

LiU IRT – Team introduction

TF-CSIRT London 2013

David Byers

LiU IRT

Enable users to perform their work in a secure computing environment

This means:

- Prevent IT security incidents
- Detect IT security incidents
- Handle IT security incidents
- Operate (some) infrastructure components

We have:

- Five members (three core members; 3+ FTE)

Linköping University

A multi-campus university

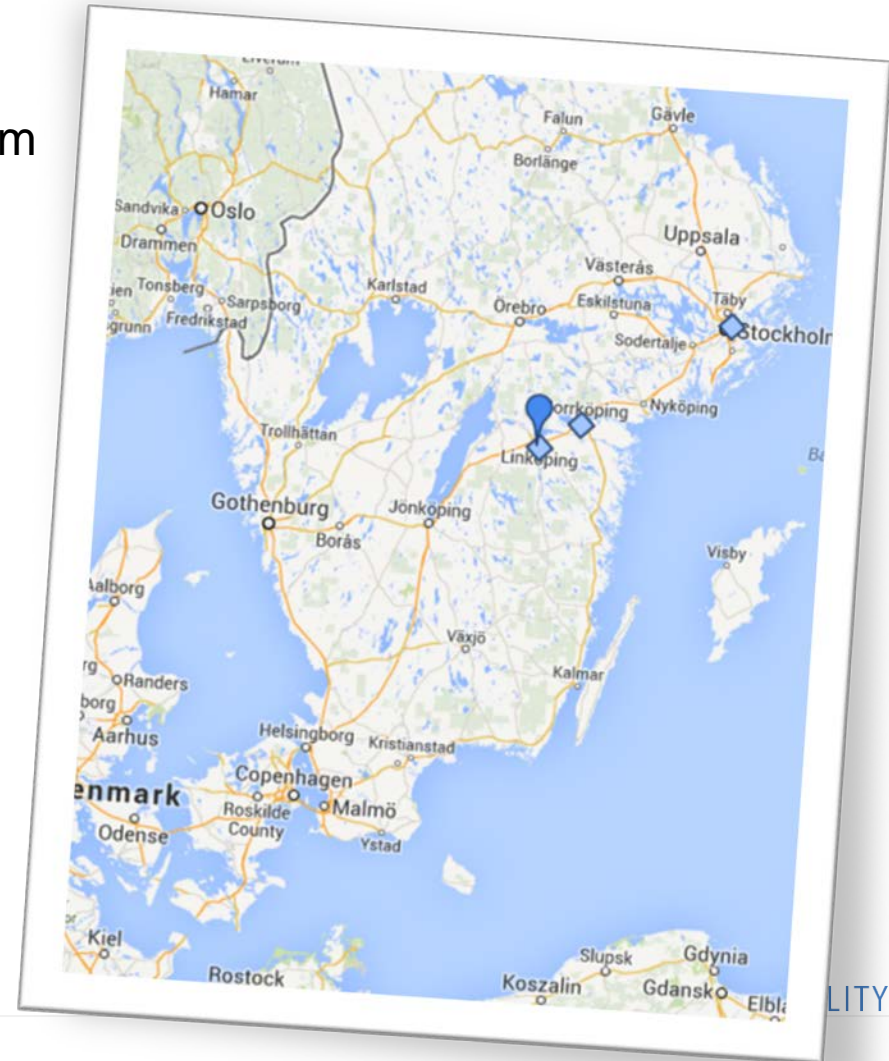
- Linköping, Norrköping and Stockholm

Students and staff

- 27000 students and 3900 staff
- Students from 80 countries

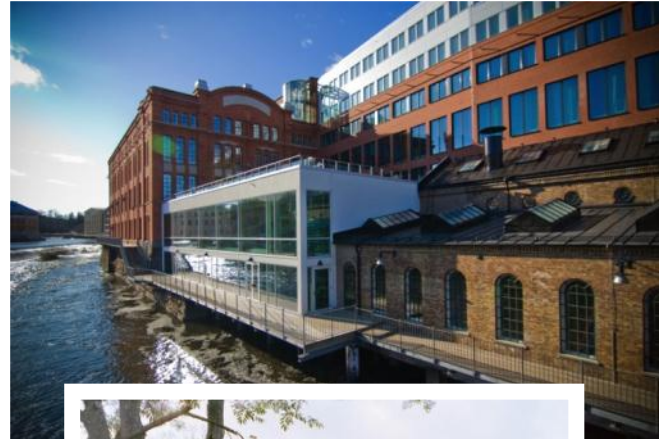
Four faculties

- Arts and sciences
- Educational sciences
- Health sciences
- Institute of technology



Our campuses

**Campus Valla,
Linköping,
18,000 students**



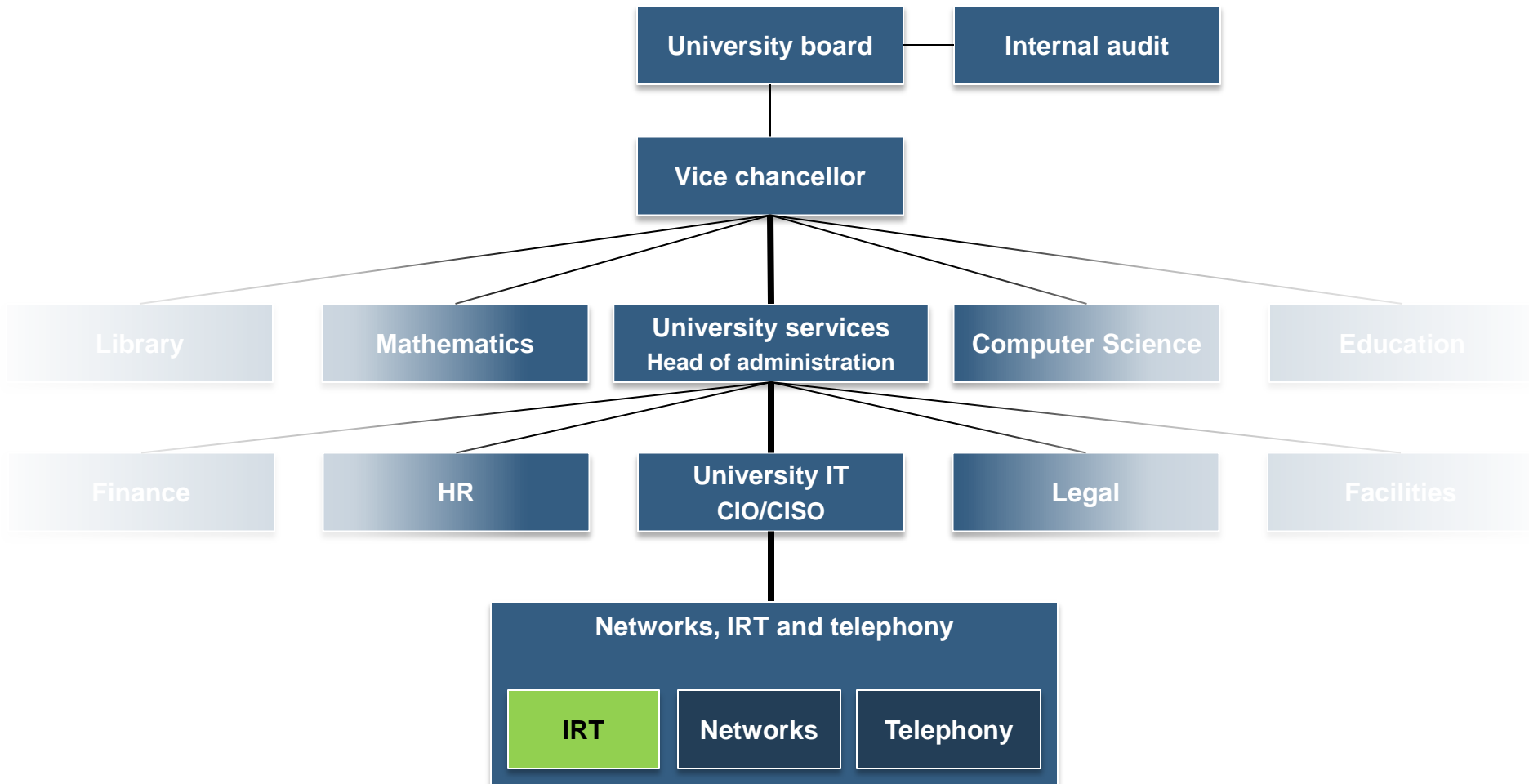
**Campus US (University Hospital), Linköping,
3,000 students**



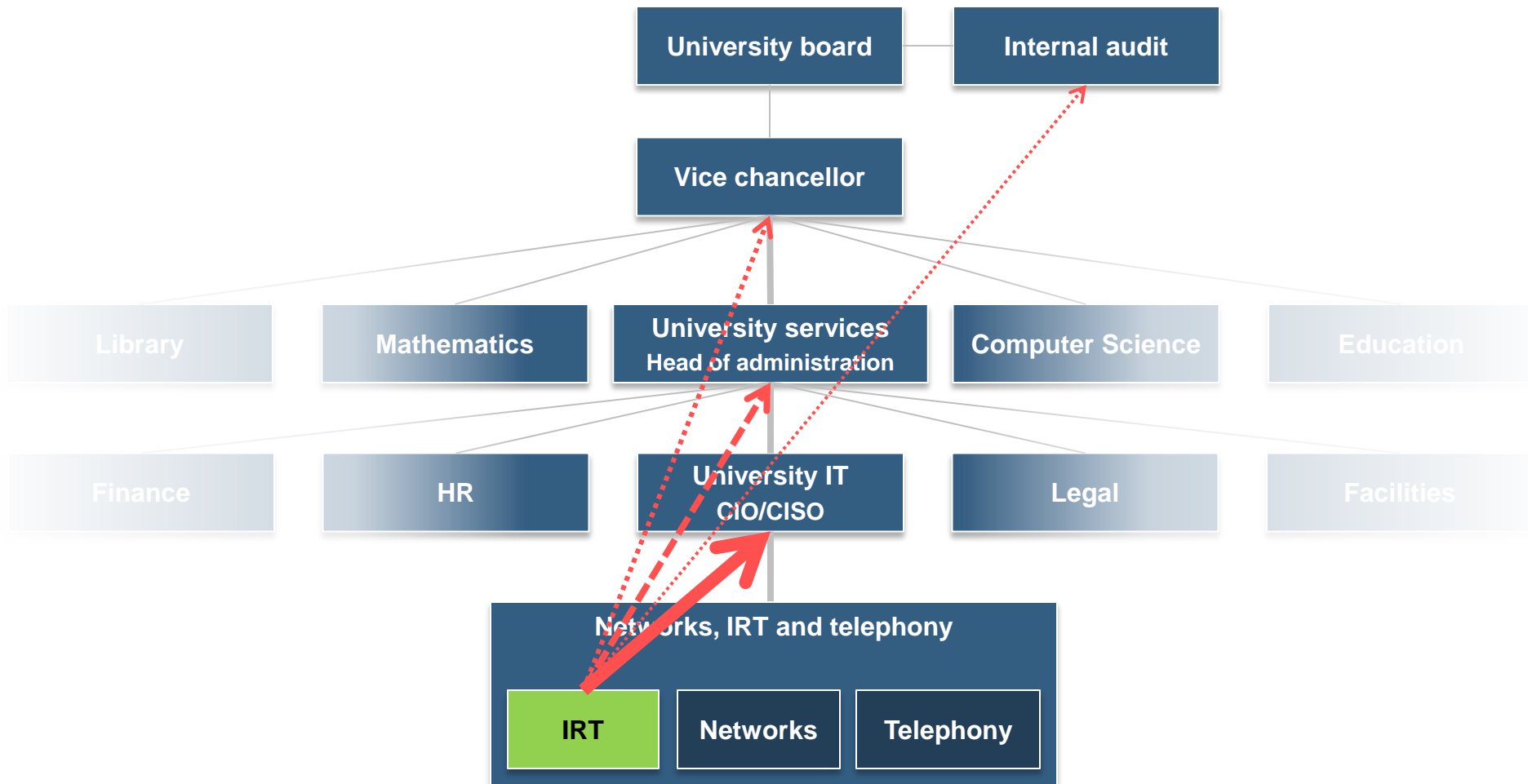
**Campus Norrköping,
5,000 students**

**Malmstens, Stockholm,
70 students**

Organization



Reporting



LiU IRT

Core members

David Byers

Johannes Hassmund

Ulrik Haugen

Associated members

Emil Palm

Kent Engström

Typical activities in a typical week

Block malware-infested computers

Block open resolvers

Manage firewall rulesets

Provide advice for procurement

Formulate security policy

Issue certificates

Interpret university policy

Assist the legal department

Perform vulnerability scans

Develop and deploy new tools

Things we do

Support the CISO

- Formulate and interpret information security policy
- Investigate information security issues (not just incidents)

Support the organization

- Review technical designs for risks and security issues
- Provide information security training for university staff
- Provide advice on information security in any context
- Assist with handling information security issues (not just incidents)

Things we do

Prevent and detect IT security incidents

- Scan for vulnerable network-connected devices
- Provide information and advice to operations staff
- Monitor network flows, system logs and external sources

Respond to, handle and resolve IT security incidents

- Respond to incidents reported from internal and external sources
- Perform forensic analysis of compromised devices
- Cooperate with law enforcement where appropriate

Closing

More details about us:

- <http://www.liu.se/insidan/it/irt/>

Contact us (even if it's not about an incident):

- abuse@liu.se

Or come see us if you're in the area!



Linköping University

expanding reality

www.liu.se

LIU EXPANDING REALITY