Reference Architecture for the Operationalization of a BCMS

Boban Kršić, Chief Information Security Officer

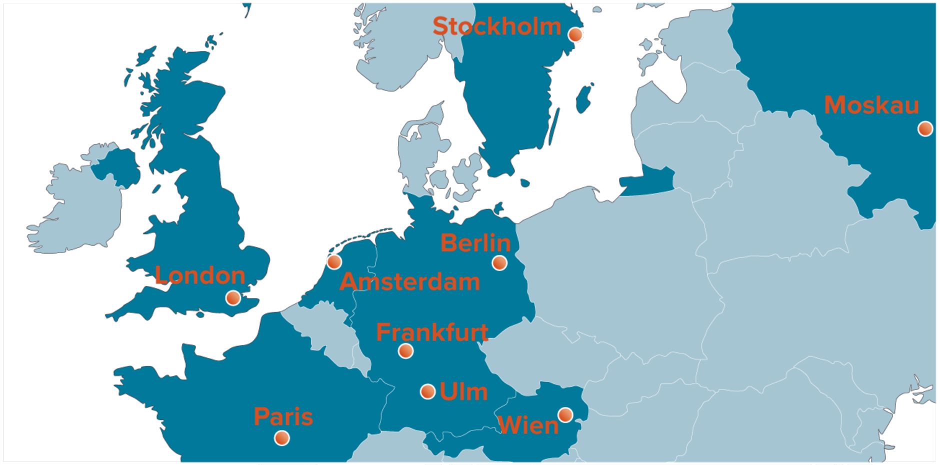
verinice.XP - Berlin, 07. February 2017

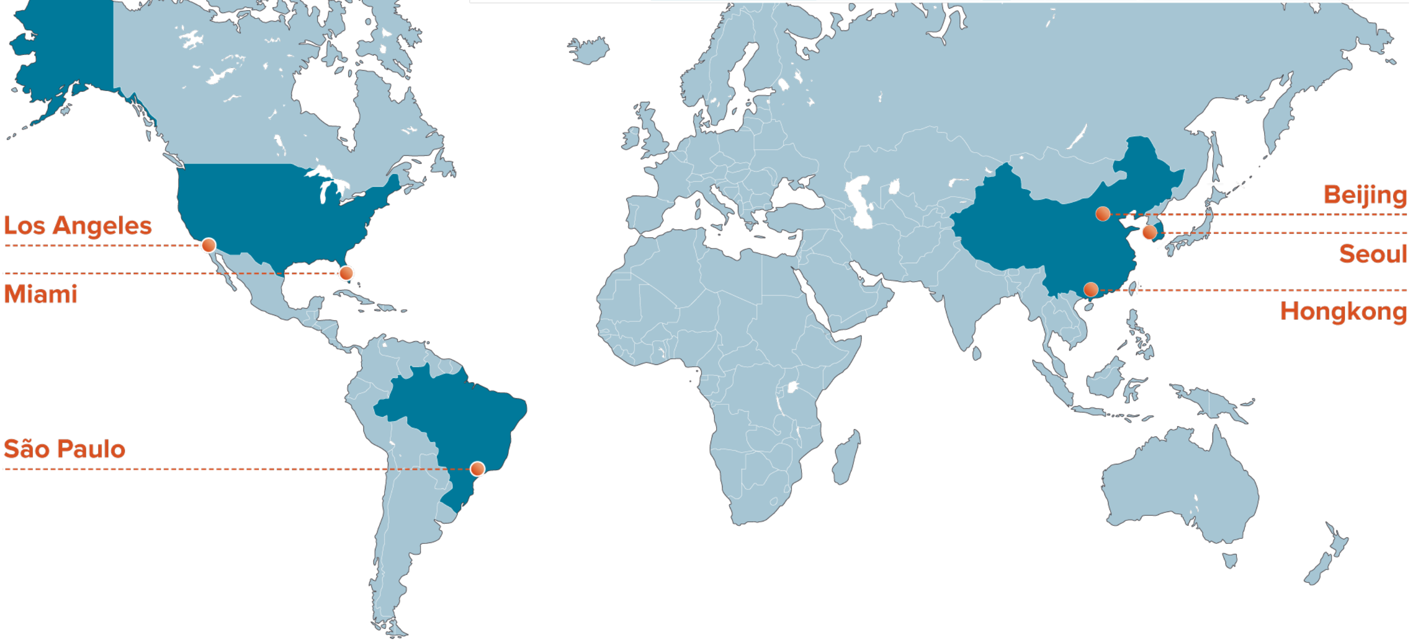
DENIC – Mission

- Founded in 1996 as a cooperative in Frankfurt / Main.
- Act as a neutral, non-discriminating and independent registry service provider for the German Internet community according to RFC 1591.
- Members are companies registering .de domains for their customers.
- Organized as an open not-for-profit institution, each member has equal rights (one member – one vote).
- Government-independent and not regulated.
- Guarantee the highest possible level of both quality as well as technical stability and security.

DENIC – Nameservice for .de

- 19 own name server locations and 35+ complementary anycast locations worldwide
- > 40.000 name server queries per second; peak 110.000 name server queries per second





DENIC – International Collaboration

- Active involvement in various bodies to shape the further development of the Internet
    - Council of European TLD-Registries (CENTR)
    - Deutscher CERT-Verbund
    - DNS-Operations, Analysis and Research Center (DNS-OARC)
    - Internet Corporation for Assigned Names and Numbers (ICANN)
    - Internet Governance Forum (IGF)
    - Internet Engineering Task Force (IETF)
    - Internet Society (ISOC)
    - RIPE Network Coordination Centre (RIPE NCC)
- Further development of Internet standards
- Support of the collaboration between ccTLDs

Business Continuity Management

Business Continuity Management

- Why Business Continuity Management is important
  - to safeguard human life;
  - ensure survival of the organization;
  - enable effective decisions in case of crisis;
  - minimize loss of assets, revenue, and customers;
  - comply with legal requirements;
  - facilitate timely recovery of critical business functions;
  - maintain organization reputation.

Conway’s Law

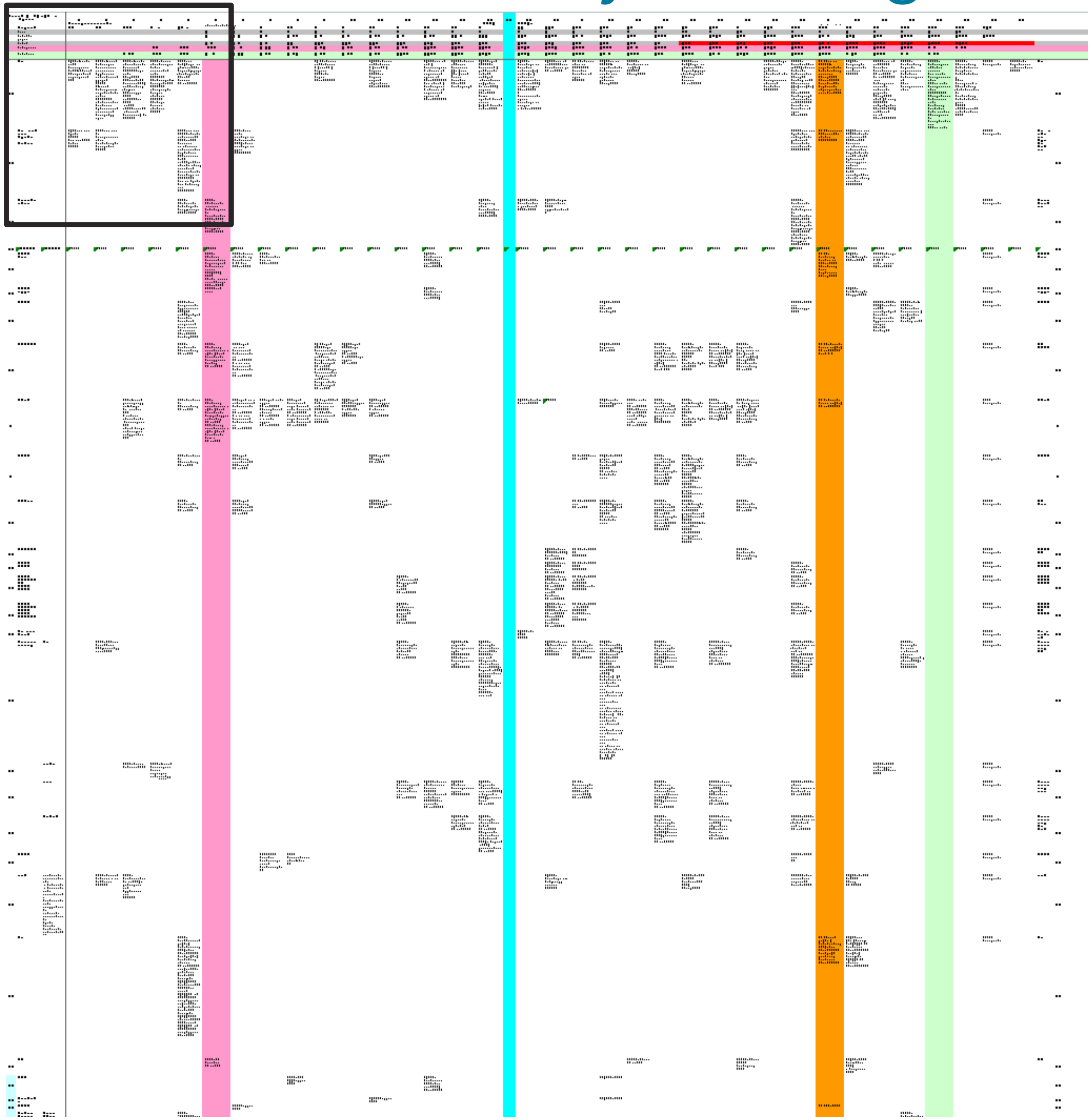
“Any organization that designs a system (defined broadly) will produce a design whose structure is a copy of the organization's communication structure.”

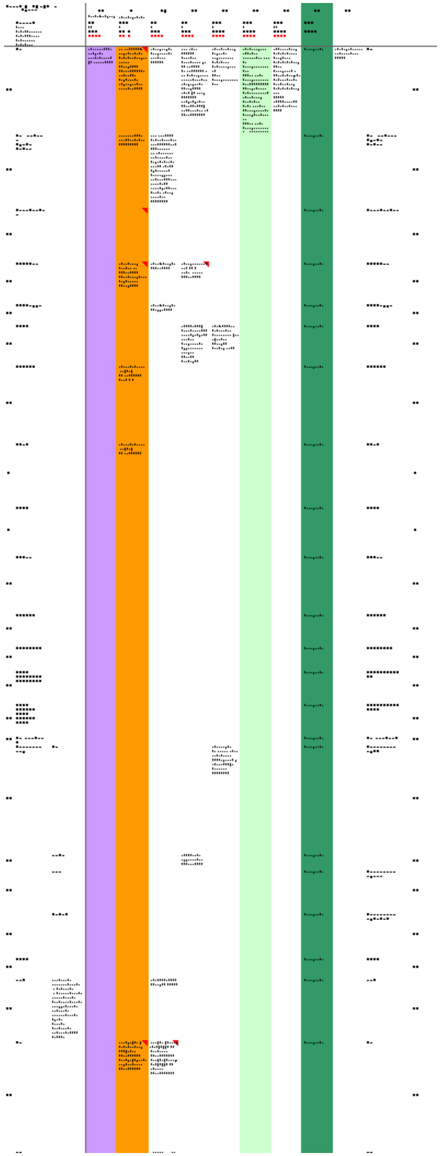
[Melvin Edward Conway, Datamation, April 1968]

**: Melvin E. Conway: How Do Committees Invent? In: F. D. Thompson Publications, Inc. (Hrsg.): Datamation. Band 14, Nr. 5, April 1968, S. 28–31 (english, melconway.com [05. February 2017]).*

Business Continuity Strategies

Business Continuity Planning – Exercise – 2010





Business Continuity Planning – Exercise – Conclusion

ISO 22301: Business Continuity Management System

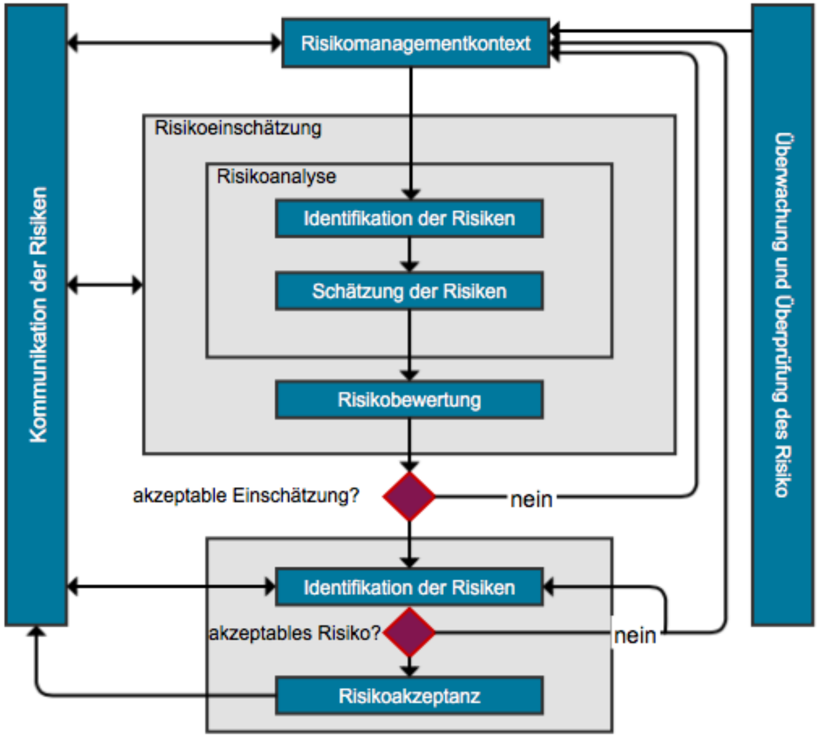
- Organization / Roles & Responsibilities
- Developing Business Continuity Strategies
- Risk Evaluation & Control
- Business Impact Analysis
- Crisis Communications
- Coordination with External Agencies
- Emergency Preparedness & Response
- Awareness & Training Programs
- Developing & Implementing BCPs
- Business Continuity Plan Exercise, Audit & Maintenance

BCMS – Strategic Level

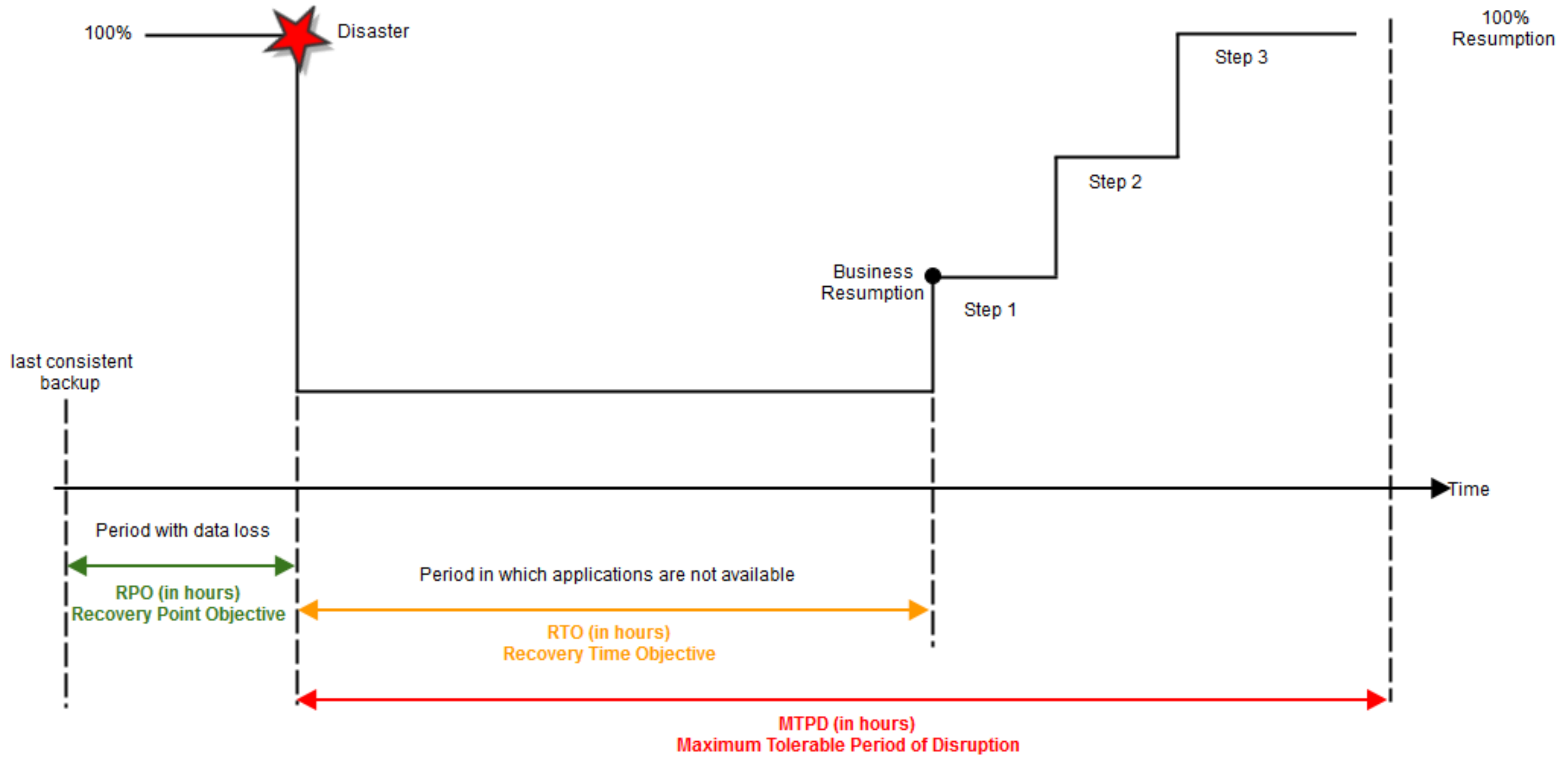
- Corporate (Organization) Strategy
    - DENIC’s Vision and Mission
- Scope of BCMS ⇔ Scope of ISMS
- Integrated Approach
    - Business Continuity Management (ISO 22301)
    - Information Security Management (ISO/IEC 27001)
    - Risk Management (ISO/IEC 27005)
- Policy and Management Review
- Roles, Responsibilities and Authorities

Risk Evaluation & Control

- Risk Management Process
- Business Impact Analysis (BIA)



Business Impact Analyse (BIA)



**: Defining RTO, RPO and MTPOD (http://www.bcmpedia.org/w/images/8/83/Recovery_Objectives_RTO_RPO_and_MTPD.png) [05. February 2017].*

BCMS – Tactical Level

- Prioritized Activity(ies) Recovery Strategy
- Resource Recovery Strategy
- Business Continuity Arrangements
- Crisis Communication
- Awareness Programme

Business Continuity Strategies

- Business Continuity Approaches:
  - Recovery Protection: (non-critical) implementing prioritized actions to return business functions to operation following a disaster.
  - Continuity Protection (critical): implementing advanced actions to respond to a disaster in a manner that critical business functions continue without any interruption.

Conway’s “clean slate" approach

Conway's insight suggests a "clean slate" approach to alignment:

1. Define the business mission;
2. Learn the business processes from business owners;
3. Reengineer these business processes to fit the mission; and
4. Structure the IT organization to support the reengineered business processes.

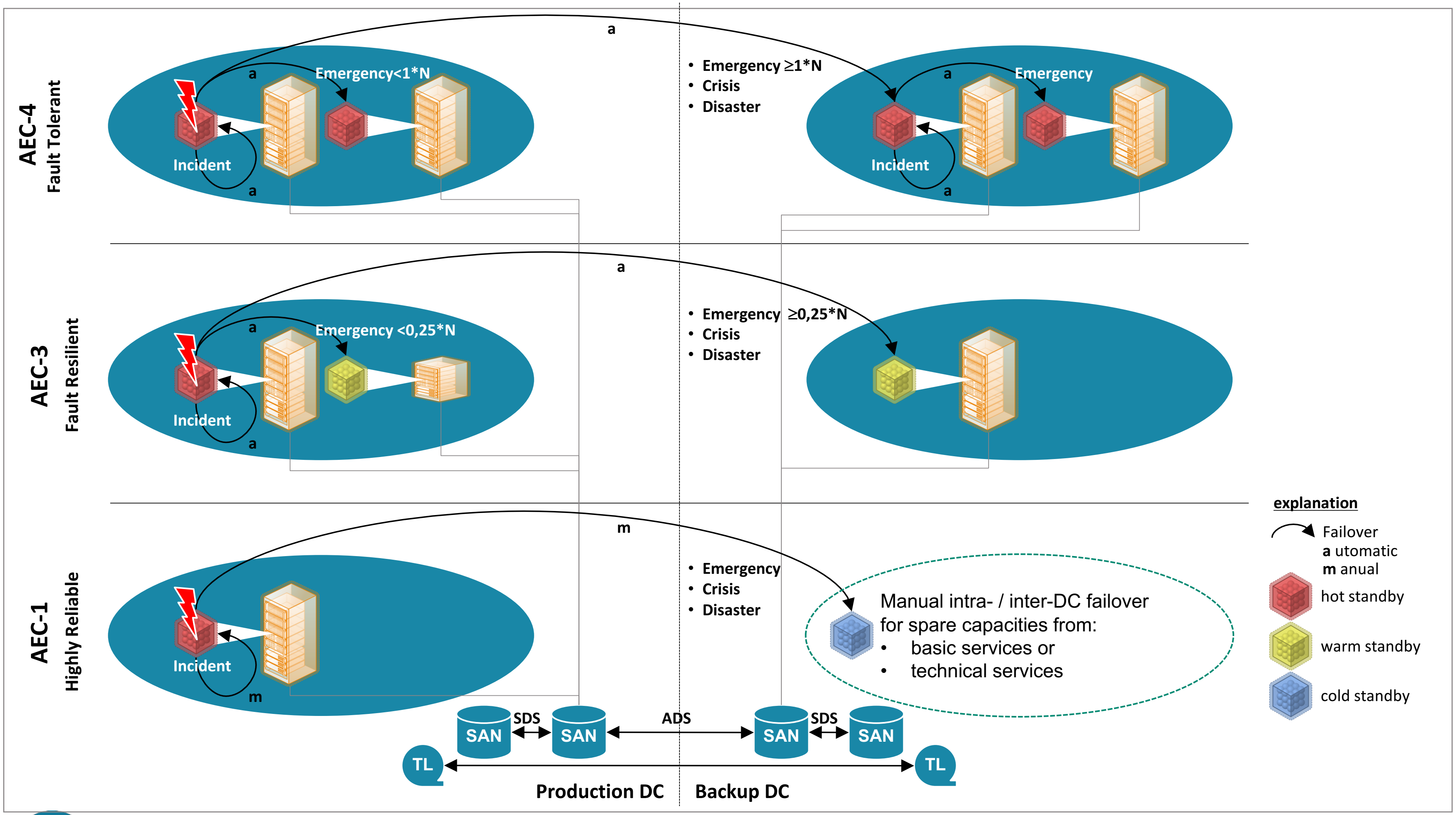
**: David Dikel, David Kane: Conway’s Law Revisited. Successfully Aligning Enterprise Architecture. In: informIT. Prentice Hall PTR, 1. Mai 2002 (english, smu.edu [PDF; 05. February 2017].*

Availability Environment Classification (AEC)

Availability Class		Indicative RPO/RTO*	Recovery Strategy
AEC-5	**Disaster Tolerant** – Business functions must be ensured available in all circumstances.	RTO: sec. – min. RPO: null	• hot standby platform, • synchronous data disk mirroring • DR location(s)
AEC-4	**Fault Tolerant** – Business functions that demand continuous computing and where any failure is transparent to the user. This means no interruption of work; no transactions lost; no degradation in performance; and continuous 24x7 operation.	RTO: sec. – min. RPO: sec. – min.	• hot standby platform • synchronous data disk mirroring
AEC-3	**Fault Resilient** – Business functions that require uninterrupted computing services, either during essential time periods, or during most hours of the day and most days of the week throughout the year.	RTO: hours RPO: sec. – min.	• hot/warm standby platform • (a)synchronous disk mirroring
AEC-2	**High Availability** – Business functions that allow minimally interrupted computing services, either during essential time periods.	RTO: hours RPO: hours	• hot/warm standby platform • synchronous backup (tape or disk)
AEC-1	**Highly Reliable** – Business functions that can be interrupted as long as the availability of the data is insured.	RTO: hours RPO: hours – days	• warm/cold standby platform • asynchronous backup (tape or disk)
AEC-0	**Conventional** – Business functions that can be interrupted and where the availability of the data is not essential.	RTO: days – weeks RPO: none	• none or cold standby platform • no backup

**: Harvard Research Group (HRG) Availability Environment Classification (AEC) - http://www.hrgresearch.com/pdf/AEC%20Defintions.pdf [05. February 2017].*

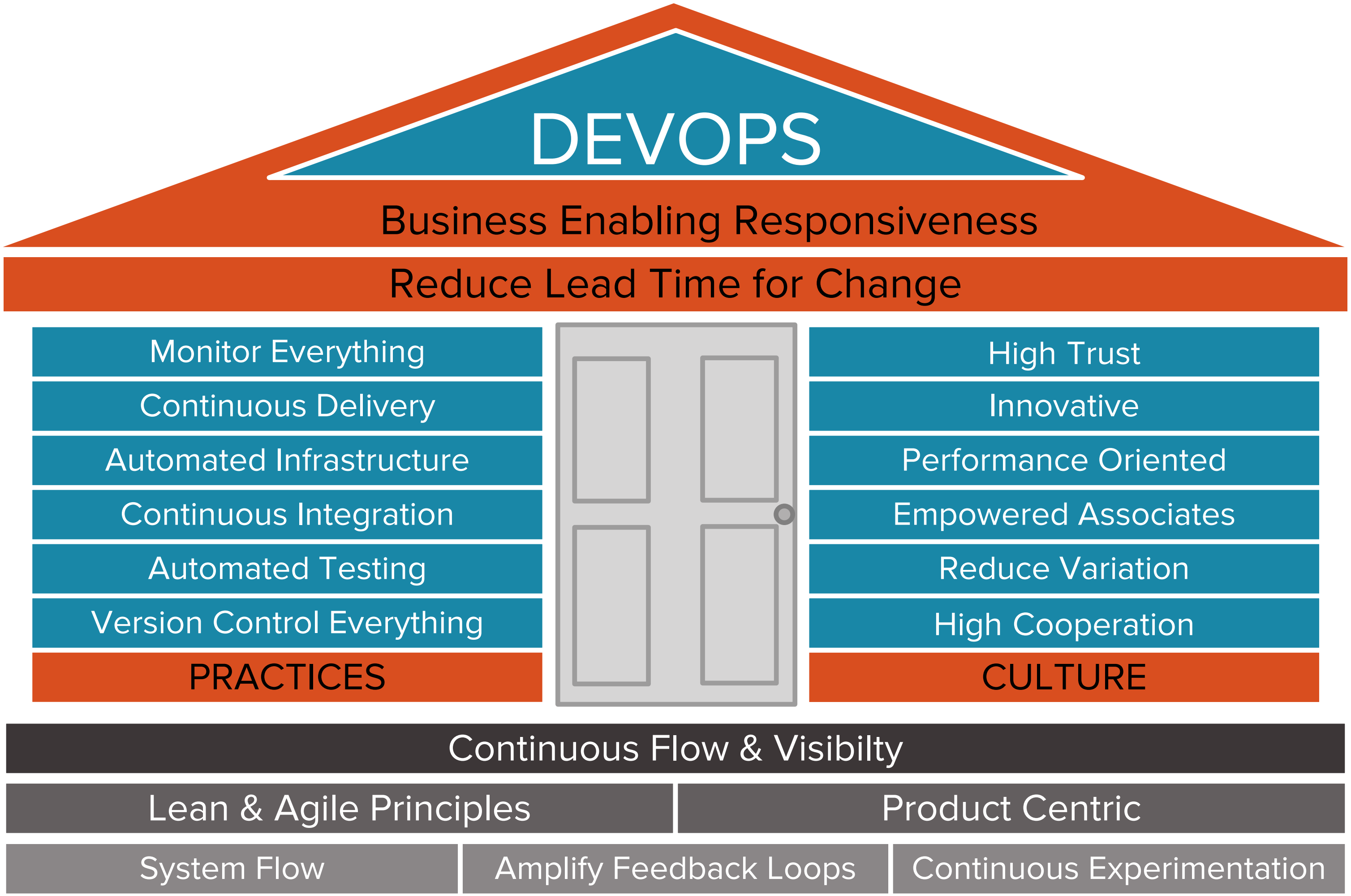
AEC – Recovery Strategies



BCMS – Operational Level

- Operational Planning and Control
- Business Continuity Plan(s)
- Incident Management
- Exercising and Testing
- Training and Competence
- Maintenance

Cultural Change – DevOps



DEVOPS

Business Enabling Responsiveness

Reduce Lead Time for Change

Monitor Everything

Continuous Delivery

Automated Infrastructure

Continuous Integration

Automated Testing

Version Control Everything

PRACTICES

High Trust

Innovative

Performance Oriented

Empowered Associates

Reduce Variation

High Cooperation

CULTURE

Continuous Flow & Visibilty

Lean & Agile Principles

Product Centric

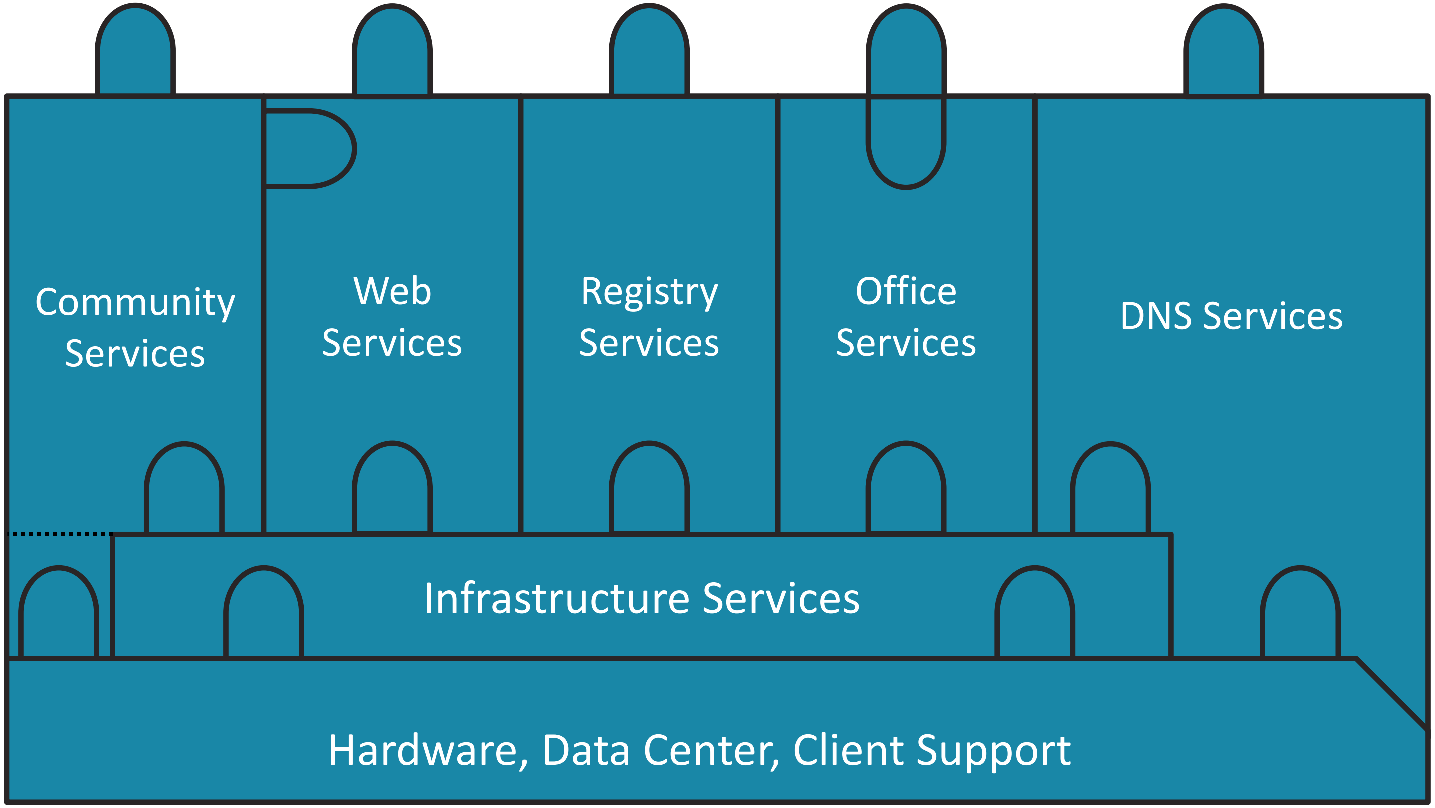
System Flow

Amplify Feedback Loops

Continuous Experimentation

*: *The Simple Math of DevOps, Lee Reid, 2015 https://devops.com/interconnect-2016-culture-matters [05. February 2017].*

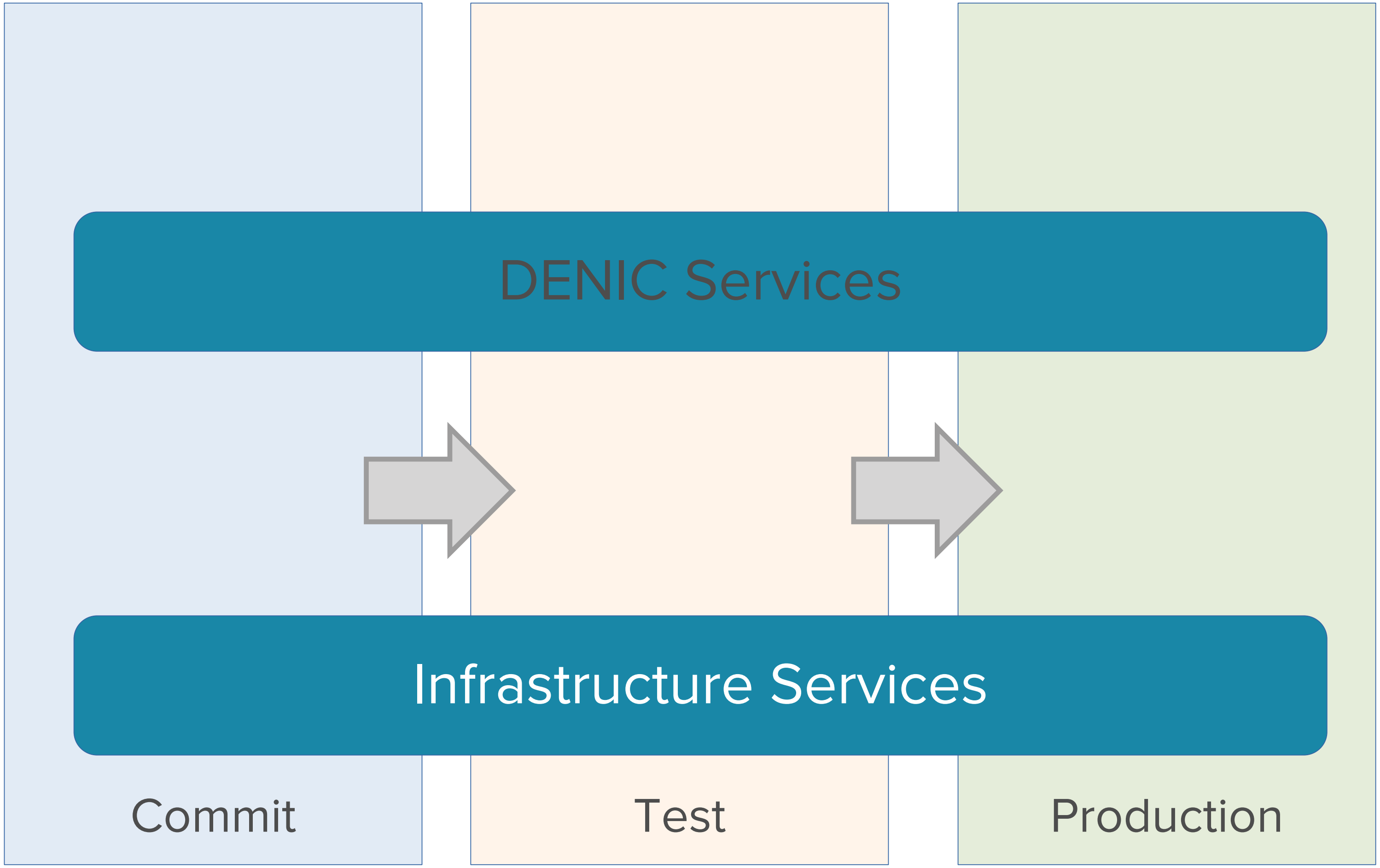
DevOps – Cross-Functional Service Teams



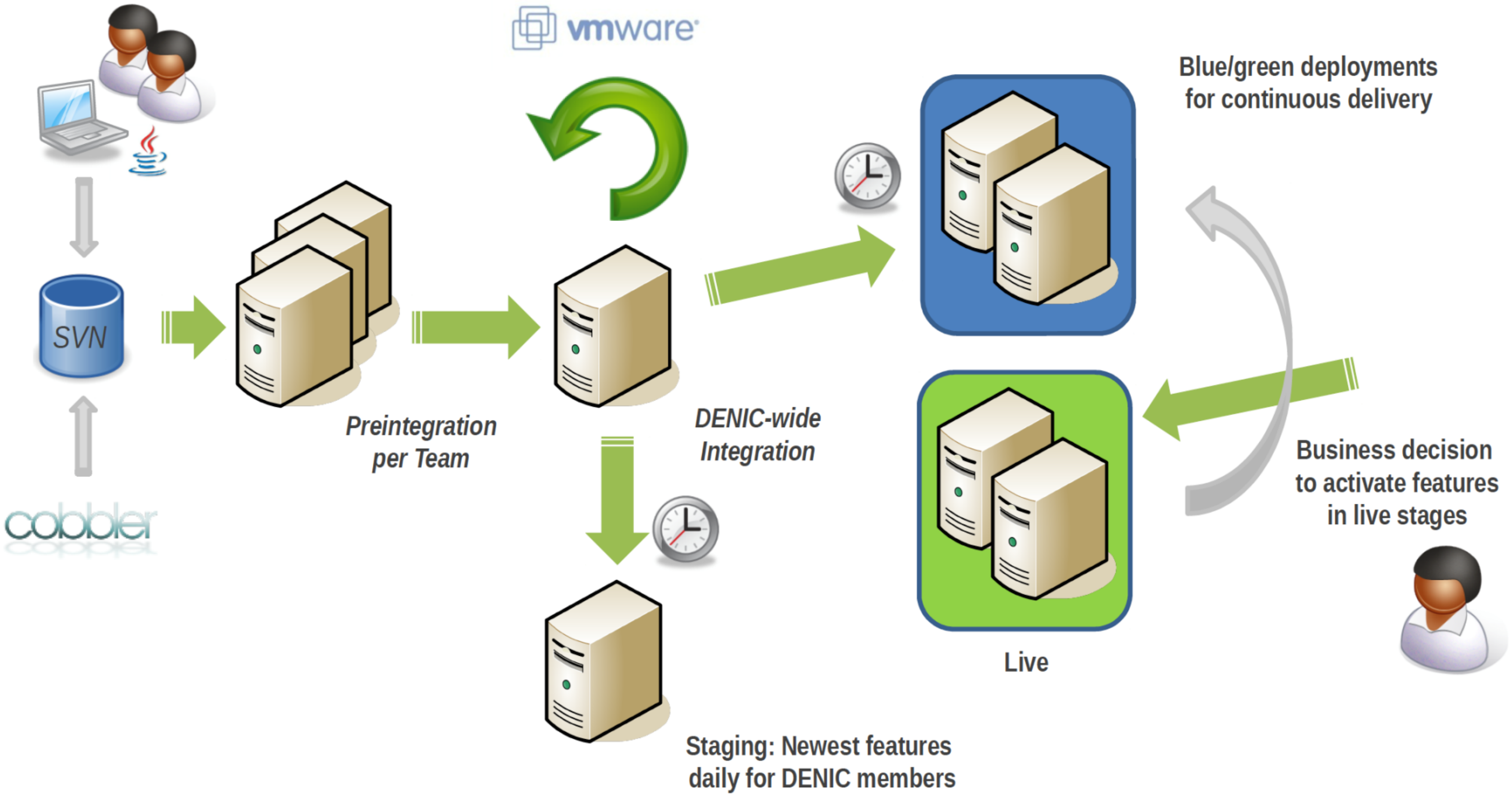
Principles for System Design

- Full-Stack-Automation
- Easy
- Repeatable
- Secure
- Up-to-date
- Homogenous

DENIC Services – Pipelines and Staging



Registry Services – Pipelines and Staging



Preintegration per Team

DENIC-wide Integration

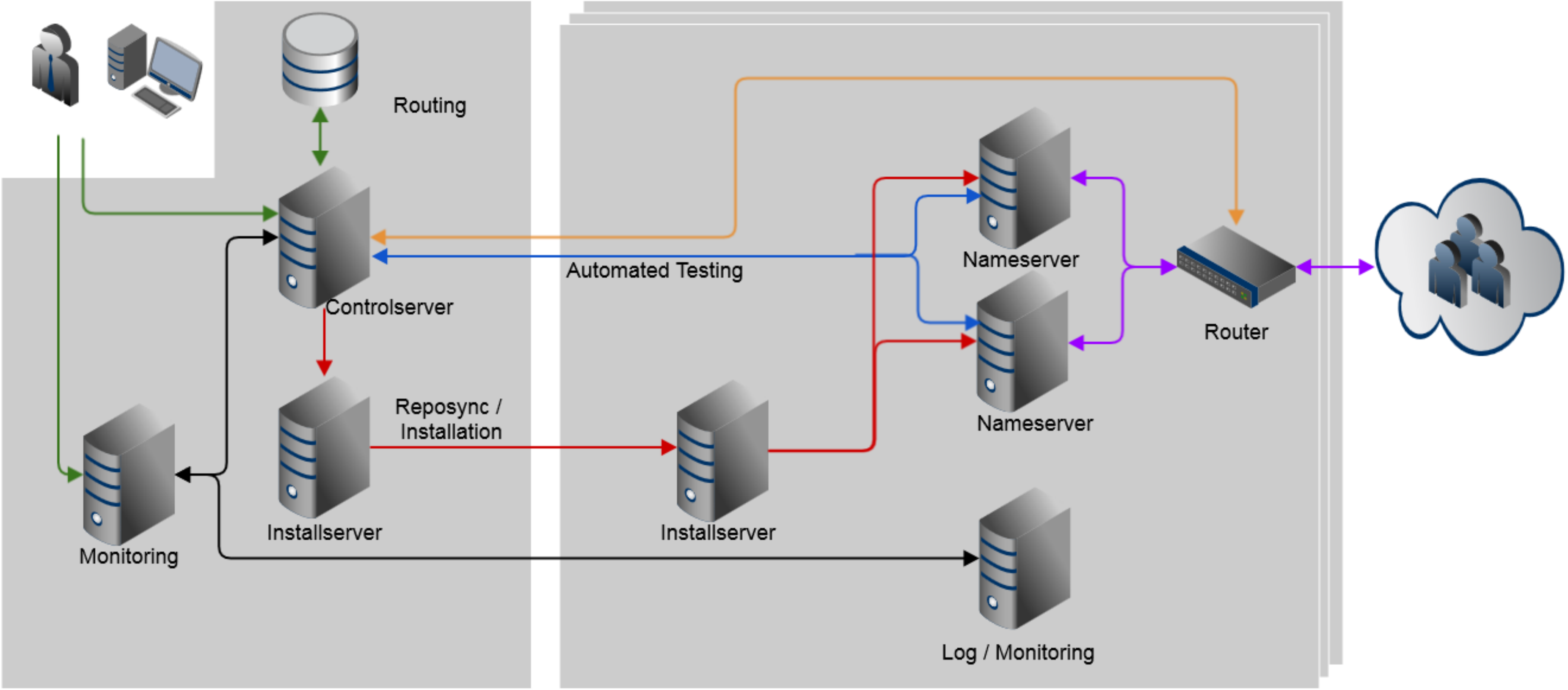
Blue/green deployments for continuous delivery

Live

Business decision to activate features in live stages

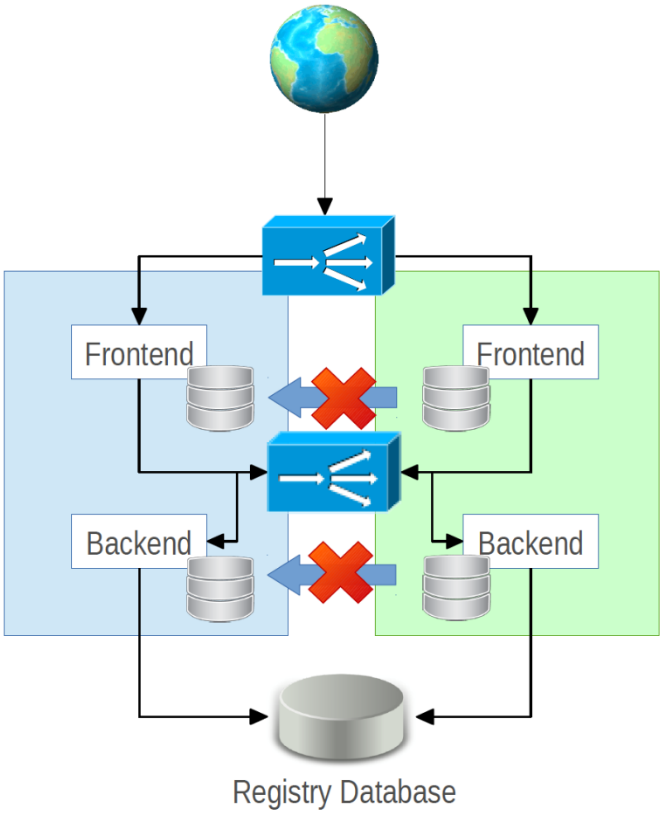
Staging: Newest features daily for DENIC members

DNS Service – Pipelines and Staging

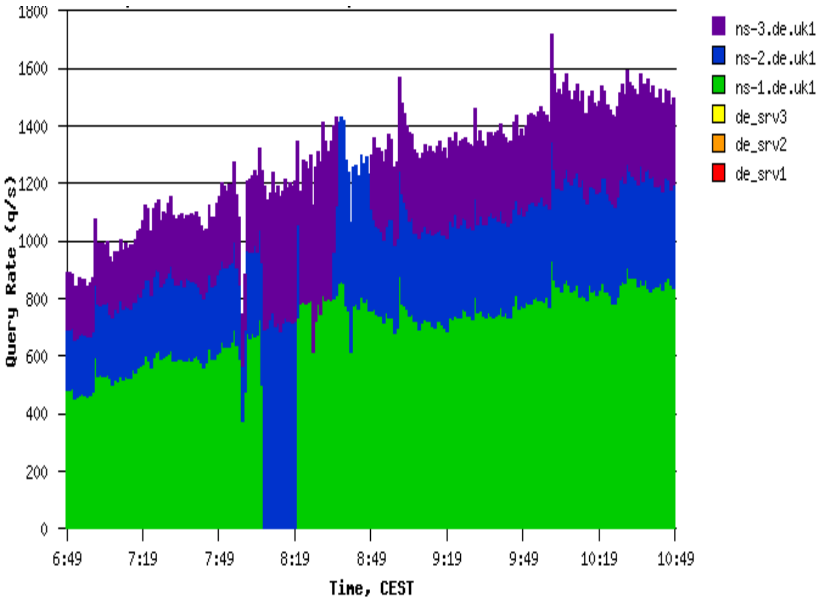


BCM Deployment Strategies

- Blue-Green-Deployment

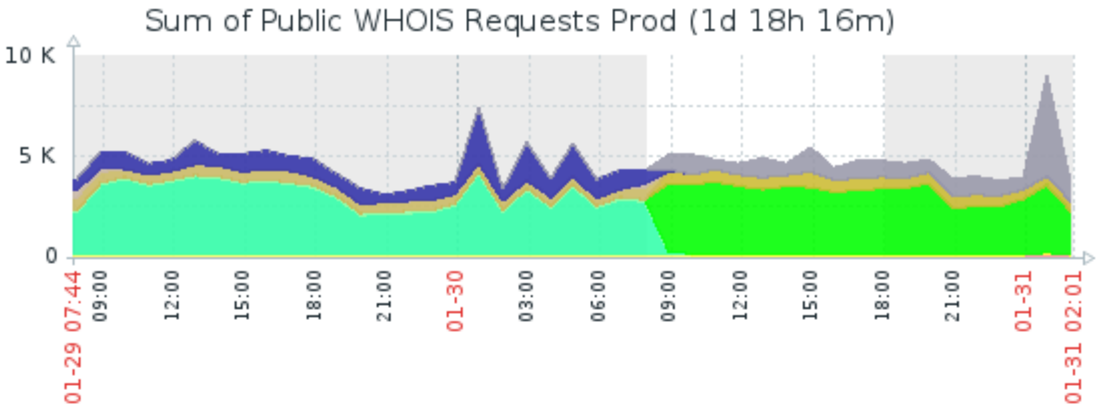


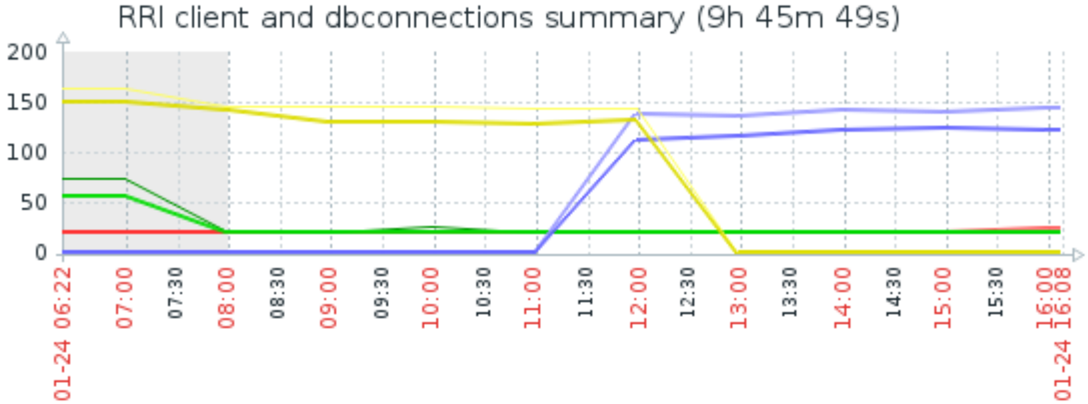
- Serial Deployment



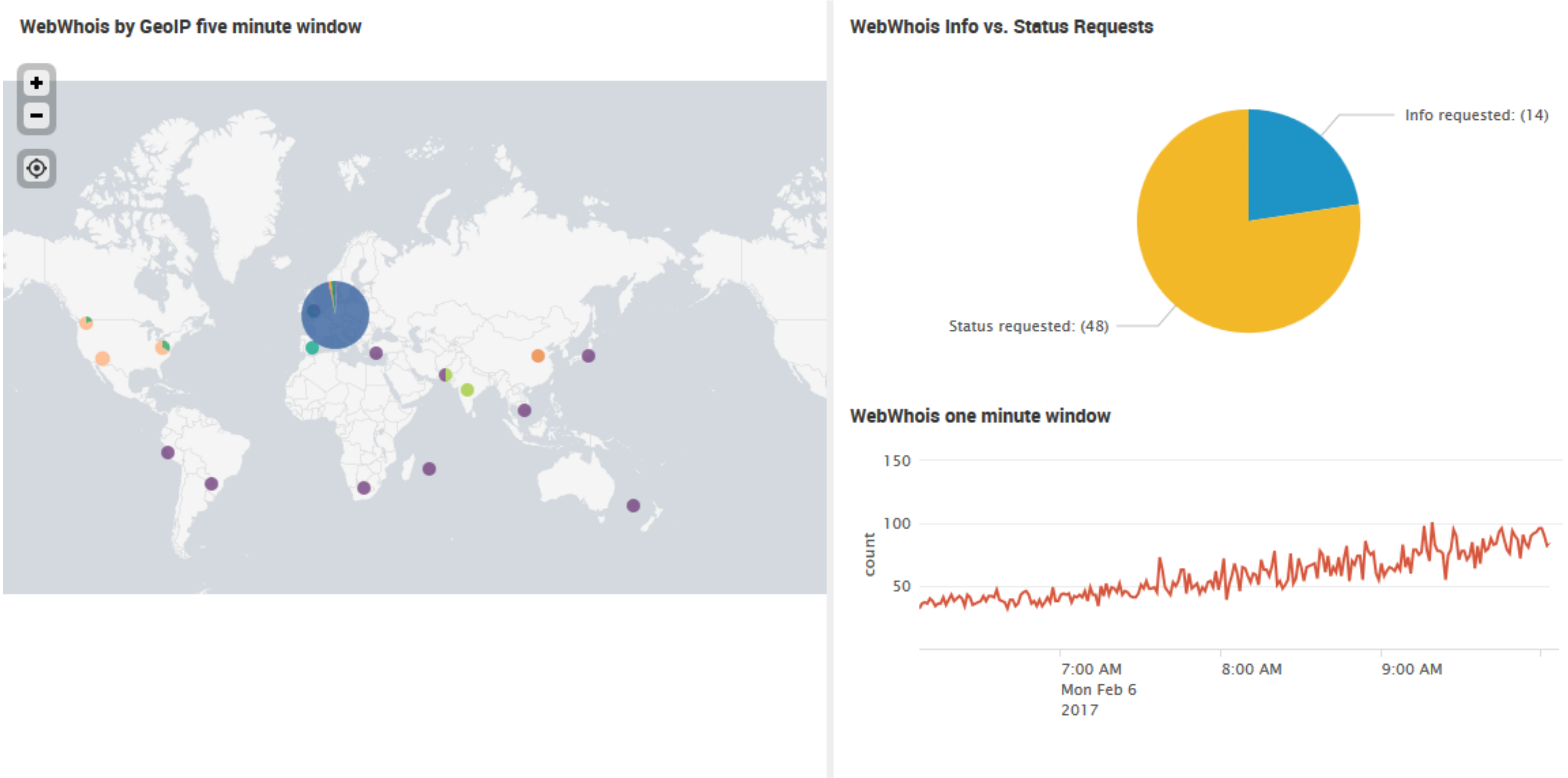
*: *Blue Green Deployment https://martinfowler.com/bliki/BlueGreenDeployment.html [05. February 2017].*
*: *Deployment Strategies for Distributed Applications on Cloud ComputingInfrastructures, University of Amsterdam [05. February 2017].*

B/G Deployment FRA to AMS

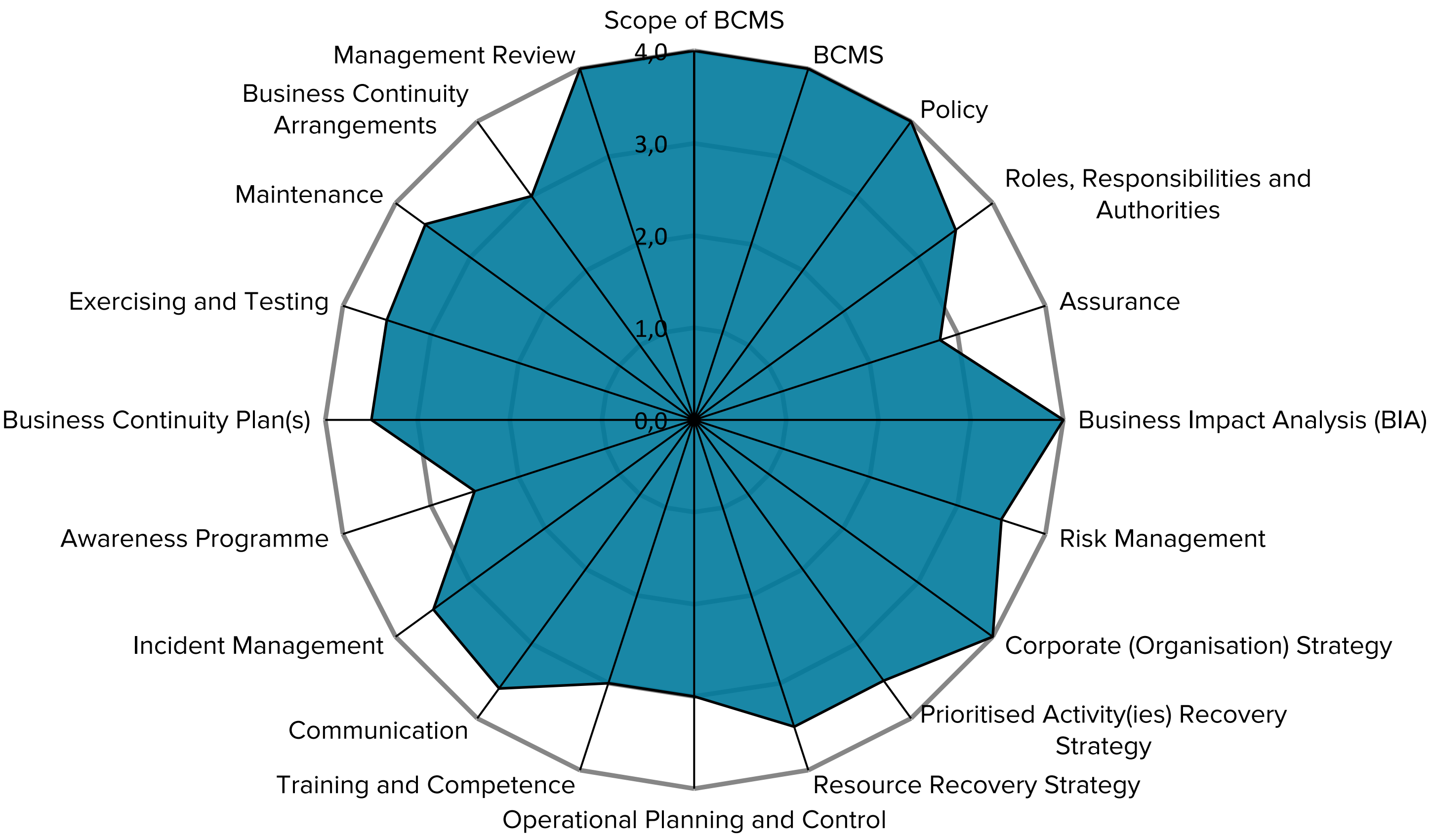




Monitoring – Registry Services - whois


WebWhois by GeoIP five minute window
WebWhois Info vs. Status Requests
Info requested: (14)
Status requested: (48)
WebWhois one minute window
150
100
50
count
7:00 AM
Mon Feb 6
2017
8:00 AM
9:00 AM

BCMS – DENIC –2016



Thank
You !

Questions ?

Contact:

Boban Kršić

<krsic@denic.de>

PGP Key-ID:
0x43C89BA9