TSD and Educloud Research
Development and management

2024, Leon du Toit

Goals

- Establish shared understanding of:
  - The platform
    - Definition
    - How it is built
    - Who builds what
  - Process used to manage and develop it

What do we sell?

Secure Extensible Collaborative Computing Projects

What do we sell?

Secure	Confidentiality, Integrity, Availability, and more
Extensible	APIs, software
Collaborative	Login, Anyone, Anywhere
Computing	HPC, VM, containers, web, DB, storage, backup
Projects	Time and purpose limited data processing enclaves

Kreft registeret

FHI
Folkehelseinstituttet

KORONASTUDIEN

nykode

moba

Avdeling for medisinsk genetikk

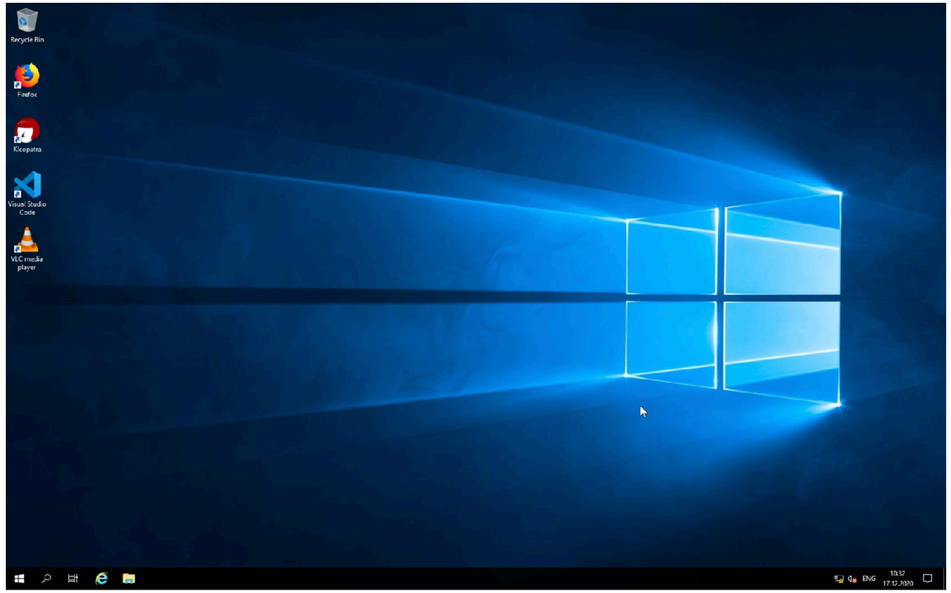
Avdeling for medisinsk genetikk er landets største medisinsk genetiske avdeling og arbeider med utredning av arvelige sykdommer og forskning på arvelige årsaker til sykdom.

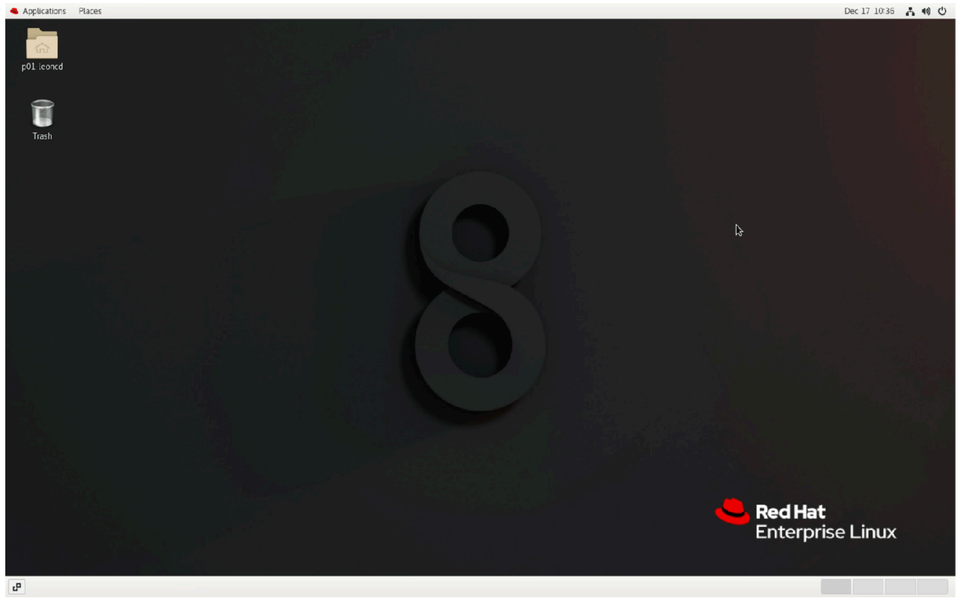
Les om Avdeling for medisinsk genetikk →

IMPRESS-Norway - clinical trial for cancer patients

FoodCapture

Løsning for sykdomsrelatert underernæring, til sykehus, sykehjem og hjemmetjeneste





UiO : University of Oslo

TSD / Data Portal

Import and export project research material

Import Files

Upload files into your project area.

Export Files

Download files from your project area.

Record Video and/or Audio

Capture and upload data from camera, microphone, computer screen or speakers, into your project area.

Your Personal Data

Review the data related to you as a member of a Educloud project.

- Review your personal data
- Change your password
- Change your OTP

Project Membership

Get access to and information about a Educloud project.

- See information about your project and the PI

Project Administration

Administer the members and resources of your Educloud project.

- Manage foreign user applications
- Manage project members
- Manage user privileges
- Manage group membership
- Manage import links

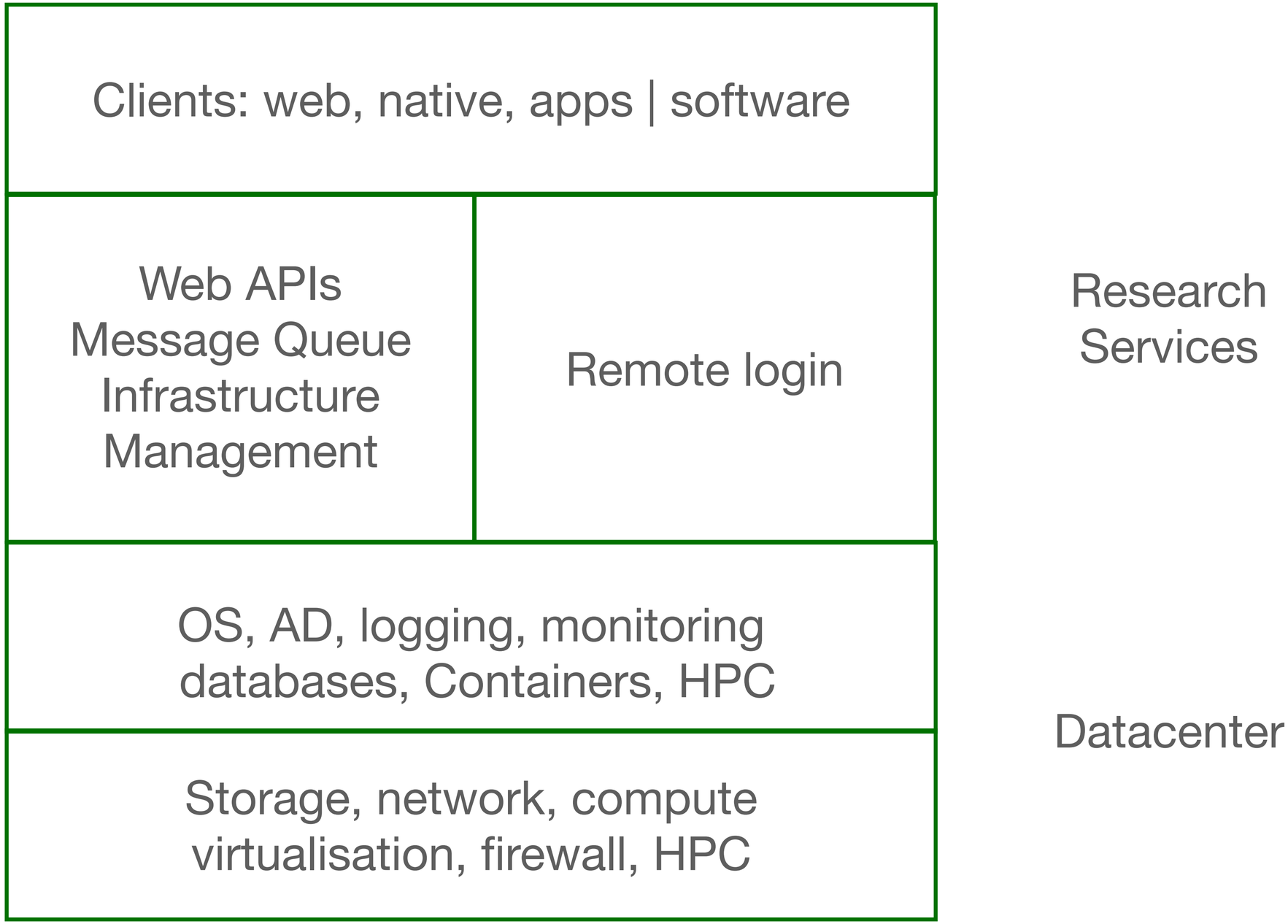
docker

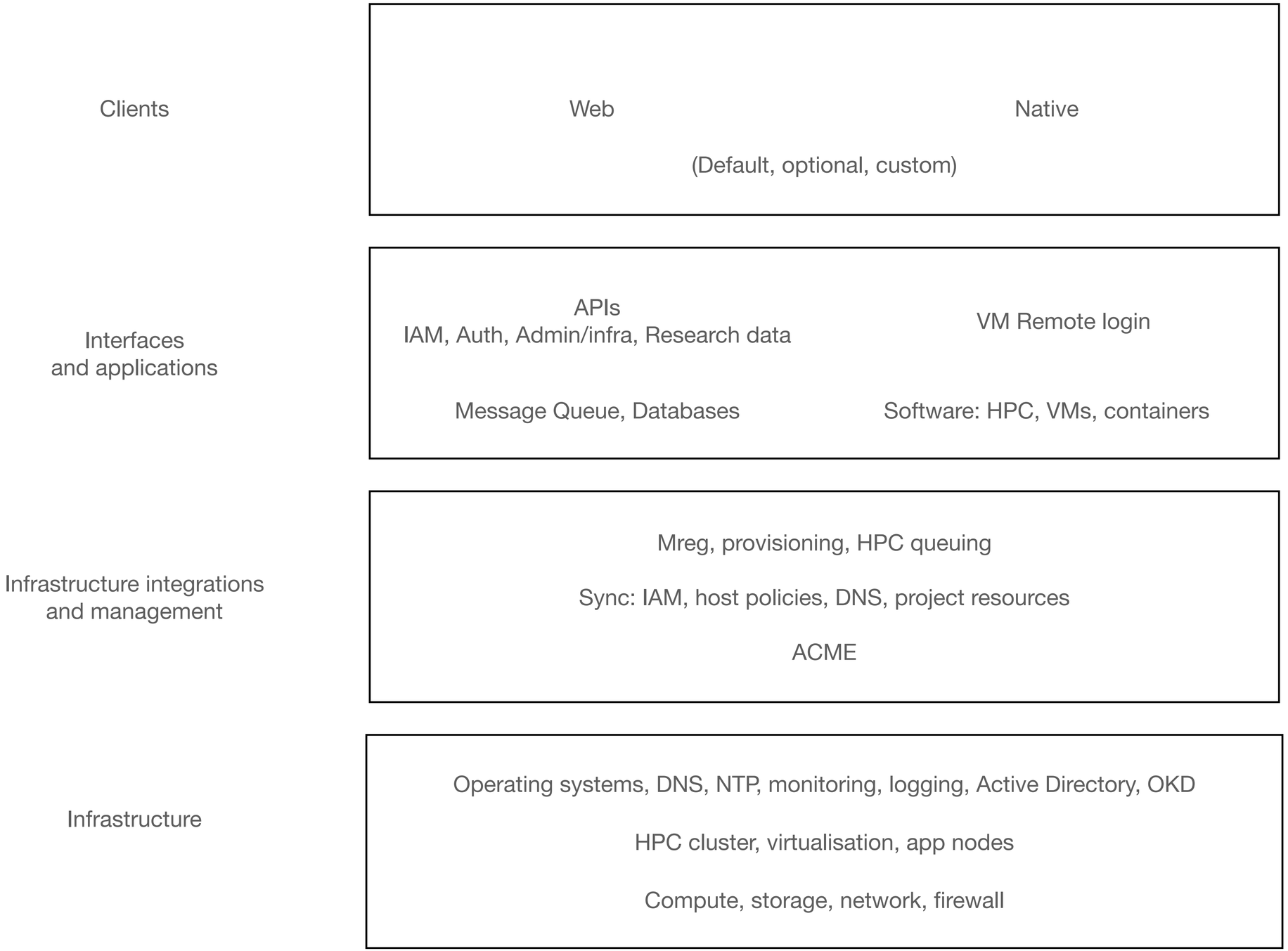
PyTorch

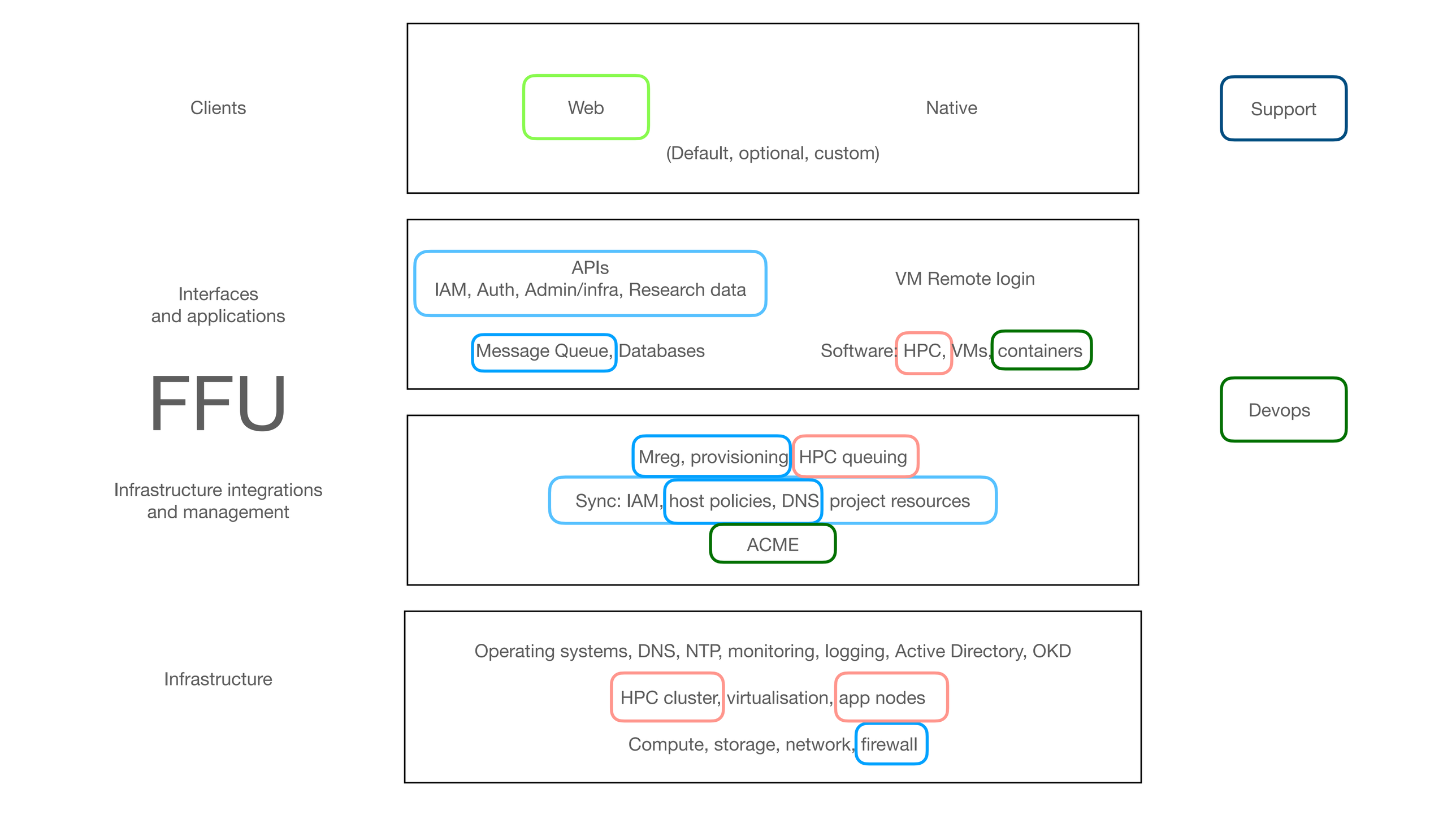
APPTAINER

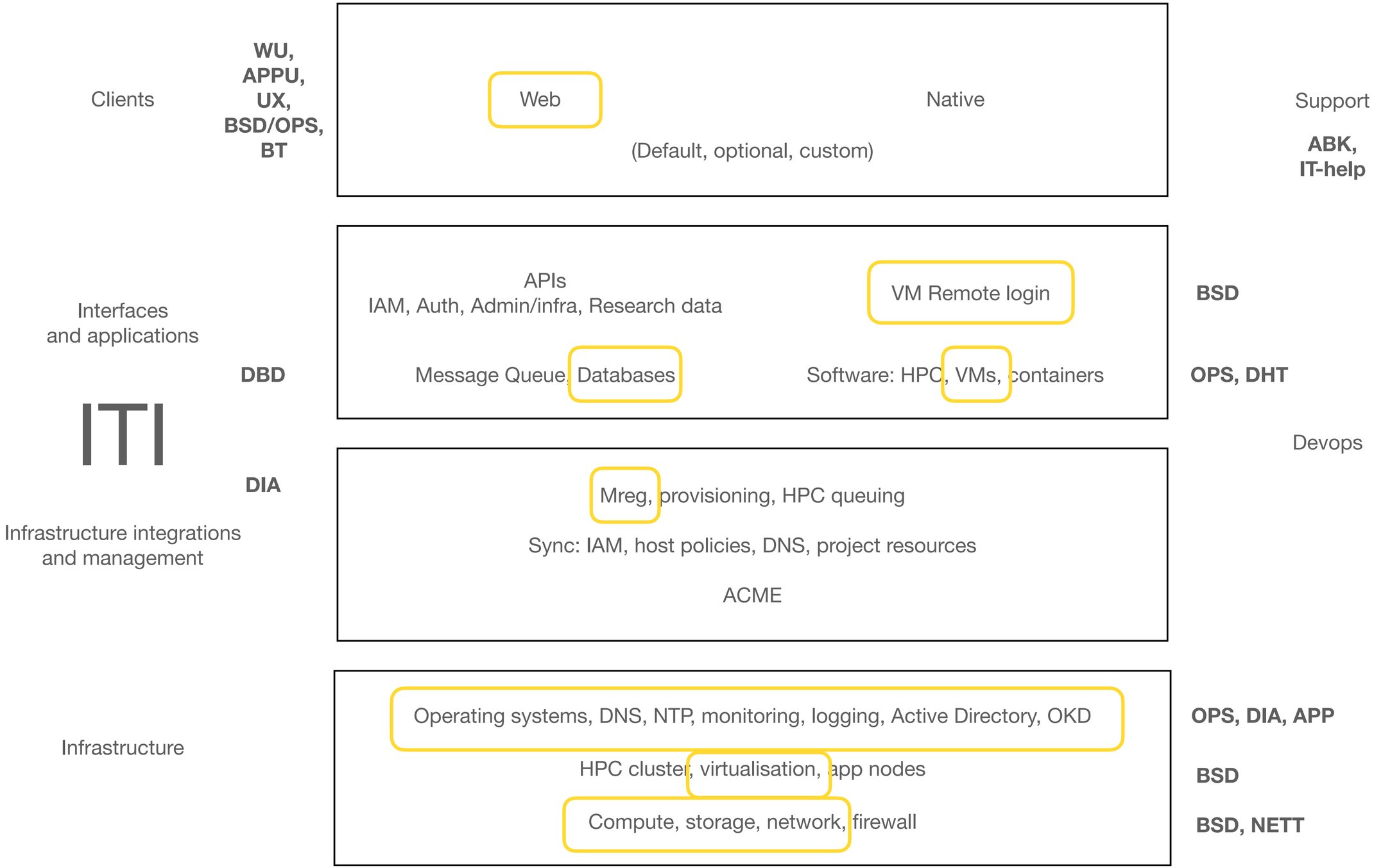
TensorFlow

R

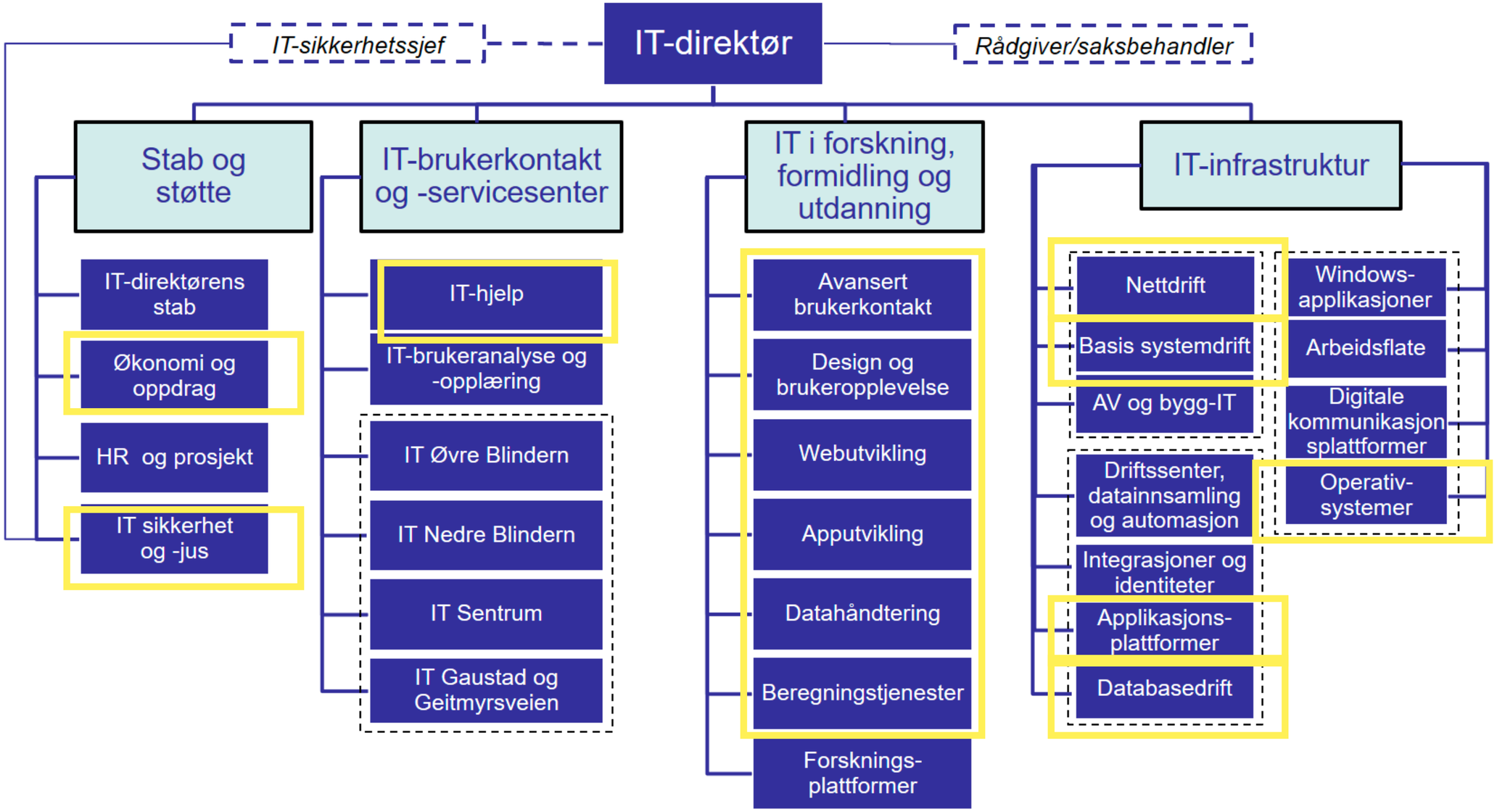

Clients: web, native, apps | software
Web APIs
Message Queue
Infrastructure
Management
Remote login
OS, AD, logging, monitoring
databases, Containers, HPC
Storage, network, compute
virtualisation, firewall, HPC
Research
Services
Datacenter


Clients
Web
Native
(Default, optional, custom)
Interfaces
and applications
APIs
IAM, Auth, Admin/infra, Research data
VM Remote login
Message Queue, Databases
Software: HPC, VMs, containers
Infrastructure integrations
and management
Mreg, provisioning, HPC queuing
Sync: IAM, host policies, DNS, project resources
ACME
Infrastructure
Operating systems, DNS, NTP, monitoring, logging, Active Directory, OKD
HPC cluster, virtualisation, app nodes
Compute, storage, network, firewall


Clients
Web
Native
(Default, optional, custom)
Support
Interfaces
and applications
APIs
IAM, Auth, Admin/infra, Research data
VM Remote login
Message Queue, Databases
Software: HPC, VMs, containers
FFU
Devops
Infrastructure integrations
and management
Mreg, provisioning
HPC queuing
Sync: IAM, host policies, DNS, project resources
ACME
Infrastructure
Operating systems, DNS, NTP, monitoring, logging, Active Directory, OKD
HPC cluster, virtualisation, app nodes
Compute, storage, network, firewall


Clients
WU,
APPU,
UX,
BSD/OPS,
BT
Web
Native
(Default, optional, custom)
Support
ABK,
IT-help
Interfaces
and applications
APIs
IAM, Auth, Admin/infra, Research data
VM Remote login
BSD
DBD
Message Queue, Databases
Software: HPC, VMs, containers
OPS, DHT
ITI
Devops
DIA
Mreg, provisioning, HPC queuing
Sync: IAM, host policies, DNS, project resources
ACME
Infrastructure integrations
and management
Infrastructure
Operating systems, DNS, NTP, monitoring, logging, Active Directory, OKD
OPS, DIA, APP
HPC cluster, virtualisation, app nodes
BSD
Compute, storage, network, firewall
BSD, NETT

IT-avdelingen på UiO



Roles

In terms of relation to “the platform”

- Service provider - platform builds on top
- Integrator - builds on top of platform

How do we manage what we implement?

- We need (at least):
  - Common process
  - Common understanding

Process

https://www.uio.no/tjenester/it/sikkerhet/lsis/

Ledelsessystem for informasjonssikkerhet

Dokumentene som utgjør «Ledelsessystem for informasjonssikkerhet» (LSIS) for Universitetet i Oslo er delt inn i tre deler, som du ser under. Du kan lese denne korte introduksjonen eller gå til denne siden for å få brukerrettet informasjon om informasjonssikkerhet og hva det betyr for deg. Denne typen dokumenter kalles også ISMS.

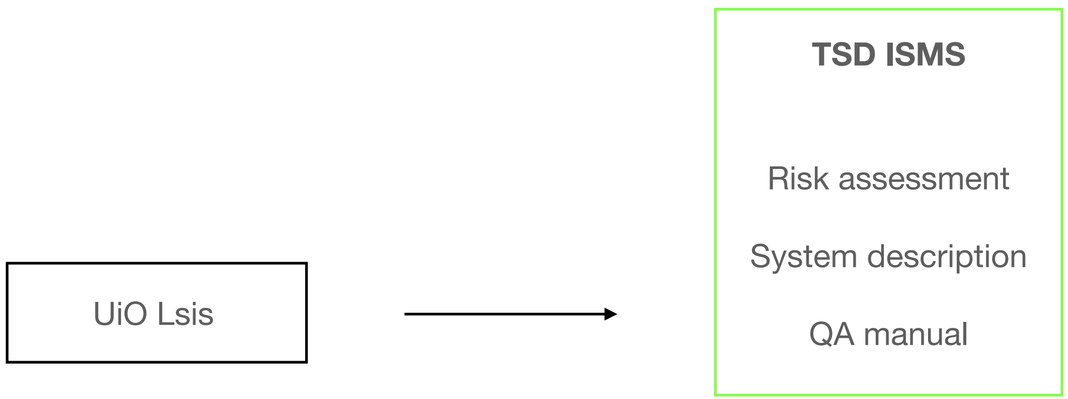
Styrende del

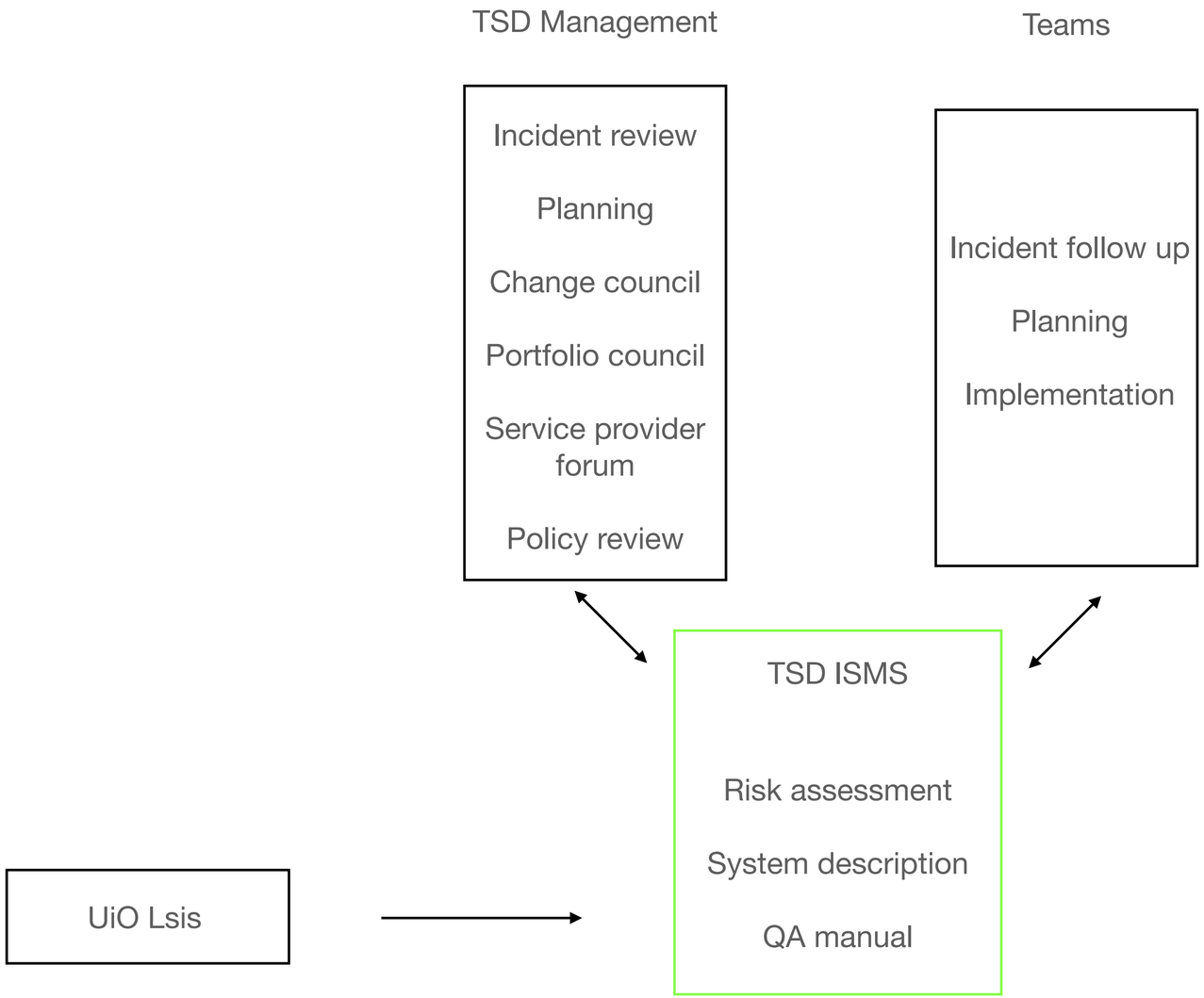
- Kapittel 1 – Innledning
- Kapittel 2 – Lover, forskrifter og bestemmelser
- Kapittel 3 – Mål og strategi
- Kapittel 4 – Sikkerhetsorganisasjon og ledelse

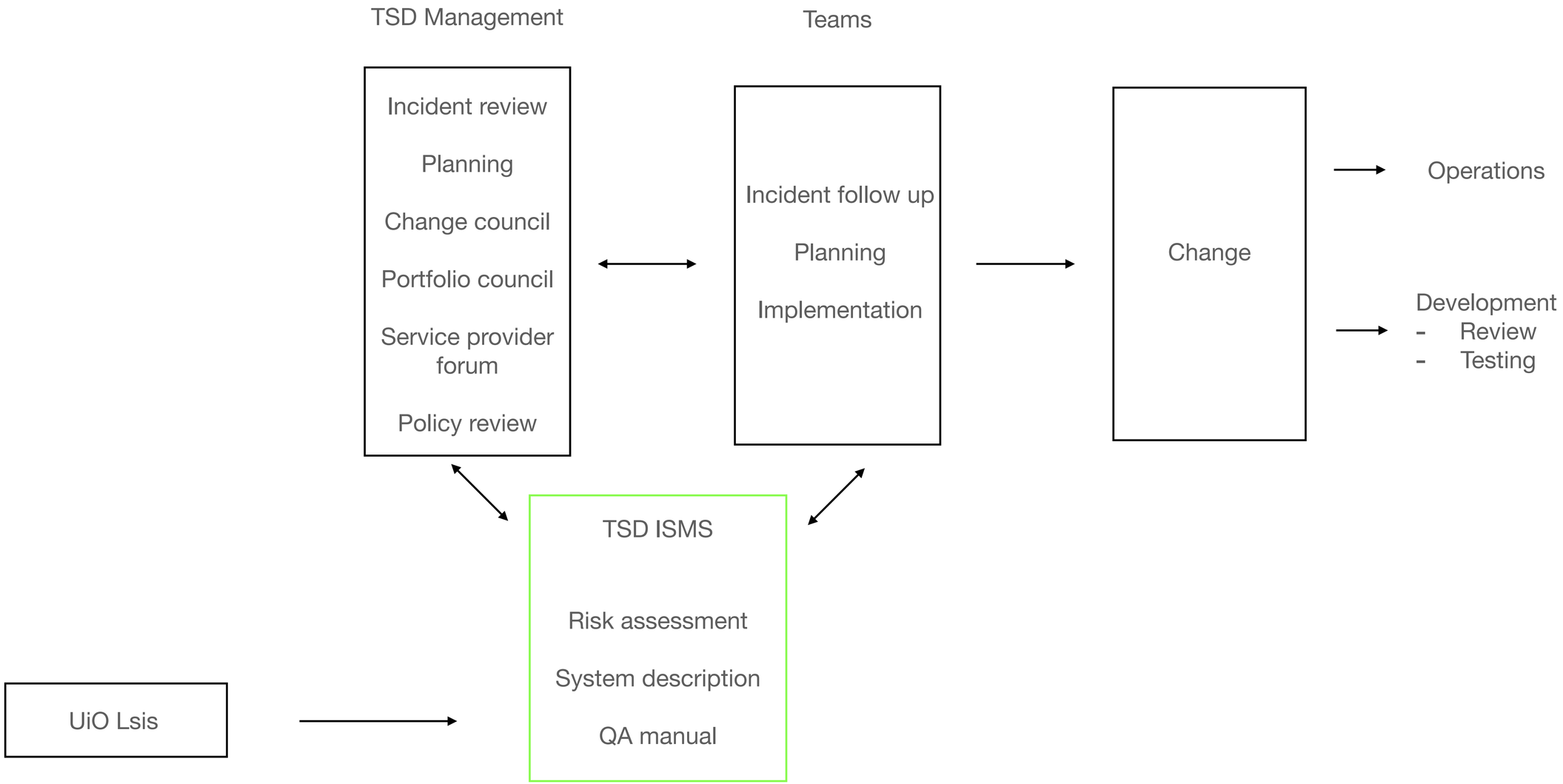
Gjennomførende del

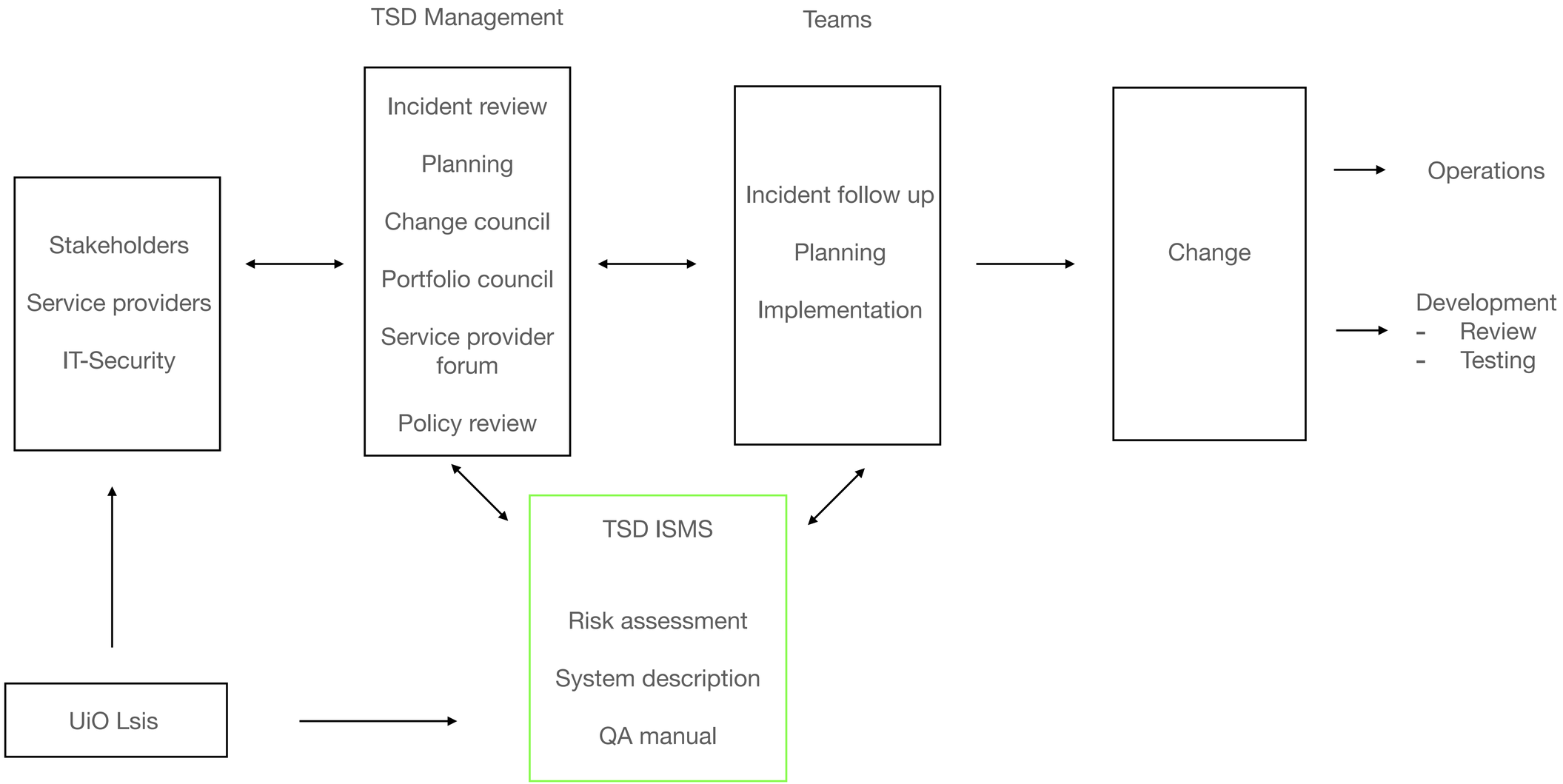
- Kapittel 5 – Oppgavebeskrivelser
- Kapittel 6 – Sikkerhetsplan
- Kapittel 7 – Risiko- og sårbarhetsanalyser
- Kapittel 8 – Grunnsikring av infrastruktur og tjenester
- Kapittel 9 – Brukere og deres tilgang til IT-tjenestene
- Kapittel 10 – Beredskaps- og kontinuitetsplaner
- Kapittel 11 – Anskaffelser, vedlikehold og utvikling

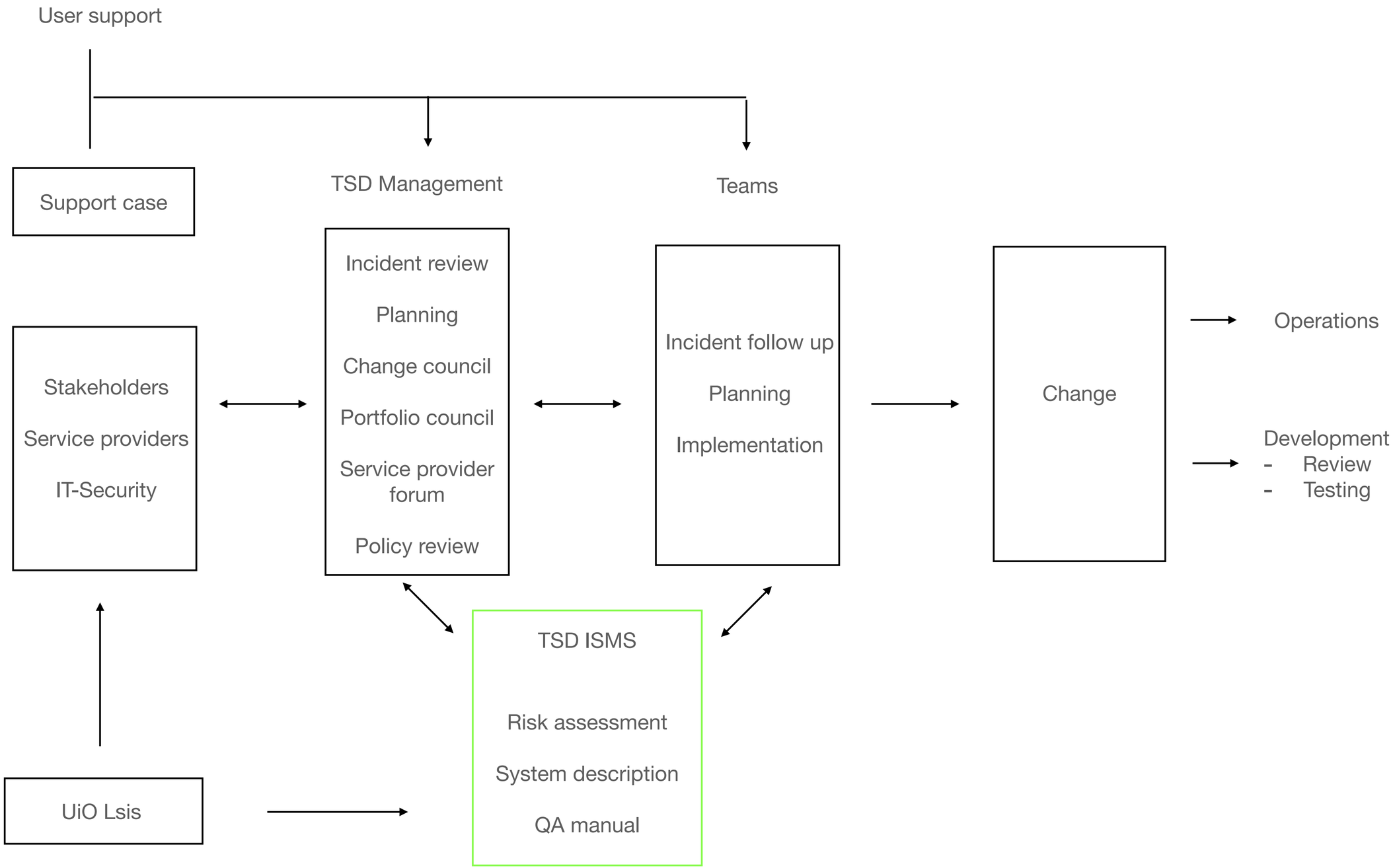
UiO Lsis

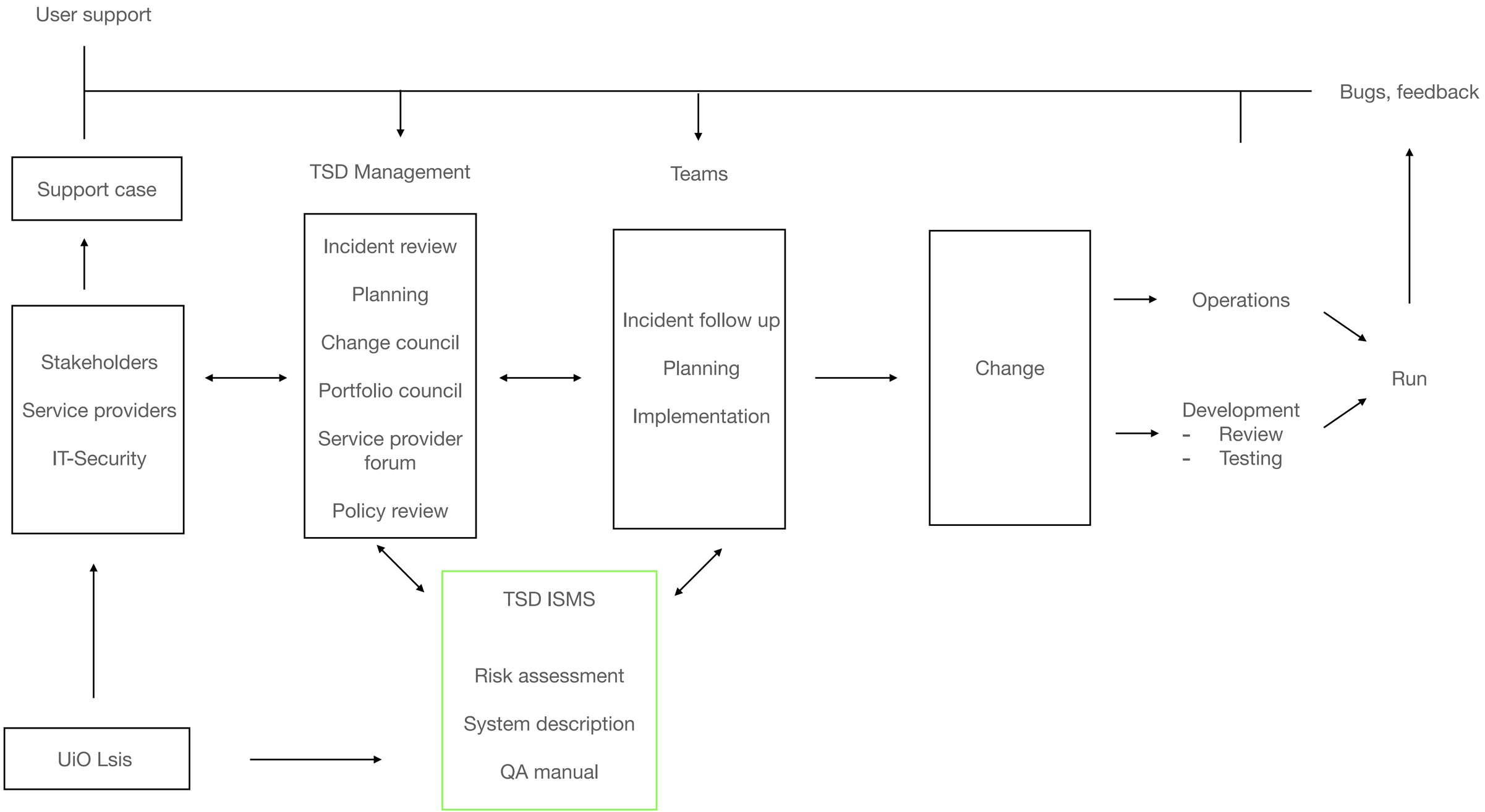

UiO Lsis
TSD ISMS
Risk assessment
System description
QA manual

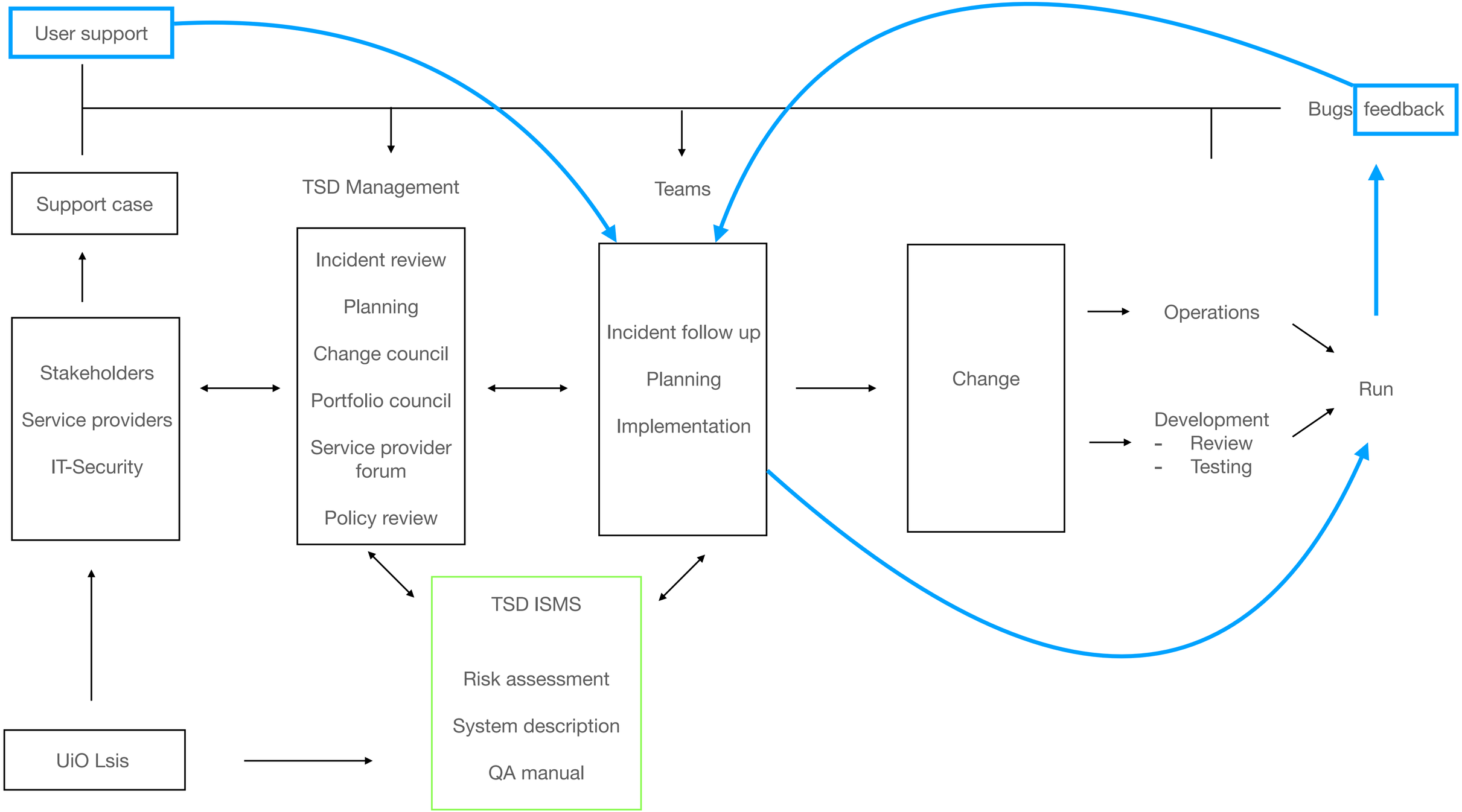

TSD Management
Teams
Incident review
Planning
Change council
Portfolio council
Service provider forum
Policy review
Incident follow up
Planning
Implementation
TSD ISMS
Risk assessment
System description
QA manual
UiO Lsis

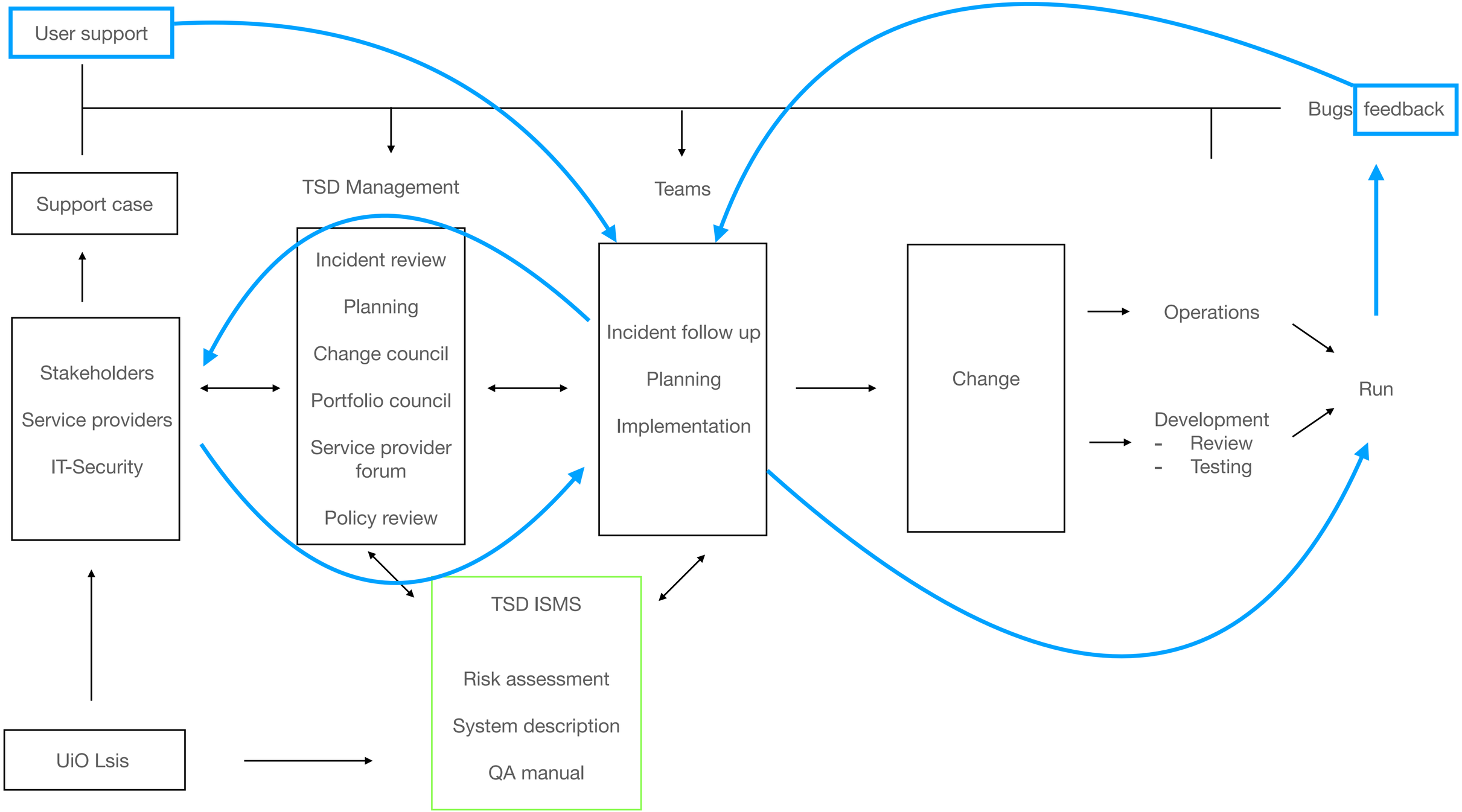

TSD Management
Teams
Incident review
Planning
Change council
Portfolio council
Service provider forum
Policy review
Incident follow up
Planning
Implementation
Change
Operations
Development
- Review
- Testing
TSD ISMS
Risk assessment
System description
QA manual
UiO Lsis

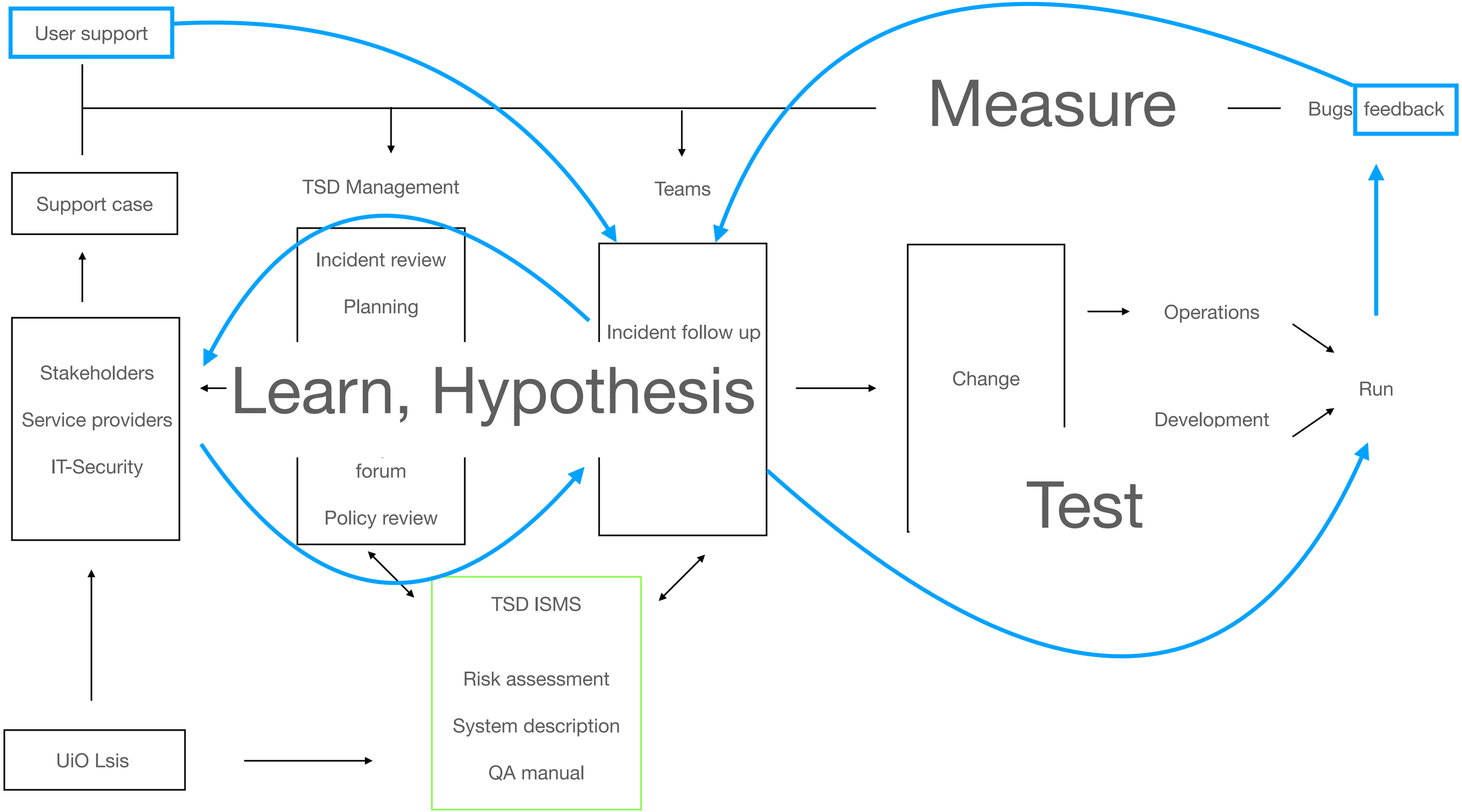

TSD Management
Teams
Stakeholders
Service providers
IT-Security
Incident review
Planning
Change council
Portfolio council
Service provider forum
Policy review
Incident follow up
Planning
Implementation
Change
Operations
Development
- Review
- Testing
TSD ISMS
Risk assessment
System description
QA manual
UiO Lsis

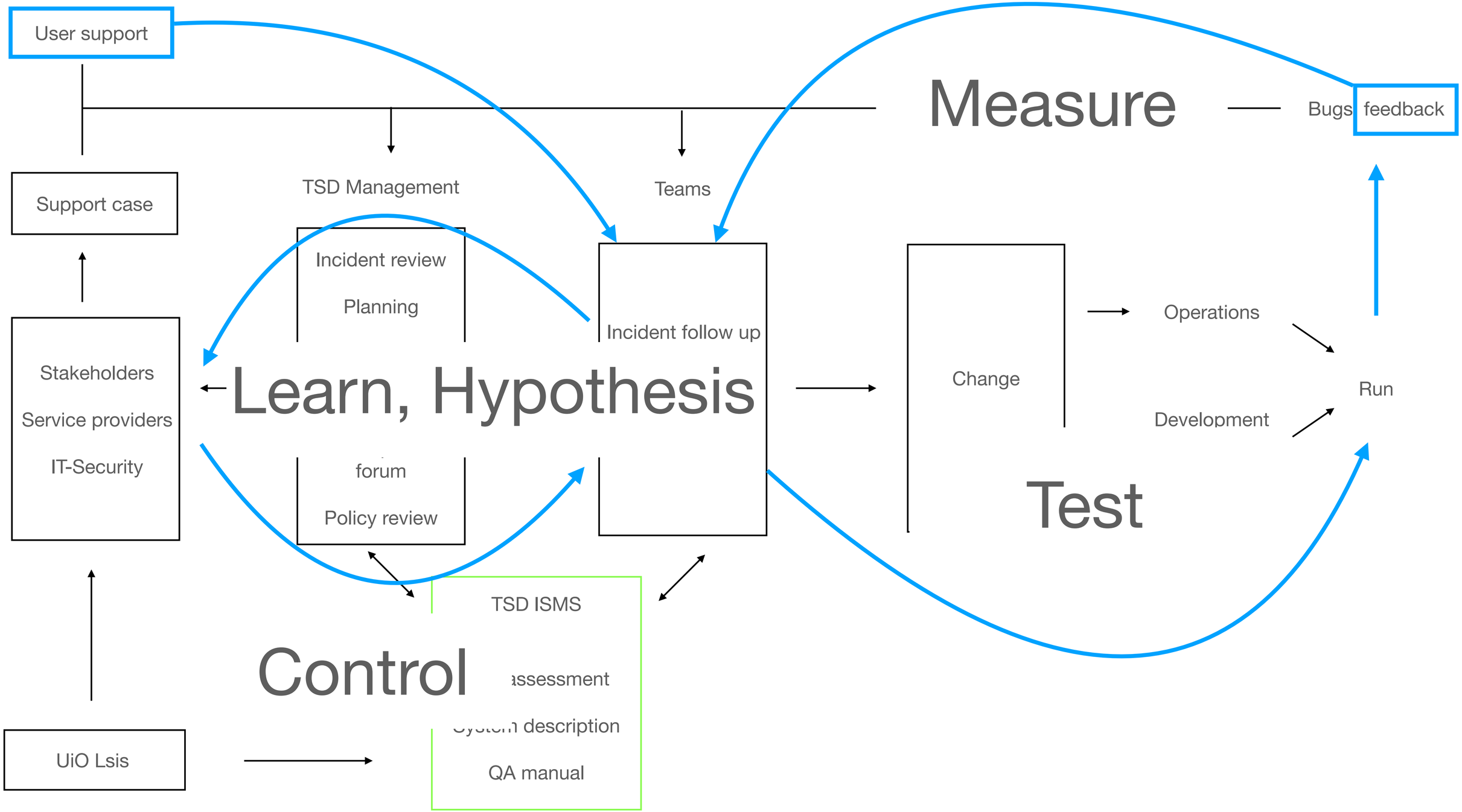

User support
Support case
TSD Management
Teams
Stakeholders
Service providers
IT-Security
Incident review
Planning
Change council
Portfolio council
Service provider forum
Policy review
Incident follow up
Planning
Implementation
Change
Operations
Development
- Review
- Testing
TSD ISMS
Risk assessment
System description
QA manual
UiO Lsis


User support
Bugs, feedback
Support case
TSD Management
Teams
Stakeholders
Service providers
IT-Security
Incident review
Planning
Change council
Portfolio council
Service provider forum
Policy review
Incident follow up
Planning
Implementation
Change
Operations
Development
- Review
- Testing
Run
TSD ISMS
Risk assessment
System description
QA manual
UiO Lsis


User support
Bugs
feedback
Support case
TSD Management
Teams
Incident review
Planning
Change council
Portfolio council
Service provider forum
Policy review
Incident follow up
Planning
Implementation
Change
Operations
Development
- Review
- Testing
Run
Stakeholders
Service providers
IT-Security
TSD ISMS
Risk assessment
System description
QA manual
UiO Lsis


User support
Bugs
feedback
Support case
TSD Management
Teams
Incident review
Planning
Change council
Portfolio council
Service provider forum
Policy review
Incident follow up
Planning
Implementation
Change
Operations
Development
- Review
- Testing
Run
Stakeholders
Service providers
IT-Security
TSD ISMS
Risk assessment
System description
QA manual
UiO Lsis


User support
Measure
Bugs
feedback
Support case
TSD Management
Teams
Incident review
Planning
Incident follow up
Stakeholders
Service providers
IT-Security
Learn, Hypothesis
Change
Operations
Development
Run
forum
Policy review
Test
TSD ISMS
Risk assessment
System description
QA manual
UiO Lsis


User support
Measure
Bugs
feedback
Support case
TSD Management
Teams
Incident review
Planning
Incident follow up
Stakeholders
Service providers
IT-Security
Learn, Hypothesis
Change
Operations
Run
Development
forum
Policy review
Test
TSD ISMS
Control
ıssessment
System description
QA manual
UiO Lsis

Other principles

- Platforms rant
  - https://news.ycombinator.com/item?id=3102800
- The normalization of deviance
  - https://danluu.com/wat/
- End-to-end arguments in system design
  - https://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf

1) All teams will henceforth expose their data and functionality through service interfaces.

2) Teams must communicate with each other through these interfaces.

3) There will be no other form of interprocess communication allowed: no direct linking, no direct reads of another team's data store, no shared-memory model, no back-doors whatsoever. The only communication allowed is via service interface calls over the network.

4) It doesn't matter what technology they use. HTTP, Corba, Pubsub, custom protocols -- doesn't matter. Bezos doesn't care.

5) All service interfaces, without exception, must be designed from the ground up to be externalizable. That is to say, the team must plan and design to be able to expose the interface to developers in the outside world. No exceptions.

6) Anyone who doesn't do this will be fired.

7) Thank you; have a nice day!

- Pay attention to weak signals
- Resist the urge to be unreasonably optimistic
- Teach employees how to conduct emotionally uncomfortable conversations
- System operators need to feel safe in speaking up
- Realize that oversight and monitoring are never-ending

END-TO-END ARGUMENTS IN SYSTEM DESIGN

J.H. Saltzer, D.P. Reed and D.D. Clark*

M.I.T. Laboratory for Computer Science

This paper presents a design principle that helps guide placement of functions among the modules of a distributed computer system. The principle, called the end-to-end argument, suggests that functions placed at low levels of a system may be redundant or of little value when compared with the cost of providing them at that low level. Examples discussed in the paper include bit error recovery, security using encryption, duplicate message suppression, recovery from system crashes, and delivery acknowledgement. Low level mechanisms to support these functions are justified only as performance enhancements.

Takk

leoncd@uio.no