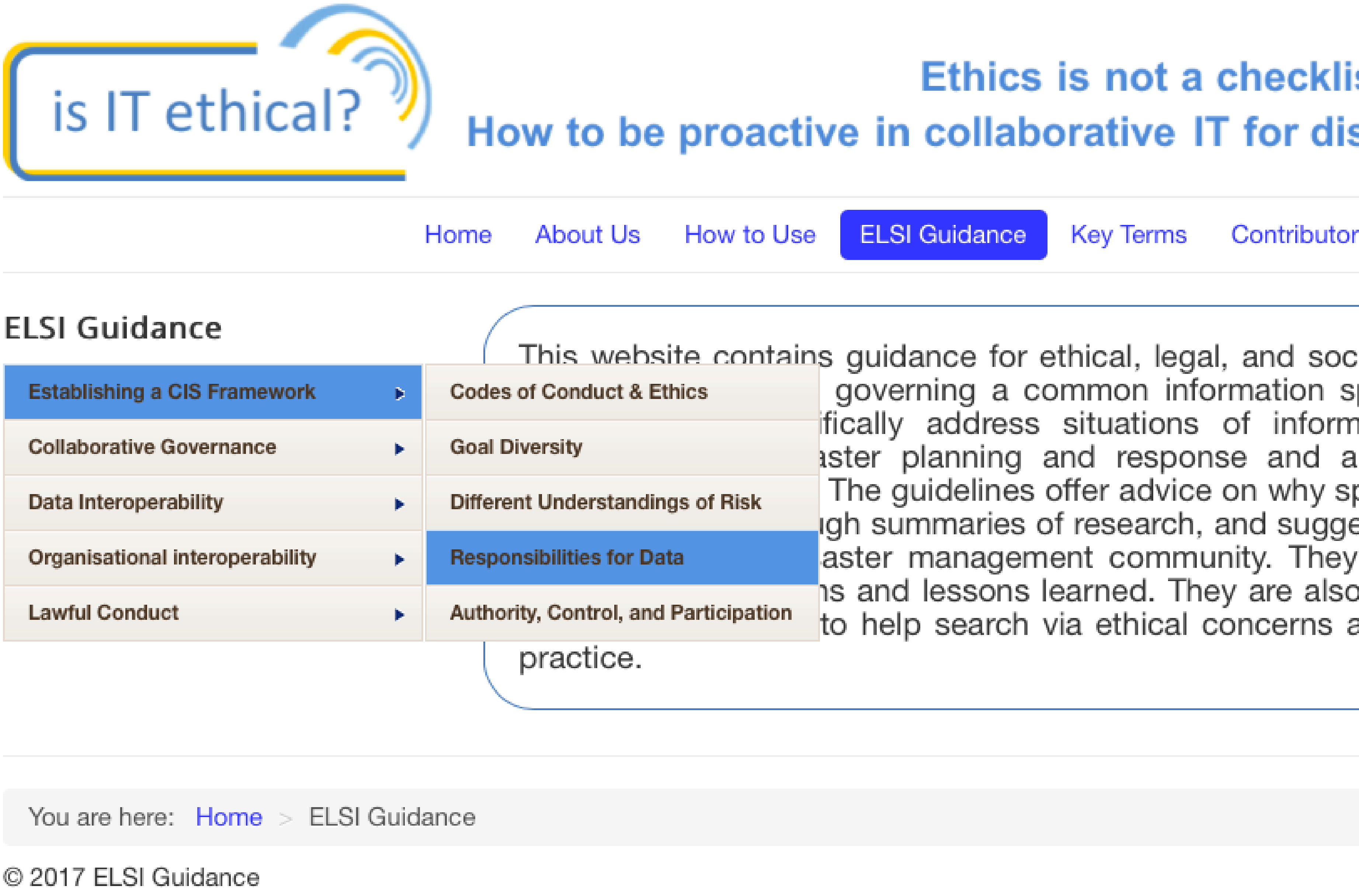
This platform contains guidance for addressing ethical, legal, and social principles when governing information sharing using technology for disaster risk management.

ELSI Guidance
Effective, efficient and ethical collaborative information management

Key Terms

You are here: Home

© 2017 ELSI Guidance



Ethics is not a checkli

How to be proactive in collaborative IT for dis

Home
About Us
How to Use
ELSI Guidance
Key Terms
Contributor

ELSI Guidance

Establishing a CIS Framework
Collaborative Governance
Data Interoperability
Organisational interoperability
Lawful Conduct
Codes of Conduct & Ethics
Goal Diversity
Different Understandings of Risk
Responsibilities for Data
Authority, Control, and Participation

This website contains guidance for ethical, legal, and soc

governing a common information sp

ifically address situations of inform

aster planning and response and a

The guidelines offer advice on why sp

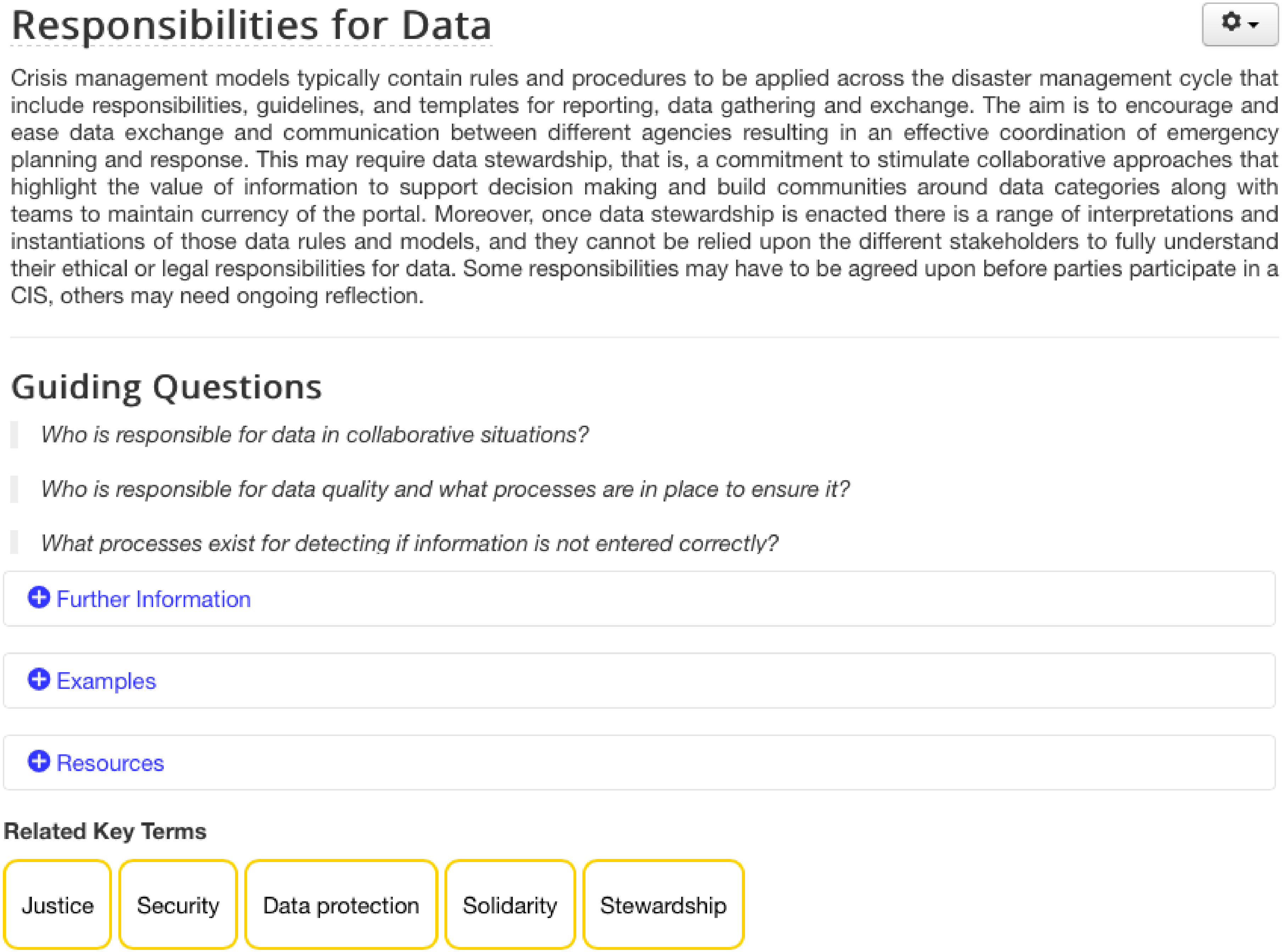
ugh summaries of research, and sugge

aster management community. They

ns and lessons learned. They are also

to help search via ethical concerns a

practice.



Responsibilities for Data

Crisis management models typically contain rules and procedures to be applied across the disaster management cycle that include responsibilities, guidelines, and templates for reporting, data gathering and exchange. The aim is to encourage and ease data exchange and communication between different agencies resulting in an effective coordination of emergency planning and response. This may require data stewardship, that is, a commitment to stimulate collaborative approaches that highlight the value of information to support decision making and build communities around data categories along with teams to maintain currency of the portal. Moreover, once data stewardship is enacted there is a range of interpretations and instantiations of those data rules and models, and they cannot be relied upon the different stakeholders to fully understand their ethical or legal responsibilities for data. Some responsibilities may have to be agreed upon before parties participate in a CIS, others may need ongoing reflection.

Guiding Questions

> *Who is responsible for data in collaborative situations?*

> *Who is responsible for data quality and what processes are in place to ensure it?*

> *What processes exist for detecting if information is not entered correctly?*

⊕ Further Information

⊕ Examples

⊕ Resources

Related Key Terms

Justice | Security | Data protection | Solidarity | Stewardship

> *How is access to data logged? If a user accesses data, are they then assumed to know and expected to respond to it?*

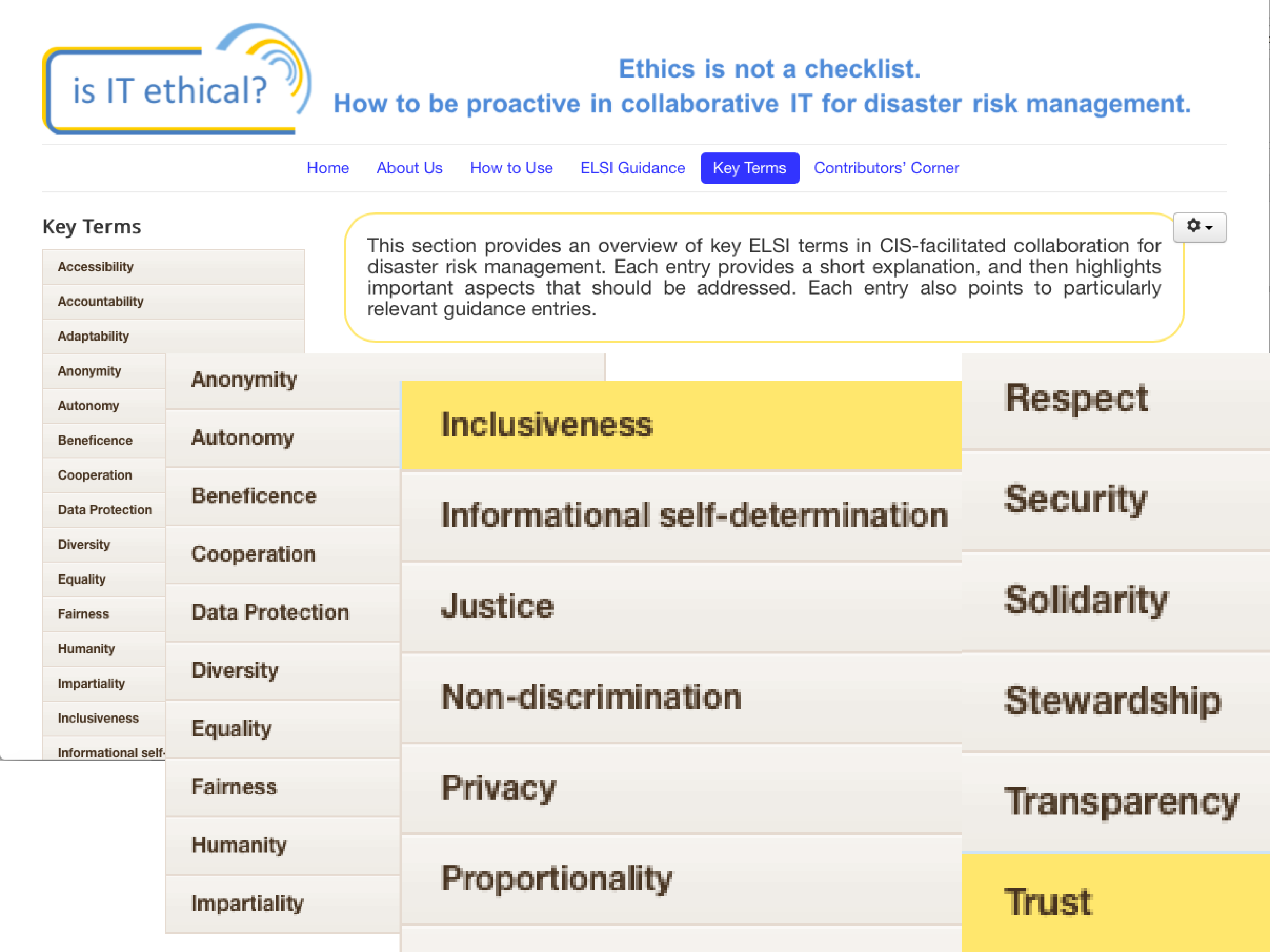
⊕ Further Information

⊖ Examples

In reaction to a perceived failure of data sharing practices after the 2016 Paris terrorist attack there were calls for more data sharing. However, commentators argue that this may not be the best way forward. In a critical discussion, Didier Bigo, Sergio Carrera, Elspeth Guild and Valsamis Mitsilegas from CEPS - a leading think tank and forum for debate on EU affairs argue that

> the fact that the attackers were allegedly 'known' by some authorities suggests that more information sharing would do little as a response to events like those that took place in Brussels. This was also the case with the Paris events, in both January and November 2015, which proved that from the perspective of crime fighting, 'more intelligence' is not an efficient law enforcement tool for countering terrorism and crime. What is needed is better instead of more information sharing. The challenge is not so much that information is not shared within the EU or with third countries, or that focus is needed on ways to enable 'more' data sharing in the EU. Instead, priority should be given to assessing the reasons why that 'information' was not used by the relevant national authorities, to ensuring better targeted and more accountable information exchange, and to boosting EU operational cooperation and joint (cross-border) investigations (2016).

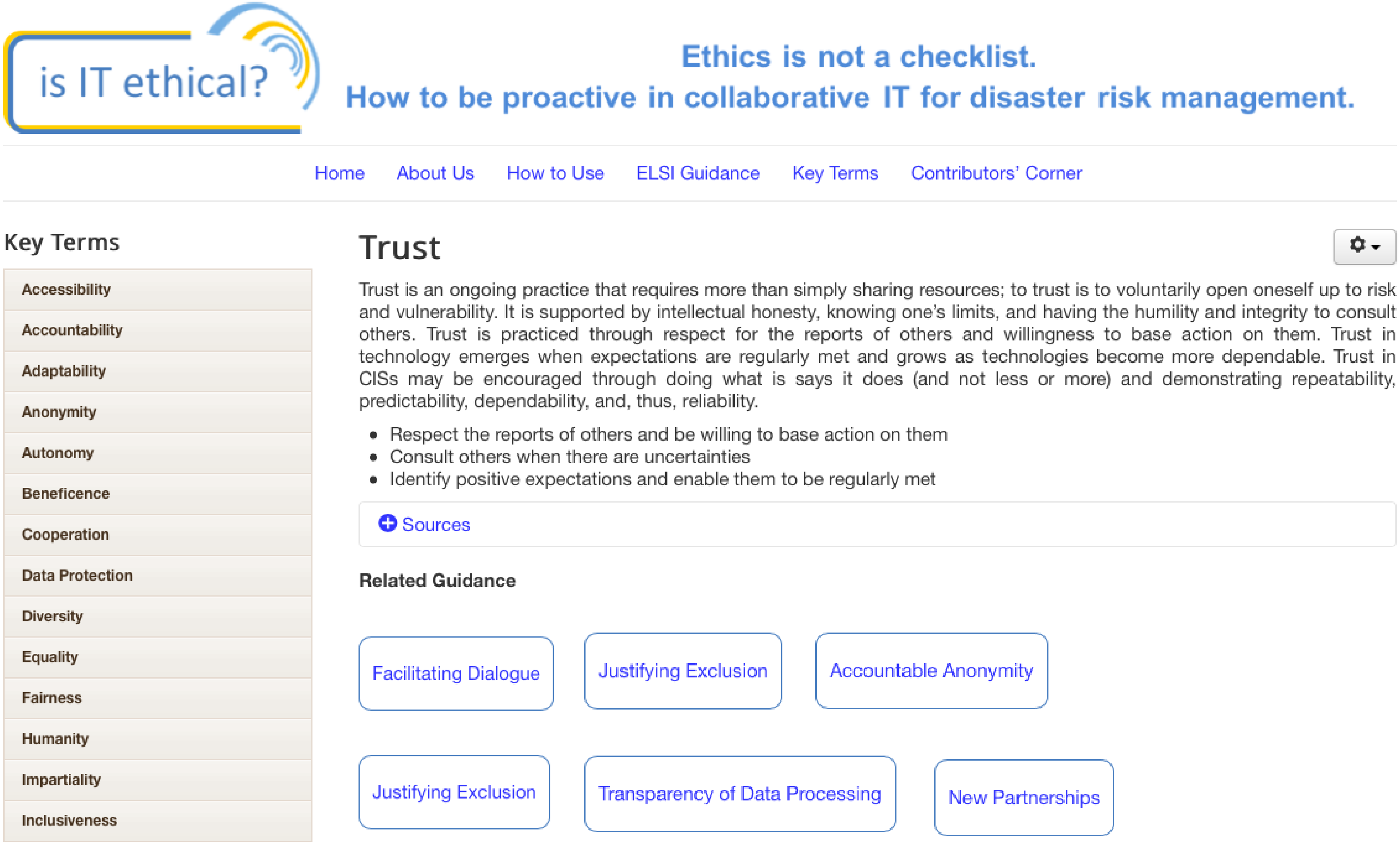
⊕ Resources



Ethics is not a checklist.
How to be proactive in collaborative IT for disaster risk management.

Key Terms

This section provides an overview of key ELSI terms in CIS-facilitated collaboration for disaster risk management. Each entry provides a short explanation, and then highlights important aspects that should be addressed. Each entry also points to particularly relevant guidance entries.



is IT ethical?

Ethics is not a checklist.

How to be proactive in collaborative IT for disaster risk management.

Key Terms

- Accessibility
- Accountability
- Adaptability
- Anonymity
- Autonomy
- Beneficence
- Cooperation
- Data Protection
- Diversity
- Equality
- Fairness
- Humanity
- Impartiality
- Inclusiveness

Trust

Trust is an ongoing practice that requires more than simply sharing resources; to trust is to voluntarily open oneself up to risk and vulnerability. It is supported by intellectual honesty, knowing one's limits, and having the humility and integrity to consult others. Trust is practiced through respect for the reports of others and willingness to base action on them. Trust in technology emerges when expectations are regularly met and grows as technologies become more dependable. Trust in CISs may be encouraged through doing what is says it does (and not less or more) and demonstrating repeatability, predictability, dependability, and, thus, reliability.

- Respect the reports of others and be willing to base action on them
- Consult others when there are uncertainties
- Identify positive expectations and enable them to be regularly met

Related Guidance

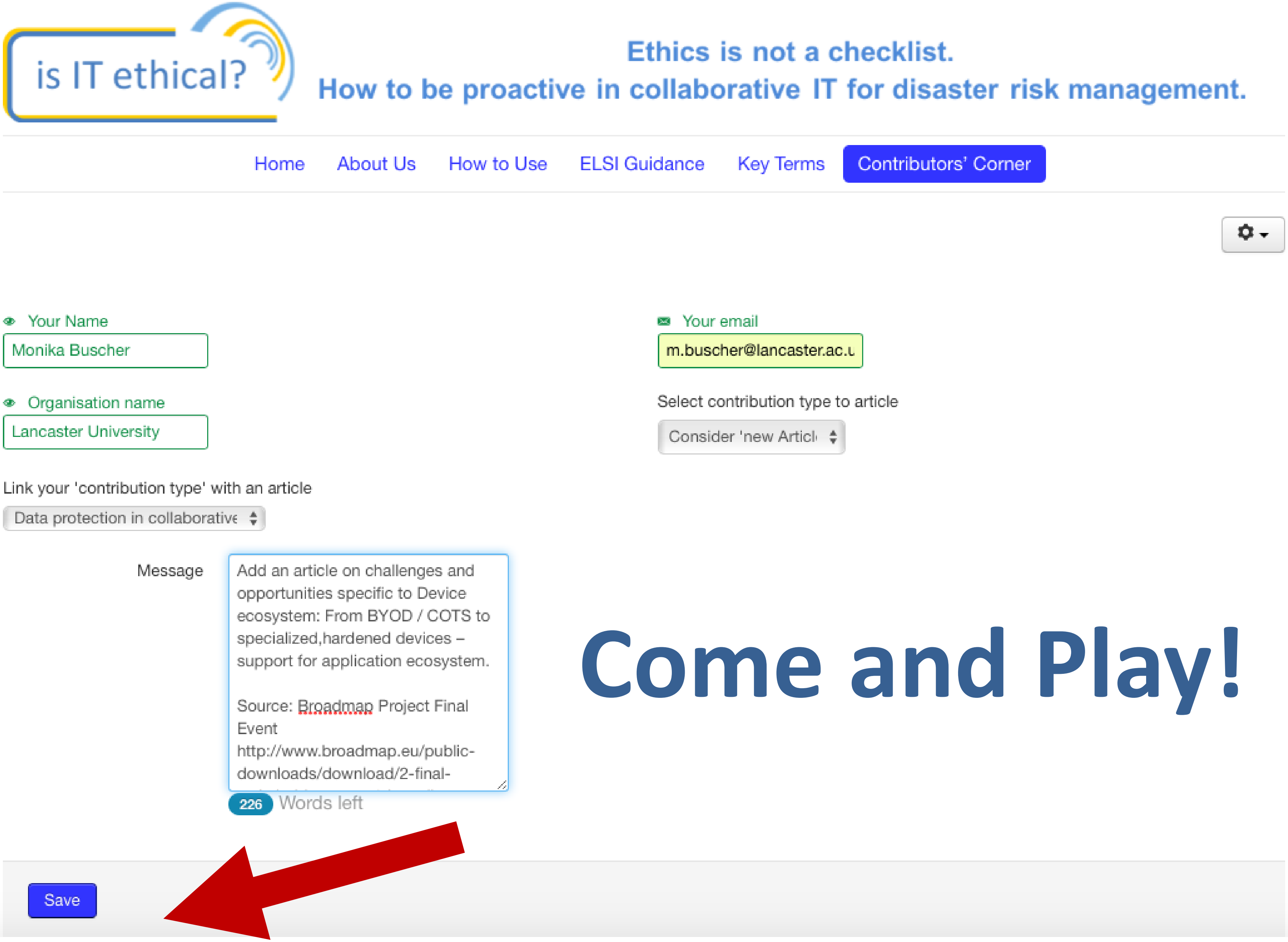
Cooperation with PSCE

- Sharing information is not only a technical issue but also implies the management of different sorts of data
- Requirements that are legal ethical, societal have also to be fulfilled.
- How to help PPDR organisations to assess the respect of these requirements?

Cooperation with PSCE

- Support the setting-up of an easy tool
- Accessible via PSCE website
- Interest of having an evolving tool

(questions, feedback from users).



Ethics is not a checklist.
How to be proactive in collaborative IT for disaster risk management.

Your Name: Monika Buscher

Your email: m.buscher@lancaster.ac.u

Organisation name: Lancaster University

Select contribution type to article: Consider 'new Articl

Link your 'contribution type' with an article: Data protection in collaborative

Message: Add an article on challenges and opportunities specific to Device ecosystem: From BYOD / COTS to specialized,hardened devices – support for application ecosystem.

Source: Broadmap Project Final Event
http://www.broadmap.eu/public-downloads/download/2-final-

226 Words left

Come and Play!

Monika Buscher, Katrina Petersen, Sarah Becklake, Catherine Easton, Male Lujan Escalante, Xaroula Kerasidou, Rachel Oliphant
SecInCoRe, Lancaster University
www.secincore.eu @FP7_SecInCoRe

Lina Jasmontaite, Kristof Huysmans
KU Leuven
EPISECC
www.episecc.eu @EPISECC_FP7

Matthias Leese, Andreas Baur-Ahrens
Tübingen University
SECTOR
www.fp7-sector.eu @SECTORFP7

George Mourikas, David Lund, Marie-Christine Bonnamour
Public Safety Communications Europe
PSCE
www.psc-europe.eu @psc_e

ELSITask Force

in coordination action for topic FP7 SEC-2012.5.1-1 Analysis and identification of security systems and data set used by first responders and police authorities: EPISECC (GA Nº 607078), REDIRNET (GA Nº 607768), SecInCoRe (GA Nº 607832), SECTOR (GA Nº 607821)