FSTA
Årsmøde 2014
Kolding

Beredskabskrav til It-infrastruktur

23. september 2014
Faruque Sayed
Team Consultants

PRÆSENTATIONENS INDHOLD

PRÆSENTATIONENS INDHOLD

1. **Beredskab og It-beredskab**
2. **Hvilke normer gøre sig gældende ved implementering**
3. **Hvordan integreres processen i organisationen**

(Bemærk venligst, at ikke slides bliver behandlet ved gennemgangen)

BEREDSKAB OG IT-BEREDSKAB

IT-BEREDSKABS MÅLSÆTNINGER

- It-beredskab i en organisation skal understøtte den samlede It-drift på et passende og forud defineret niveau, til at minimere konsekvenserne af driftsafbrydelser som følge af nødsituationer eller katastrofer.

- Forretningsområderne skal understøttes af It-beredskab med det formål at kunne håndtere kritiske arbejdsgange under en nødsituation eller katastrofe.

4 FOKUSOMRÅDER FOR IT-BEREDSKAB

- Sandsynlighed for nedbrud og driftsforstyrrelser, inkl. organisationens evne til at overvåge beredskabsforhold, opdage og reagere på forekomsten af nedbrud og driftsforstyrrelser, samt udpege kritiske interne ressourcer, eksterne samarbejdspartnere og leverancer;

- Forretningsmæssige konsekvenser for nedbrud og driftsforstyrrelser samt genskabelse af normaldrift efter på forhånd definerede prioriteringer i samråd med forretningen;

- Organisationens arbejde med normalisering af nødvendige driftsprocesser beskrevet i It-beredskabsplan, afprøve genskabte driftsforhold i samarbejde med forretningen og returnere til normaldrift indenfor definerede rammer; samt

- Overholde politiske forventninger (eksempelvis patient sikkerhed), lovmæssige krav (kritiske systemers tilgængelighed, civil beredskab) samt organisationens strategiske beslutninger (inklusiv fremtidig udviklingsplan for infrastruktur baseret på teknologividen og teknik).

INTRO TIL BEREDSKAB OG IT-BEREDSKAB

WHAT IS BCM?

'Business Continuity Management (BCM) is an holistic process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause.

It provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of key stakeholders, reputation, brand and value-creating activities.'

BS 25999-1:2006

Standards for Business Continuity Management comprises 2 parts:

- BS 25999-1:2006 BCM - Part 1: Code of Practice
- BS 25999-2:2007 BCM - Part 2: Specification
- DS/ISO 22301:2012 BCM Requirements
- DS/ISO 22313:2013 BCM Guidance

BCM BACKGROUND PERSPECTIVE

- BCM methodology was a spin-off development from IT Disaster Recovery methodology
- Developed over ca. 3 – 4 decades
- Initial effort was to embrace business areas alongside IT
- Natural catastrophe was in focus in early days
- Diseases and epidemics came next
- Man made disasters, including war, terror activities were included later
- Due to randomness of possible scenarios focus was led more to the impact and consequences
- Resilience activities are limited to well known issues
- Major focus is given to 'how to return to normalcy'

WHAT IS ICT-CM (OR IRBC)?

IRBC is Concepts and principles of ICT readiness for business continuity, that provides frameworks of methods and processes to identify and specify all aspects for improving organizations ICT readiness to ensure business continuity.

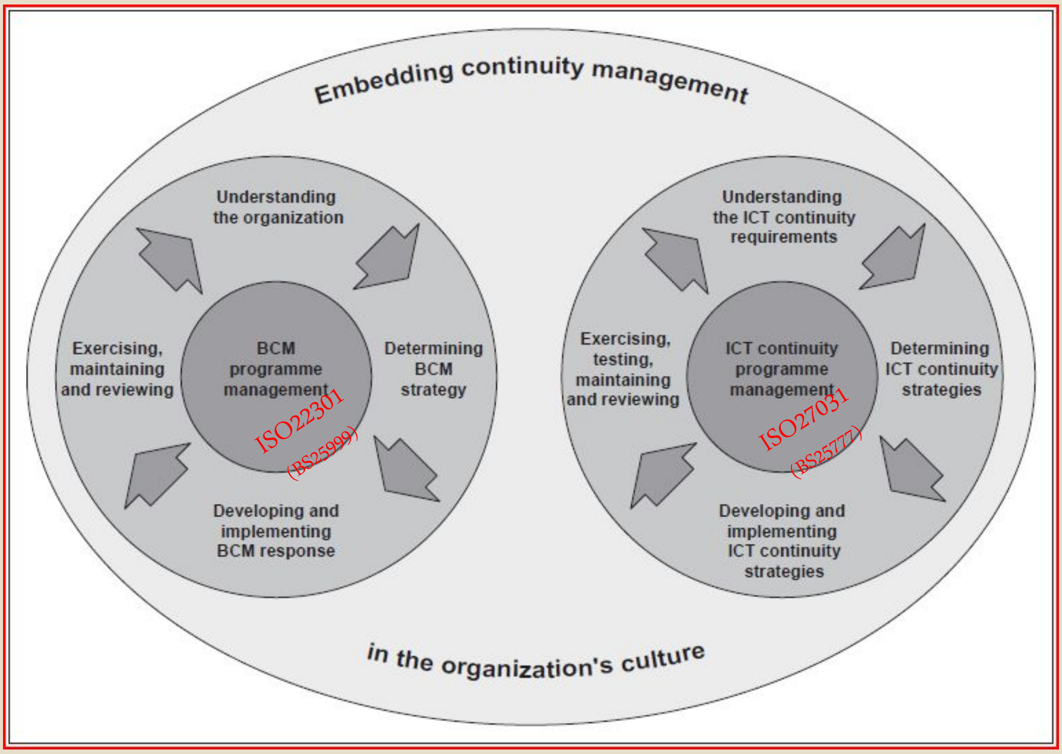
It applies to an organization's program requiring its ICT services and infrastructure to be ready to support its business operations in the events of emerging incidents and related disruptions that could affect continuity (including security) of critical business functions…
ICT continuity supports the overall BCM process of an organization.

DS/ISO 27031:2011

Standards for IRBC is complex and comprises many parts:

- BS 25777-1:2008 ICT-CM: Code of Practice
- DS/ISO 27031:201 ICT Readiness for Business Continuity

BCM AND ICT READINESS ALIGNMENTS



Embedding continuity management
Understanding the organization
Exercising, maintaining and reviewing
BCM programme management
Determining BCM strategy
Developing and implementing BCM response
ISO22301
(BS25999)
Understanding the ICT continuity requirements
Exercising, testing, maintaining and reviewing
ICT continuity programme management
Determining ICT continuity strategies
Developing and implementing ICT continuity strategies
ISO27031
(BS25777)
in the organization's culture

IRBC Principles:

1. Protect
2. Detect
3. React
4. Recover
5. Operate
6. Return

IRBC Elements:

1. People
2. Premises
3. Technology
4. Data
5. Processes
6. Suppliers

HVAD ER SÅ FORSKELLEN?

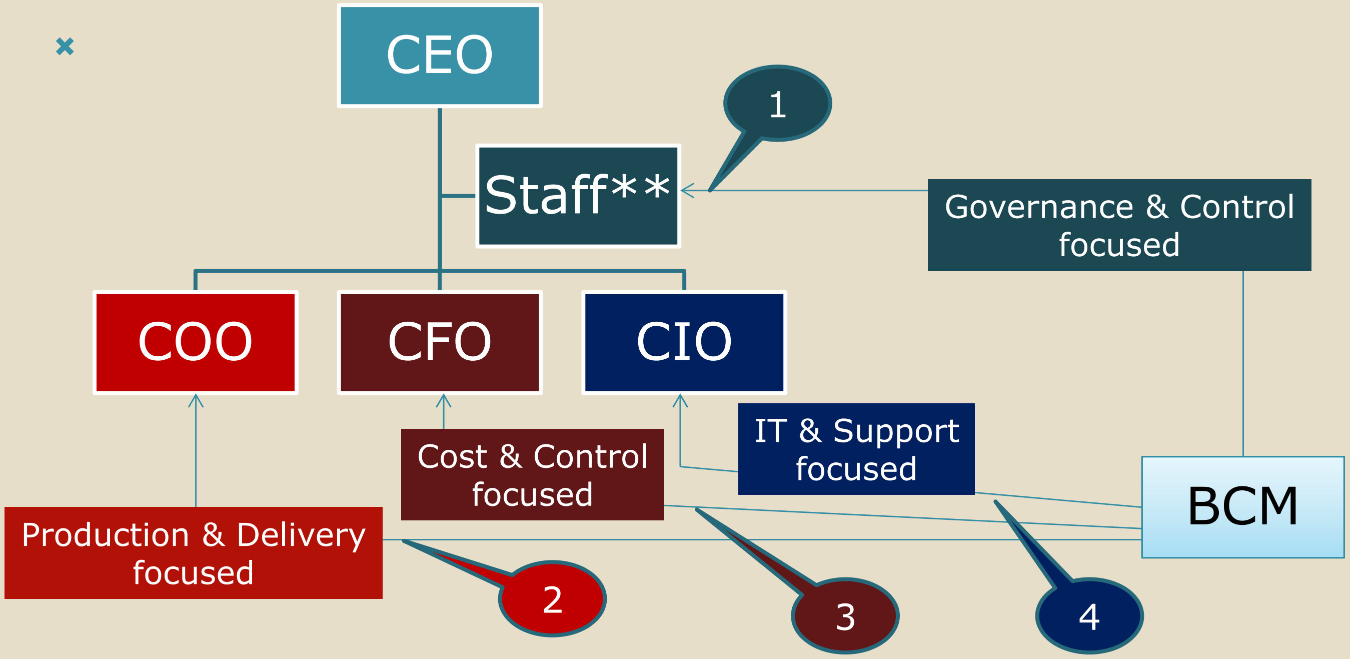
- Omfang og afdækning (hvad)
- Målsætninger og fokusområder (hvad)
- Ansvarsplacering (hvem)
- Involvering i organisationen (hvem)
- Planlægningsproces - parathed (hvordan)
- Løsningsproces (hvordan)
- (… hvornår)

CONTINUAL IMPROVEMENT
PLAN
DO
CHECK
ACT

- - så er der forskrifter

IT eller IKT (ICT) betragtes som en del af service som forretningen bygger sine kerneydelser på

IRBC IN ORGANIZATIONAL STRUCTURE WHEN & WHY



CEO

Staff**

1

Governance & Control focused

COO

CFO

CIO

IT & Support focused

Cost & Control focused

BCM

Production & Delivery focused

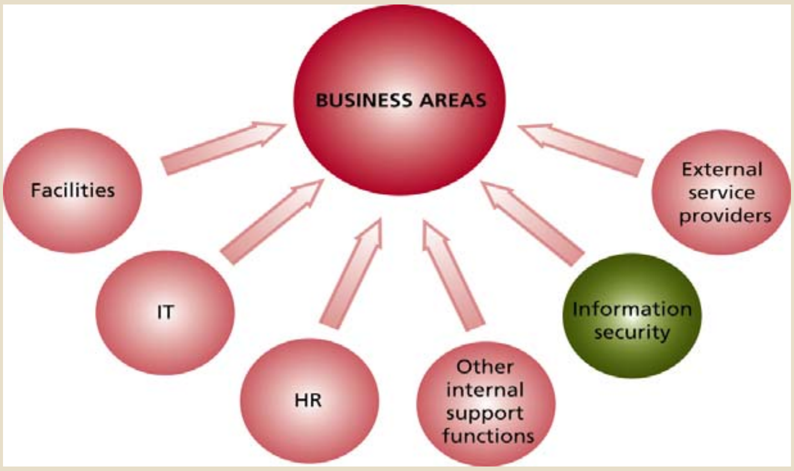
2

3

4

UNDERSTANDING IRBC CAPABILITY

...the capability of the organisation to plan for and respond to incidents and disruptions, in order to continue services at an ***ACCEPTABLE PREDEFINED LEVEL.***



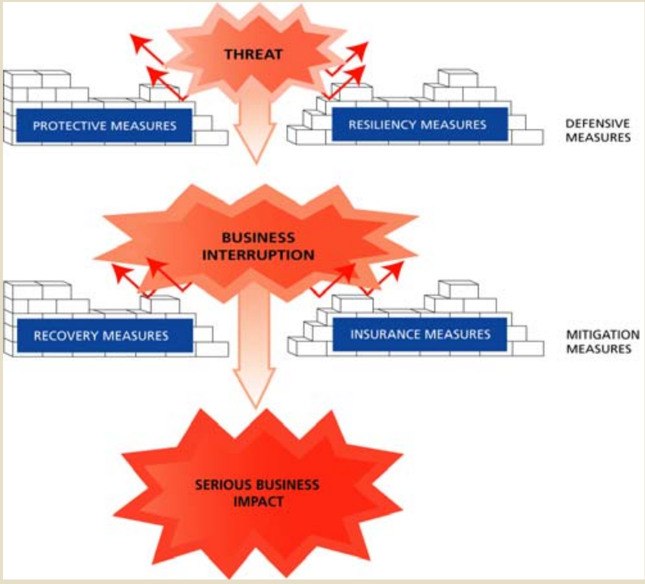
In other words:

- *People*
- *Premises*
- *Technology*
- *Data/Services*
- *Processes*
- *Suppliers*

UNDERSTANDING IRBC MEASURES

In order to protect against risks to business continuity, organisations need to consider an appropriate balance between four types of solution measures:

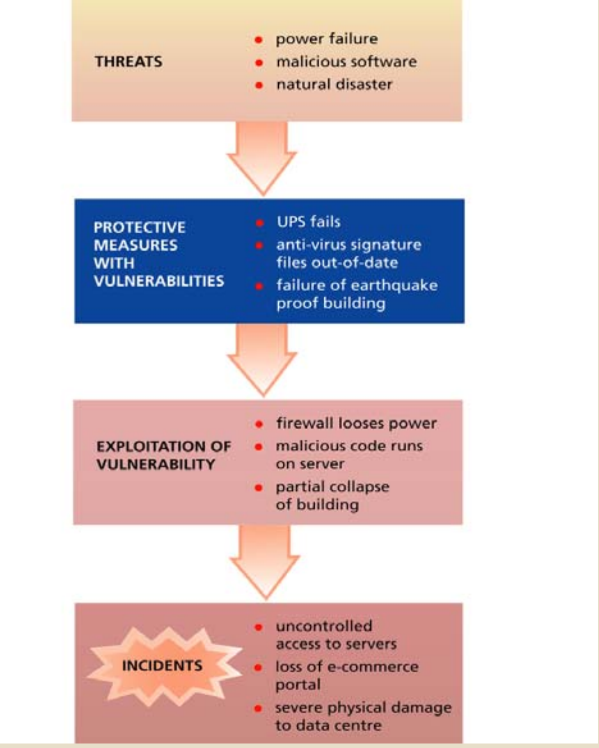
- protective measures – preventing incidents to take place
- resiliency measures – absorbing the impact of incidents when taken place
- recovery measures – recovering from incidents afterwards
- insurance measures – compensating for the impact of incidents



UNDERSTANDING PROTECTIVE MEASURES

Protective or Preventive measures aim to reduce the likelihood of threats materialising into incidents and affecting critical business assets. Examples of protective measures include:

- + Virus protection software
- + Uninterruptible Power Supplies (UPS)
- + Earthquake-proof buildings.



THREATS
- power failure
- malicious software
- natural disaster

PROTECTIVE MEASURES WITH VULNERABILITIES
- UPS fails
- anti-virus signature files out-of-date
- failure of earthquake proof building

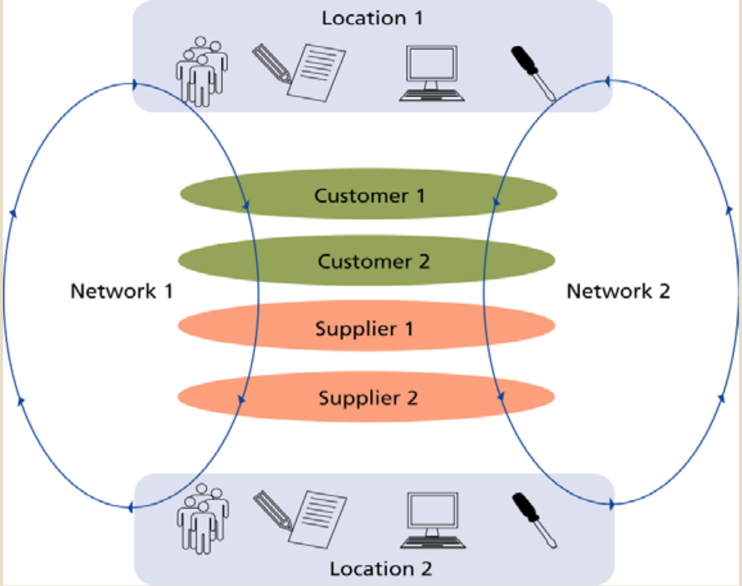
EXPLOITATION OF VULNERABILITY
- firewall looses power
- malicious code runs on server
- partial collapse of building

INCIDENTS
- uncontrolled access to servers
- loss of e-commerce portal
- severe physical damage to data centre

UNDERSTANDING RESILIENCY MEASURES

Resiliency measures aim to absorb the impact of an incident by avoiding *single points of failure* and enable an *acceptable level of service* to continue with minimum disruption. Examples include:

- ✓ Mirrored and remote storage to share workload and takeover at short notice,
- ✓ multiple call centres around the world to share calls and continue servicing,
- ✓ Computer networks that can re-route traffic around failed components.



UNDERSTANDING RECOVERY MEASURES

Recovery measures are measures which are invoked if both protective and resiliency measures prove <u>insufficient or uneconomic</u>. Examples include:

- + Work area recovery – re-locate staff to alternative premises
- + Site recovery – salvage and restore a damaged site
- + Human resources planning – to plan for unavailability of critical staff

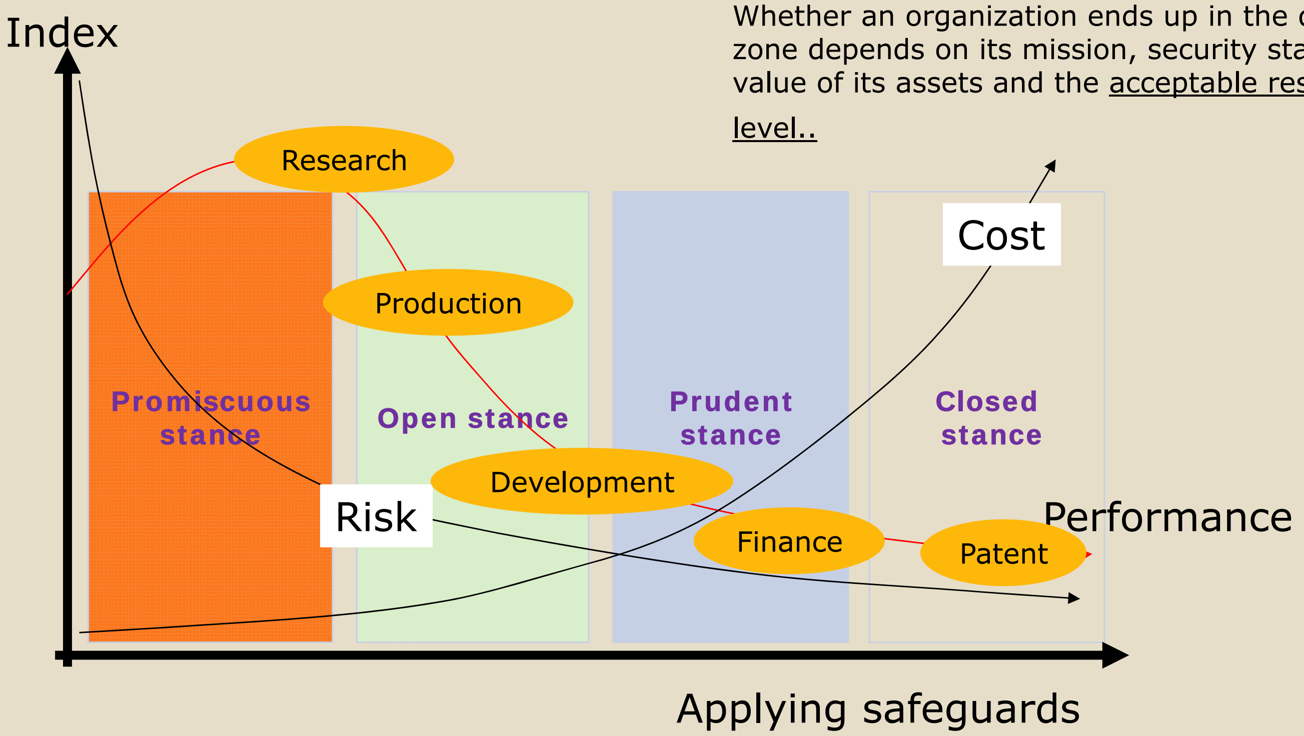
UNDERSTANDING INSURANCE MEASURES

Insurance

- Insurance transfers some of the financial risk to a third party – the insurance company – and provides compensation for losses in return for a risk premium.
- We should be careful about relying too heavily on insurance.
- Policies can be restrictive in terms of the risks included and the level of coverage provided.

OPTIMAL POINT FOR ROI (USE A R S A)

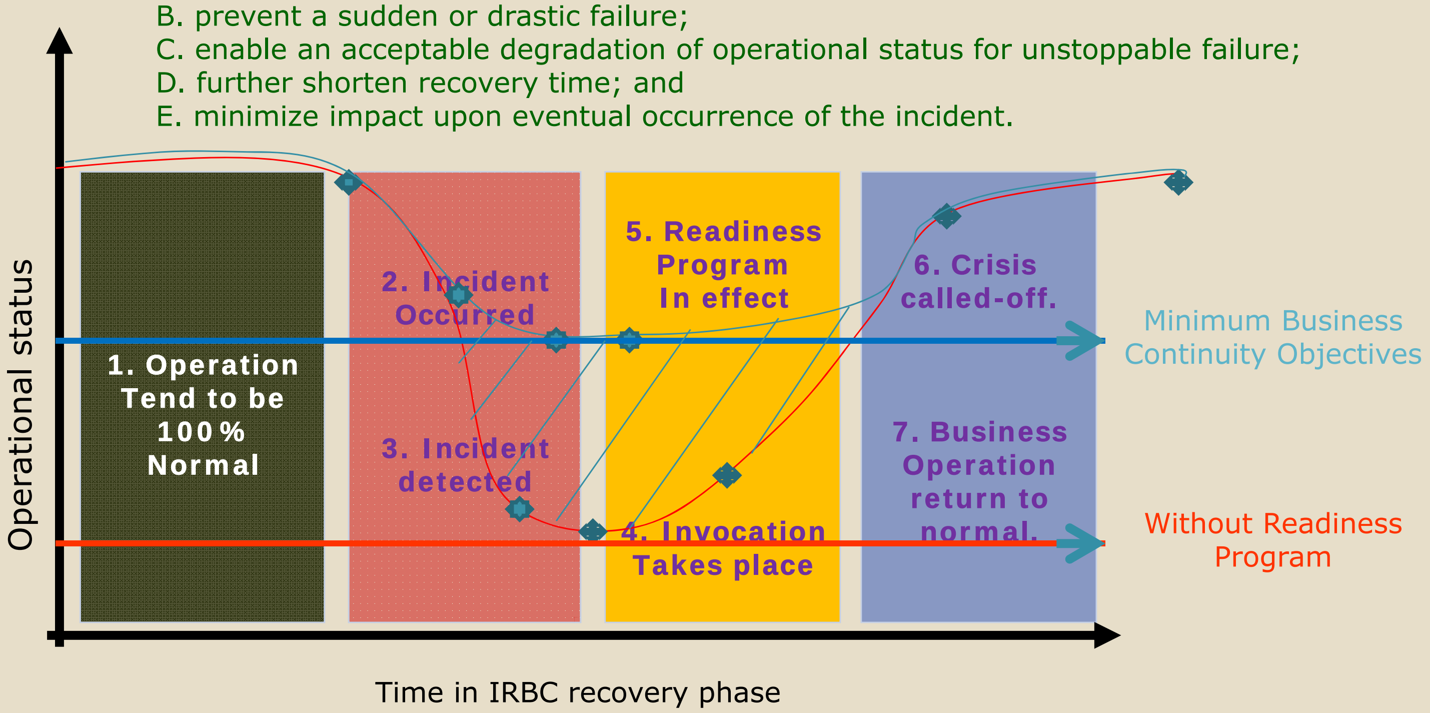
Whether an organization ends up in the desired zone depends on its mission, security stance, the value of its assets and the acceptable residual risk level..



Source: John McCumber, Assessing and Managing Risks - modified

IRBC ACTIVITIES WOULD AIM TO DO THE FOLLOWING

A. improve the incident detection capabilities;
B. prevent a sudden or drastic failure;
C. enable an acceptable degradation of operational status for unstoppable failure;
D. further shorten recovery time; and
E. minimize impact upon eventual occurrence of the incident.



Operational status

1. Operation Tend to be 100% Normal

2. Incident Occurred

3. Incident detected

4. Invocation Takes place

5. Readiness Program In effect

6. Crisis called-off.

7. Business Operation return to normal.

Minimum Business Continuity Objectives

Without Readiness Program

Time in IRBC recovery phase

HVORDAN HÆNGER DET SAMMEN MED IRBC?

- Understøtter kritiske forretningsområder (hvad)
- Parathed for definerede serviceniveau (hvad)
- Ansvar uddelegeres i organisationen (hvem)
- Både eksterne og interne involveres (hvem)
- Man kender organisationens risikovillighed (hvordan)
- Minimumsniveauet er på forhånd kendt (hvordan)
- Vi skal gennemgå de 6 faser mht. tidsaspektet (hvornår)

- husk også på, at sammenhængen mellem organisationens strategi, It-strategi, målsætninger for driftens kapacitet samt performance (ikke mindst også It-sikkerheds strategi og –politik) har relationer til GRC, som igen til infrastruktur samt facilities!

Igen, IT betragtes som en del af service som forretningen bygger sine kerneydelser på og IT er afhængig af Facilities og Infrastruktur

DEFINING CRISIS MANAGEMENT

"The overall coordination of an organization's response to crisis, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organizations profitability, reputation, and ability to operate"

- The Disaster Recovery Journal

"… Crisis Management is often seen as the domain of communication and PR practitioners with the BCM practitioner in a support role, … Crisis Management is also seen as responding to non-physical as well as physical events such as financial performance and reputation damaging incidents'.

- Good Practice Guidelines 2010

DEFINING EMERGENCY MANAGEMENT

"The capability that enables an organization or community to respond to an emergency in a coordinates, timely, and effective manner to prevent the loss of life and minimize injury and property damage"

- The Disaster Recovery Journal

"… the immediate response to an emergency, such as an Evacuation Plan … emergency planning is normally seen as the domain of 'blue light services' such as police, fire, ambulance and local authorities rather than for organizations in general,."

- Good Practice Guidelines 2010

DEFINING DISASTER RECOVERY MANAGEMENT

> "The technical aspect of business continuity. The collection of resources and activities to re-establish information technology services (including components such as infrastructure, telecommunication, systems, application and data) at an alternate site, following a disruption of IT services."
>
> - The Disaster Recovery Journal

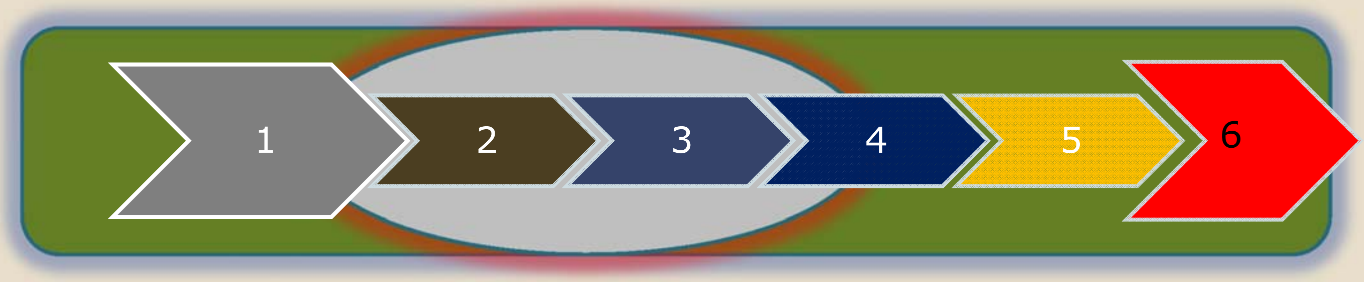
ISSUES YOU SHOULD CONSIDER FOR SERVICE RECOVERY MANAGEMENT

Service Recovery issues:

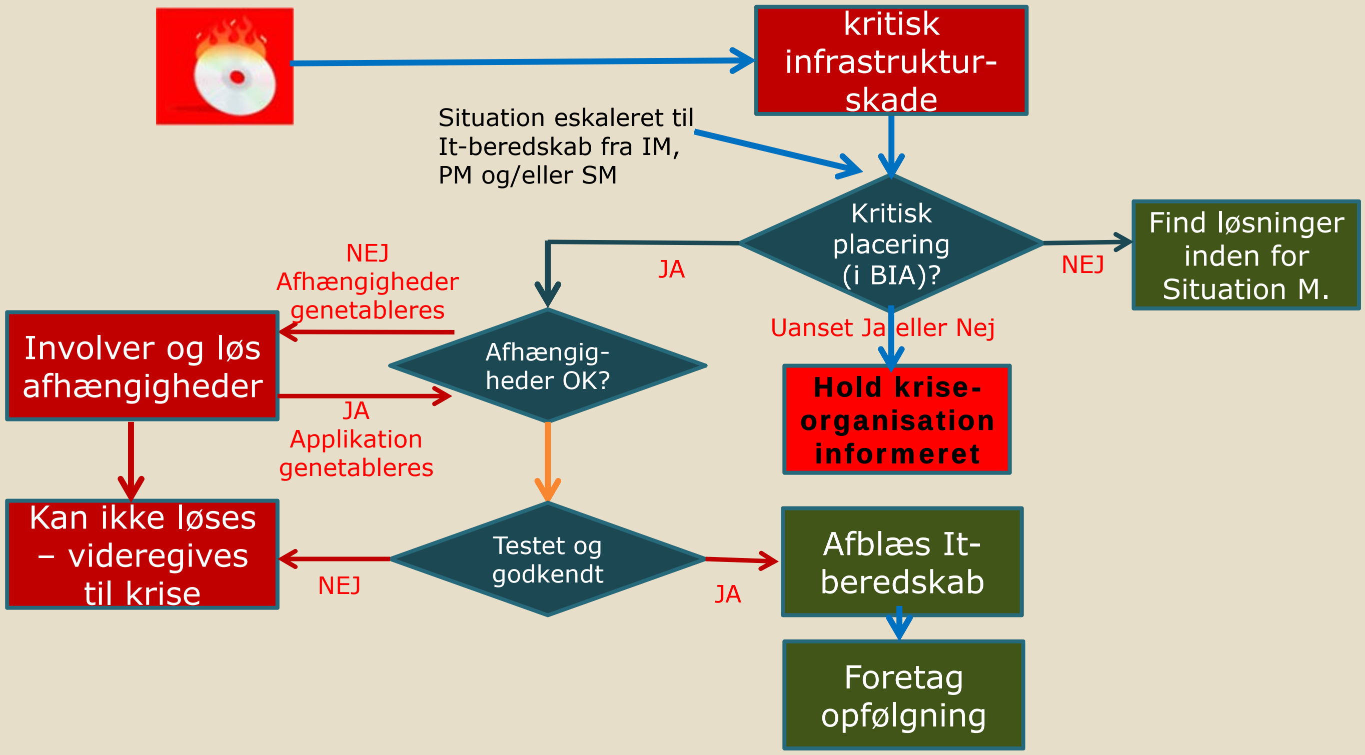
- Coverage & limitations
- Influences on BIA and embedding in the organization
- Emergency Management in BCM context
- Emergency Response Team in Crisis Organization
  - Decision process & template
  - Escalation
  - Invocation
  - Delegation of tasks
  - Communication & coordination – internal & external
  - Call-off
  - Lessons learnt
- Rehearsal & test
- Requirements for Service Level Agreement
- Standards and relevant practices

NORMALDRIFT TIL RESTORE/RECOVERY (ENKELT STÅENDE)

1. Almindelig enkeltstående sag for applikation / system.
2. Behandles efter IM, PM og SM procedurer og prioriteter for SLA-kategori.
3. Ét eller flere niveau(er) af support level kan være anvendt (1., 2., og 3.).
4. CAP / CAB er anvendt.
5. Dokumentation efter alm. RM's drifts norm og krav.
6. Problemet ikke løst – videre eskaleres i systemet og følges op efter impl. ITIL processer.



INCIDENT/SITUATION TIL IT-BEREDSKAB (1)



kritisk infrastruktur-skade

Situation eskaleret til It-beredskab fra IM, PM og/eller SM

Kritisk placering (i BIA)?

NEJ

Find løsninger inden for Situation M.

JA

Uanset Ja eller Nej

Hold krise-organisation informeret

Afhængig-heder OK?

NEJ Afhængigheder genetableres

Involver og løs afhængigheder

JA Applikation genetableres

Kan ikke løses – videregives til krise

Testet og godkendt

NEJ

JA

Afblæs It-beredskab

Foretag opfølgning

INCIDENT / SITUATION TIL IT-BEREDSKAB (2)

1. Kan være eskaleret sag(er) fra IM, PM og SM (tid og kritikalitets parameter).

2. Applikation, infrastruktur eller services skal være BIA-kritiske.

3. Flere samtidig kritiske nedbrud (sager) eskaleres automatisk (ej defineret pt.).

4. Fysisk skade på BIA-kritiske infrastruktur kan direkte føre til It-beredskabs situation.

5. Normal severity action proces kan springes over.

6. Kunde- og/eller systemansvarlig involveres i kommunikation, test, godkendelse og afblæsning.

7. Support- og kriseorganisation sættes samtidig i højberedskab.

8. Drift og support af andre ikke-kritiske produkter nedprioriteres

9. Drift, support og produkt-ansvarlig sørger for viden, proces og dokumentation opdatering

10. Organisationens It-beredskabs-ansvarlig styrer slagets gang!

IT-BEREDSKAB TIL IT-KRISEBEREDSKAB

1. Organisationens sundheds-mæssige krisesituation startet pga. It afhængigheder vil automatisk føre til It-kriseberedskab.

2. Flere samtidige It-beredskabsopgaver vil automatisk føre til It-kriseberedskab (defineres)

3. Ikke afblæste It-beredskabs-situation vil automatisk føre til It-kriseberedskab (eskaleret).

4. Alvorlige fysiske skader på driftscenter og udstyr som alene kræver længere genetableringstid end tilladte maksimum nedetid vil starte It-kriseberedskab.

5. Erklæret It-kriseberedskab vil automatisk medføre annullering af It-organisationens 'normale funktioner'.

6. Erklæret It-kriseberedskab kan medføre tilsidesættelse af alle eller dele af driftsprioriteringer.

7. It-kriseberedskabsledelse skal finde alternative lokationer, ressourcer og evt. bemandinger.

7. Kommunikation og koordination kun via It-kriseberedskabsledelse.

9. Der skal findes/udpeges organisationens It-kriseberedskabs-ansvarlig. (udenfor projektet!)

STANDARDER OG BC LIFECYCLES

IRBC REQUIREMENTS FOR ORGANIZATION

External requirements & recommendations:

- RM requirements & compliance recommendations
- DS BS ISO standards BS25777 -> DS/ISO27031
- ~~Danish Standard for Information Security (DS 484)~~
- ISO/IEC (Security Standards) - 27000 series
- BS25999 -> DS/ISO22301
- ISO/IEC (Risk Management Standards)
- COSO
- CobIT (IT Gov. Institute/ISACA)
- NIST (Guide for IT Systems)
- ENISA (European)
- Audit reports & standards (including ISAE3402 etc.)
- Good Practice Guideline 2013 (Business Continuity Institute)

Internal requirements & recommendations:

- Strategies (RM, IT & NW), Policies, Work Instructions, Guidelines
- Policies: IT & NW usage, SDLC, ULCM, NW(.)M, PLCM & A&FM
- Processes: IncM, ProM, CriM, DisM, ICT-CM & BCM - also ITIL related

ORGANISATIONENS KOBLING TIL ANDRE BEREDSKABSPLANER

HVAD FINDES DER ELLERS SOM ER AKTUELT FOR ORGANISATIONEN

Nationale / lovbestemte beredskab

Civil Beredskabslov (en række love) samt bekendtgørelser kræver f.eks. at regionsrådet vedtager en beredskabsplan og planen skal vedligeholdes mindst en gang i hver valgperiode. Planen håndterer bl.a. forretningens viderførelse, krisestyring samt risiko- og sårbarhedsstyring.

Regionale / direktiver om beredskab

Den overordnede sundhedsplan (strateginiveau) som stiller krav til en række sundhedsberedskab, herunder somatiske-, præhospital- og psykiatriberedskab.

Lokale (både politiske og praktiske) beredskab

Desuden findes der en hel række decentrale beredskaber i hospitalerne mm., som er i nogle tilfælde afhængig af infrastruktur, data- og netværkstilgængelighed og indirekte afhængig af organisationens It-beredskab!

HVOR MEGET ER EN DEL AF IT BEREDSKAB?

Nationale / lovbestemte beredskab

Civil Beredskabslov (en række love) samt bekendtgørelser kræver regionsrådet vedtager en beredskabsplan og planen skal vedligeholdes mindst en gang i hver valgperiode. Planen håndterer bl.a. forretningens viderførelse, krisestyring samt risiko- og sårbarhedsstyring.

Regionale / direktiver om beredskab

Den overordnede sundhedsplan (strateginiveau) som stiller krav til en række sundhedsberedskab, herunder somatiske-, præhospital- og psykiatriberedskab.

Lokale (både politiske og praktiske) beredskab

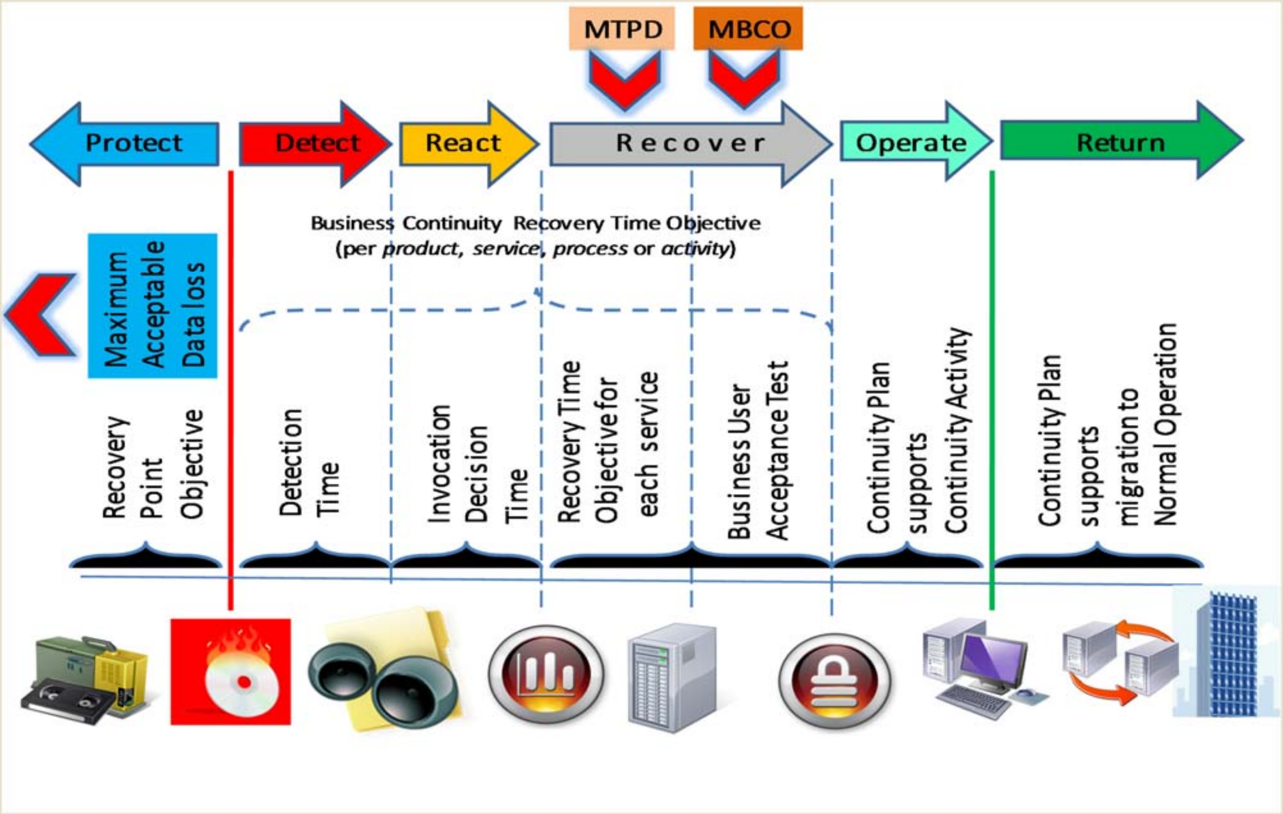
Desuden findes der en hel række decentrale beredskaber i hospitalerne mm., som er i nogle tilfælde afhængig af infrastruktur, data- og netværkstilgængelighed og indirekte afhængig af organisationens It-beredskab!

... næsten alle kræver bl.a tilgængelighed for kommunikations netværket samt andre elementer af infrastruktur.

HVOR MEGET ER EN DEL AF IT BEREDSKAB?

TEORETISKE FORUDSÆTNINGER FOR IT BEREDSKAB

'*6 PHASES*' OF A READINESS FOR IRBC PROJECT



MTPD

MBCO

Protect

Detect

React

Recover

Operate

Return

Business Continuity Recovery Time Objective
(per *product, service, process* or *activity*)

Maximum Acceptable Data loss

Recovery Point Objective

Detection Time

Invocation Decision Time

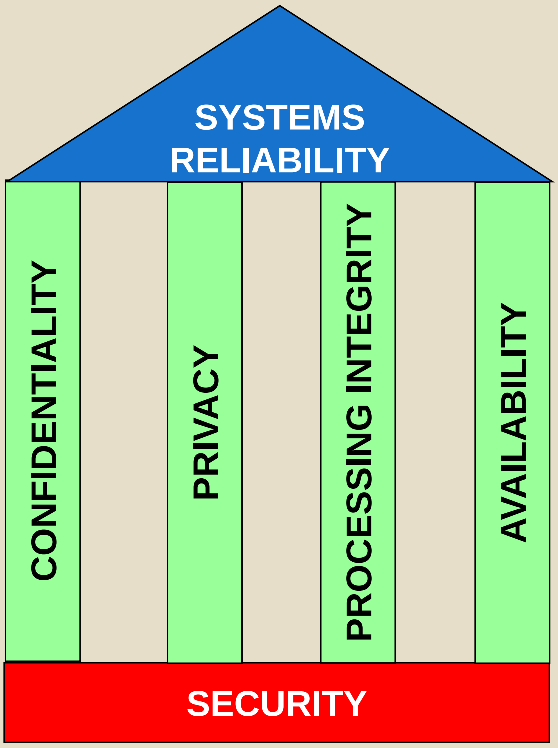
Recovery Time Objective for each service

Business User Acceptance Test

Continuity Plan supports Continuity Activity

Continuity Plan supports migration to Normal Operation

AICPA & CICA - SYSTRUST



SYSTEMS RELIABILITY

CONFIDENTIALITY

PRIVACY

PROCESSING INTEGRITY

AVAILABILITY

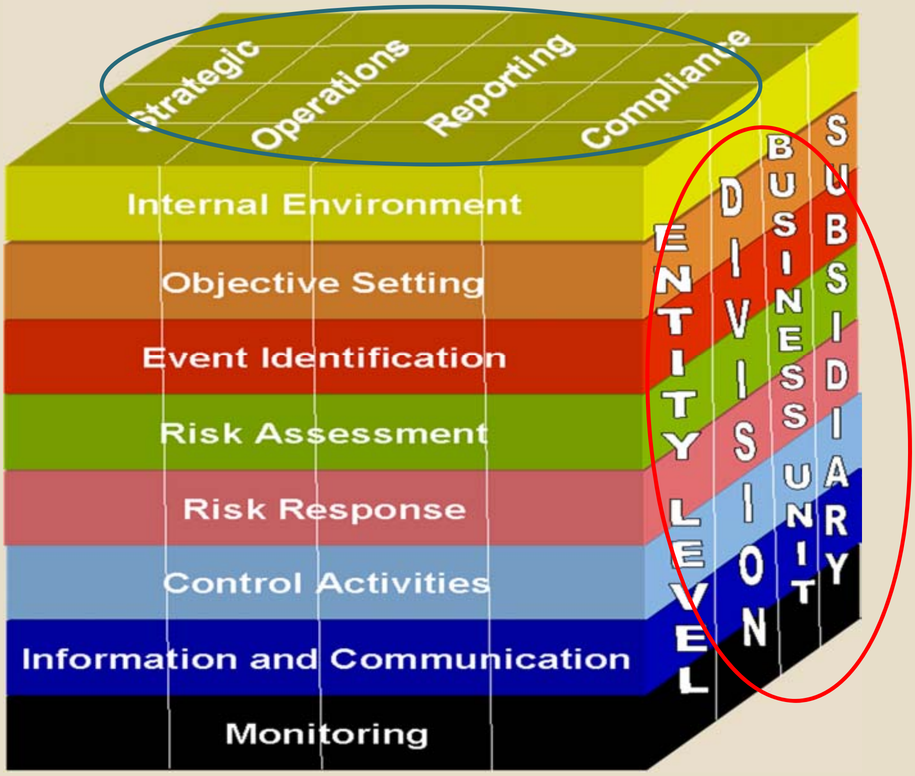
SECURITY

The Trust Services framework developed by the AICPA and the Canadian Institute of Chartered Accountants (CICA) identified five basic principles that contribute to systems reliability:

1. Security
2. Confidentiality
3. Privacy
4. Processing Integrity
5. Availability

Use of Compensating controls are requirements for mitigating risks not covered by PDC controls.

COSO INTERNAL CONTROL FRAMEWORK



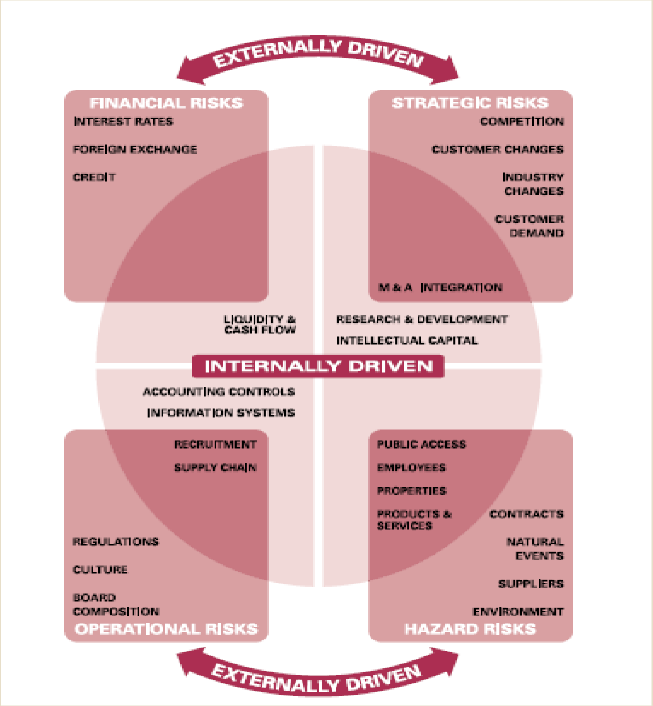
… if control framework covers it all, then why do we need any further work with ICT-RBC?

DRIVERS OF KEY RISK MANAGEMENT (ISO/IEC 73 GUIDE)

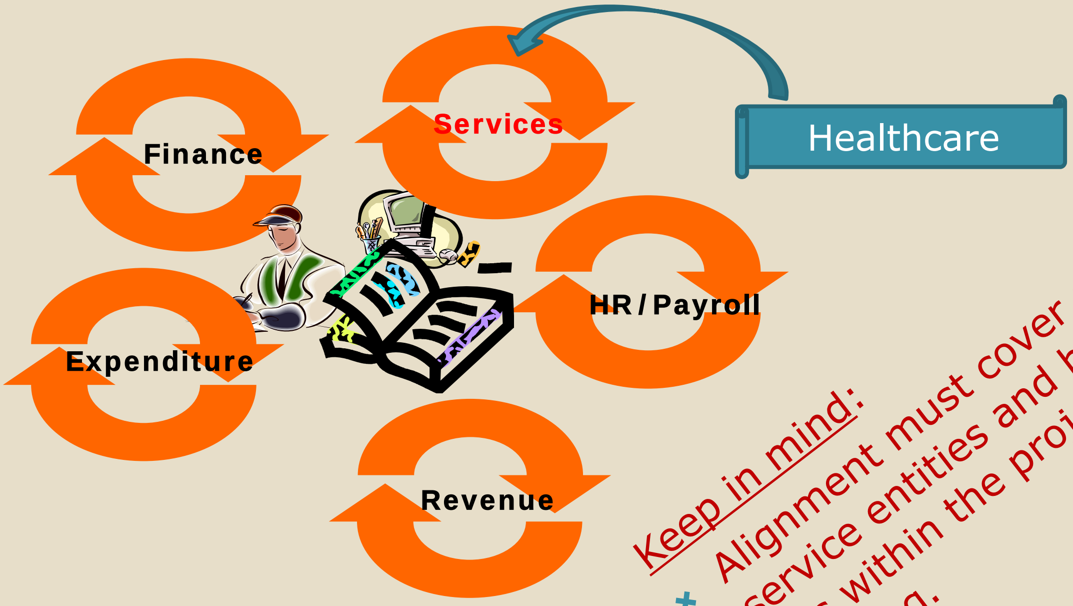
External and Internal drivers are:

- Financial Risks
- Strategic Risks
- Operational Risks
- Hazards

- closely tied up with both financial, strategic and reputational risks



ALIGNING WITH ORGANIZATION



Finance

Services

Healthcare

HR / Payroll

Expenditure

Revenue

Keep in mind:

- Alignment must cover all business & service entities and business cycles, if it is within the project and process scoping.

BUSINESS IMPACT ASSESSMENT (BIA)

SCOPING BIA

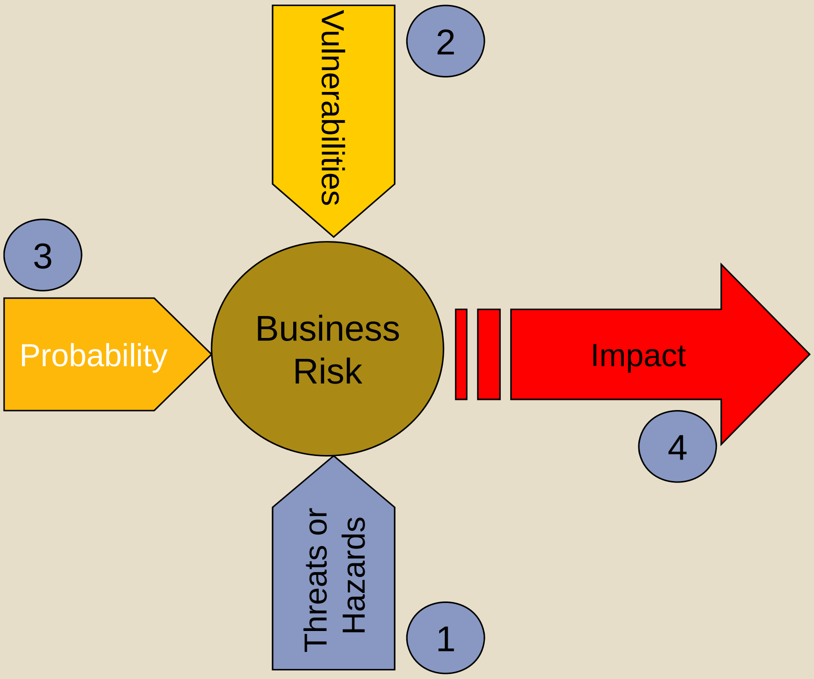
Thru Business Impact Analysis or BIA, organization's requirements in response to incidents, disasters or crisis would be accurately assessed and prioritized.

BIA would deal with e.g. compliance, business requirements, external as well as internal threats, infrastructure availability, HR-issues and their consequences.

Scope of BIA would be determined by the top Management in collaboration with Risk Management function.

- ▶ Organization / Enterprise wide contra Business entities
- ▶ Geographical sites
- ▶ Business cycles or functions
- ▶ Based on specific risk or compliance requirements

SCRUTINIZING BIA CONTENTS



SCRUTINIZING BIA CONTENTS

1 A (threat is) potential cause of an unwanted incident, which may result in harm to individuals, assets, a system or organization, the environment, or the community. Some threats, such as bad weather are more commonly referred to as "Hazards".
BCI GPG:2013

2 The vulnerabilities in the business and operating model of an organization can be considered as seven areas: Reputation, Supply Chain, Information and Communication, Sites and Facilities, People, Finance and Customers.
BCI GPG:2013

3 Likelihood is the state of being probable or chance of something happening. Chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies or mathematical probabilities.
British Standard BS25999-1:2006 Code of Practice for Business Continuity Management

4 The evaluated consequence of a particular outcome.
BCI GPG:2013

(Impact is the value, in the form of financial denomination, of the loss that is or would be incurred if and when vulnerability is successfully exploited.)
British Standard BS25777:2008 Information and Communications Technology Continuity Management: Code of Practice

BIA COMPONENTS

☑ Infrastructures for the business *(technology, premises)*

☑ Buildings, physical sites etc. *(premises)*

☑ Employees, key personnel etc. *(People)*

☑ Hardware, physical components *(Technology)*

☑ Systems and services *(Processes)*

☑ Business cycles, Markets, Clients *(Processes)*

☑ Service providers, vendors etc. *(People, Suppliers)*

☑ Techies *(People, Technology & Suppliers)*

☑ Public Services *(Compliance, technology, premises)*

☑ Laws, regulations etc. *(Compliance)*

BIA CONSIDERATIONS

- ☑ Referential identity (enterprise wide unique!)
- ☑ Identifier descriptions
- ☑ Reliable Systems requirements (SCIAP)
- ☑ Reliability on SoD and QA
- ☑ Compliance requirements (internal & external)
- ☑ Business dependencies for the (specific) Component
- ☑ Component dependencies on other pertinent components
- ☑ Numbers of Users / clients dependency
- ☑ Dependency level on key personnel
- ☑ Dependency level on suppliers & service providers
- ☑ Likelihood / Probability of threat being realized

METHODS OF ASSESSMENT

BIA is a management level analysis by which the organization assesses the quantitative (financial) and qualitative (non-financial) impacts, effects and loss that might result if the organization were to suffer a Business Continuity emergency, incident or crisis.

The findings from a BIA are used to make decisions concerning Business Continuity Management strategy and solutions.

Quantitative assessments are usually undisputable, as far as methods and results are concerned.

Qualitative assessments are usually done for intangible (non-financial) issues, and relate to Reputation, brand and presence, Legal and contractual liabilities, Quality of product and service, Stakeholder confidence and support, Staff morale and well being and Environmental damages.

RPO & RTO FOR ICT

- Recovery Point Objective (RPO): point in time to which information or data must be recovered in order to resume ICT services.

- Recovery Time Objective (RTO): target time set for resumption of product, service, or activity delivery after an incident.

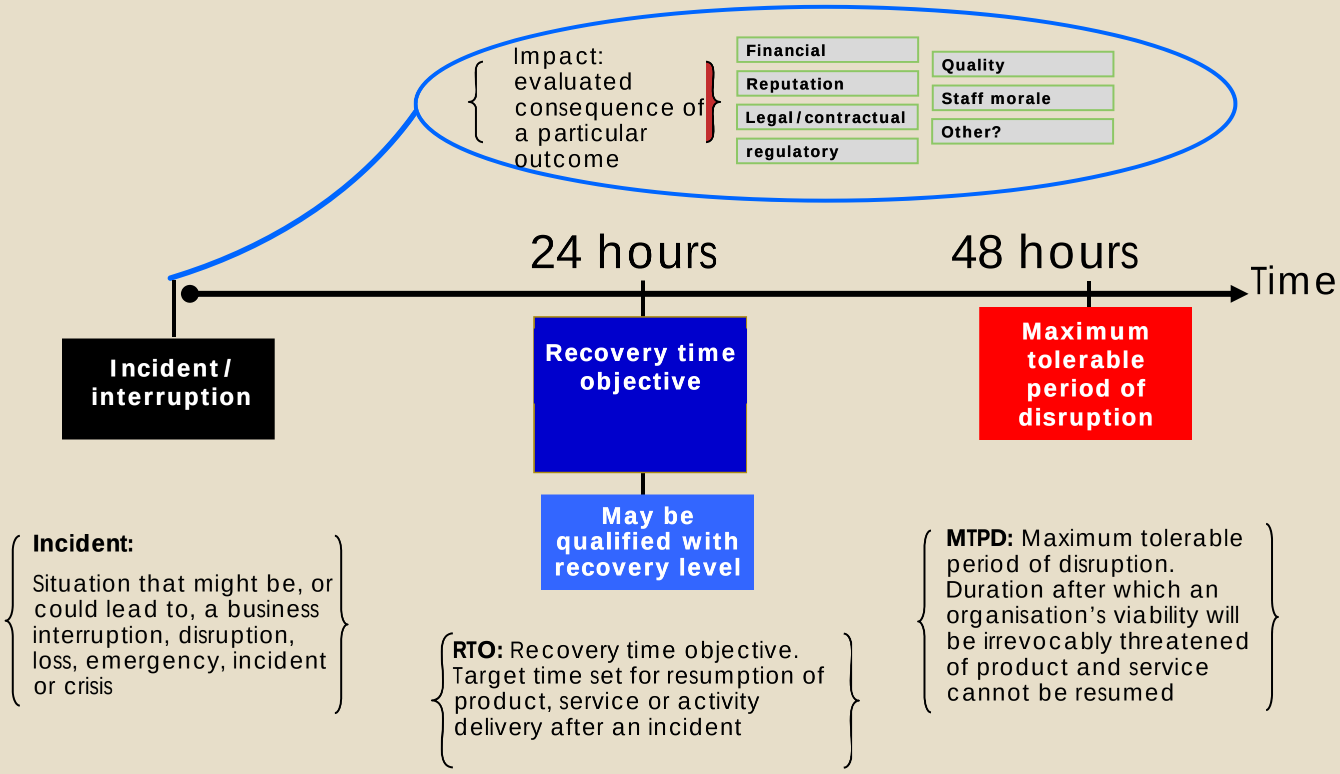
METHODS OF ASSESSMENT

- Maximum Tolerable Data Loss (MTDL): The maximum loss of information (electronic and other data) which an organization can tolerate. The age of the data could make operational recovery impossible or the value of the lost data is so substantial as to put business viability at risk..

- Maximum Tolerable Period of Disruption (MTPD): The duration after which an organization's viability will be irreparably damaged if a product or service delivery cannot be resumed.

Plan must contain: Recovery Time < MTPD

METHODS OF ASSESSMENT



Incident:
Situation that might be, or could lead to, a business interruption, disruption, loss, emergency, incident or crisis

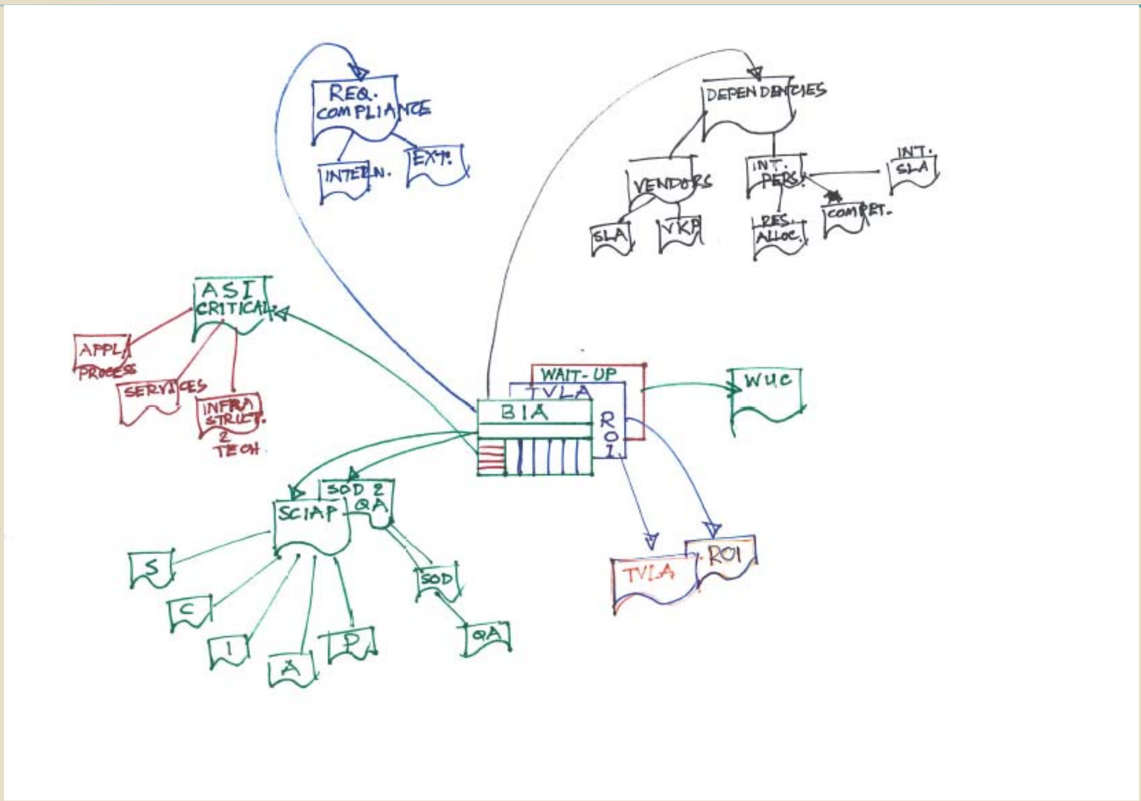
RTO: Recovery time objective. Target time set for resumption of product, service or activity delivery after an incident

MTPD: Maximum tolerable period of disruption. Duration after which an organisation's viability will be irrevocably threatened of product and service cannot be resumed

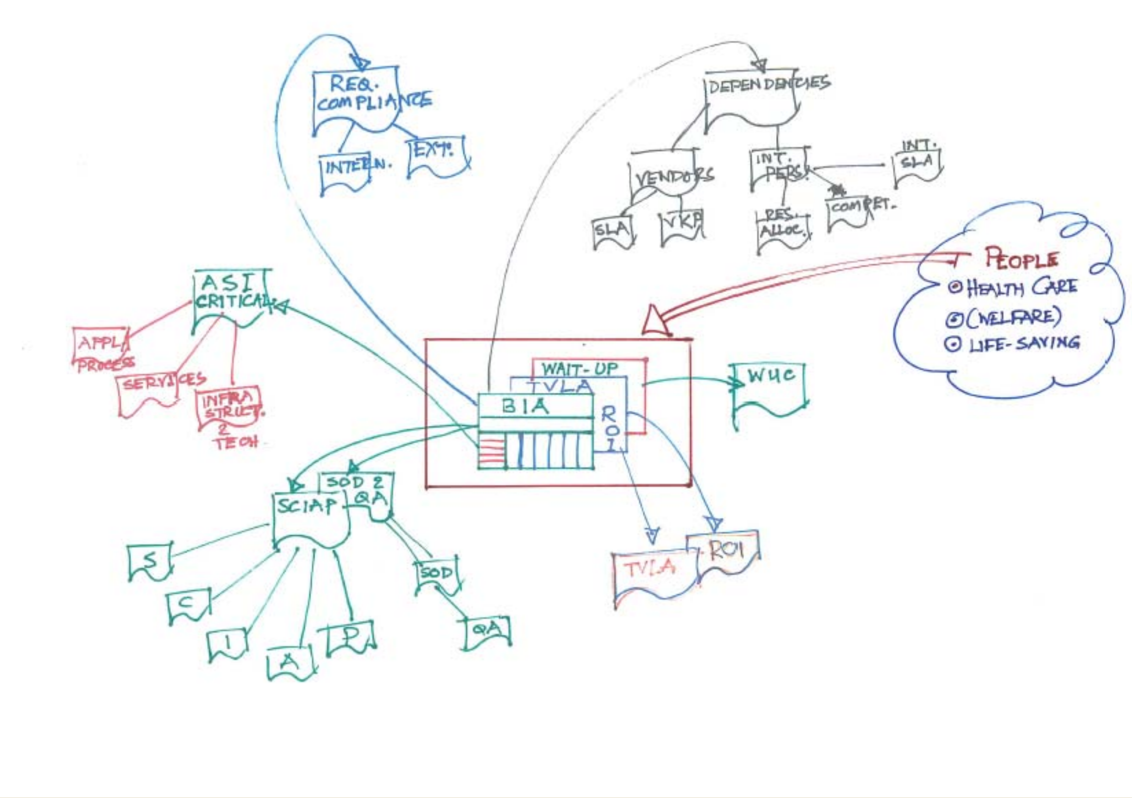
BIA SKEMA

Komponent beskrivelse		*Relevante vurderingeskriterier for komponent i 'PROTECT' process* (Høj = 5, lav = 1)						*Relevante vurderingeskriterier for komponent i 'DETECT, REACT & RECOVER' process* (Høj = 5, lav = 1)					*Relevante vurderingeskriterier for komponent i 'OPERATE & RETURN' process (Høj = 5, lav = 1)*				
Komponentreference (for grupperne A, I eller T)	Komponentnavn og detaljer (Bemærk venligst, at en komponent kan være både en fysisk- eller software 'dims', infrastruktur komponent, system eller delsystem, applikation eller en hvilken som helst anden enhed - som skal nødvendigvis indgår i BIA konsekvens-vurderingen) (se eksemplarer nedenfor)	*Relevant vedr. informationssikkerhed og forbyggende foranstaltninger*						Overholdelse af Compliance Krav (ej tidsrel.)		Komponents afhængigheder (24 timers MTPD)			Komponents afhængigheder og omkostninger for mangl. drift (24 timers MTPD)				
		Virksomhedsfortroligt	Applikations integritet	System & Data tilgængelighed	Personfølsomme oplysninger	Kvalitetssikring	Funktionsadskillelse	Regionens Interne Krav	Regionens Eksterne Krav	Centrale infrastruktur afhængigheder	Interne Nøgleperson afhængigheder	Eksterne leverandør/nøgleperson afhængigheder	Livstruende hændelser (altid = 5)	Behandling af patienter (andre konsekvenser)	Genetablerings omkostninger (ej drift)	Medarbejder ventetid omsat *(wait-up i timer)*	**Check-Out kvantitative dele**
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	√
A-1																	

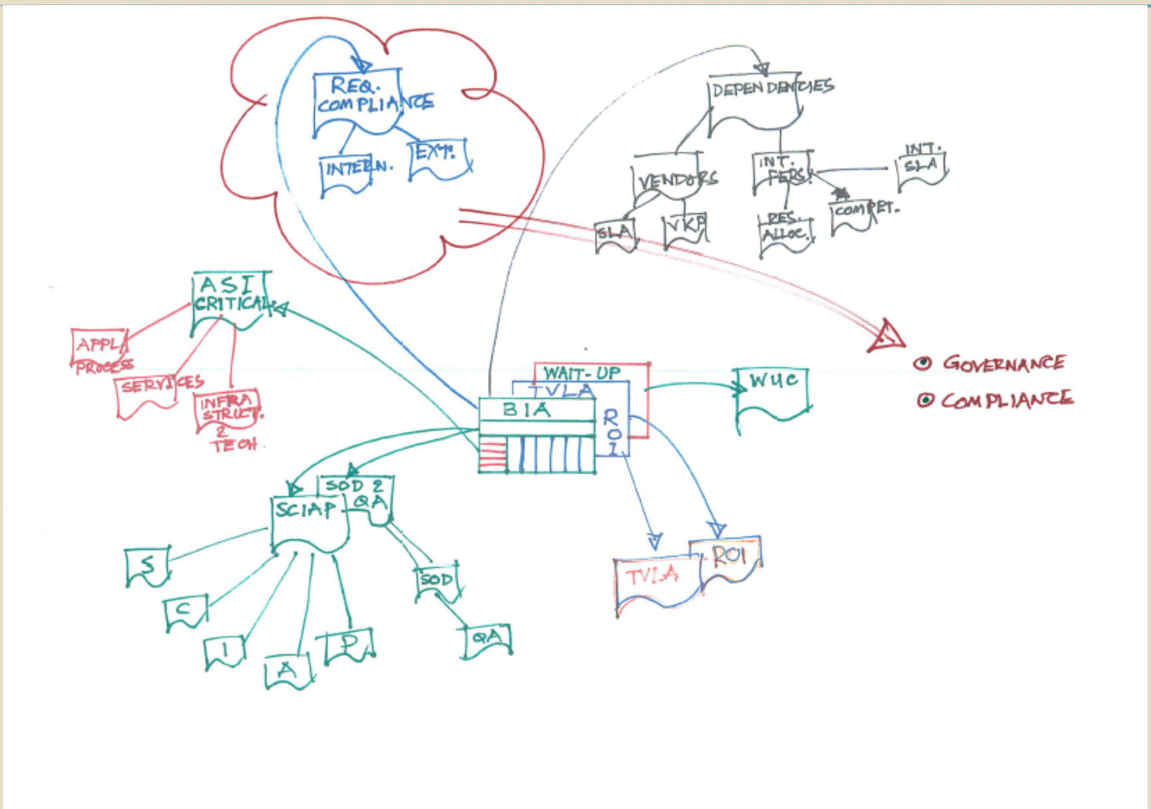
BIA OUTPUT



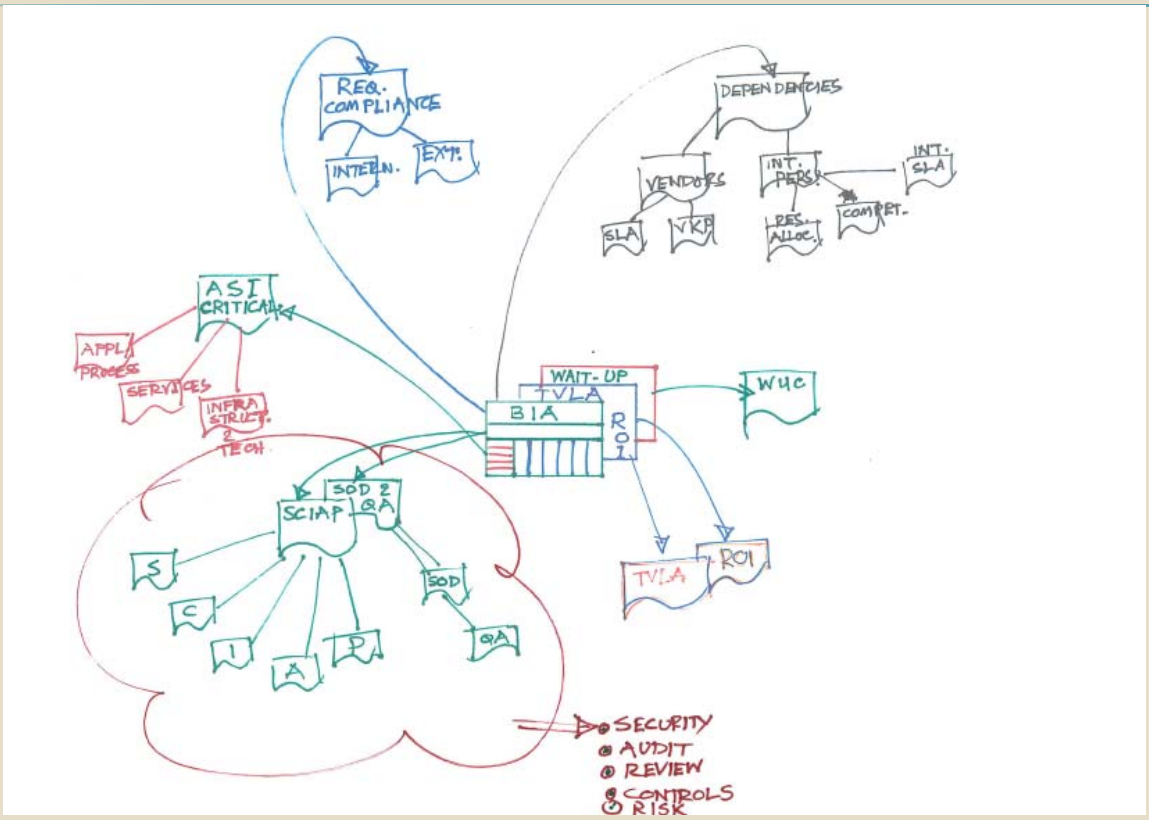
BIA OUTPUT



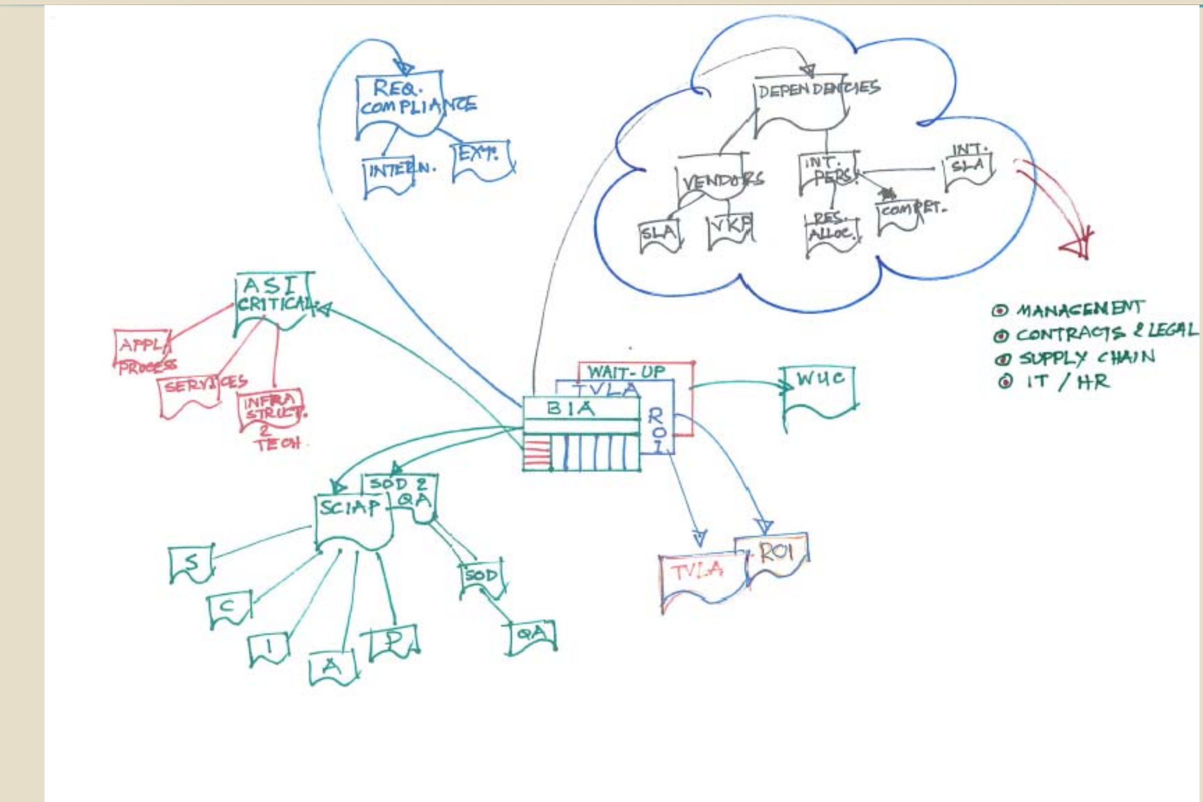
BIA OUTPUT



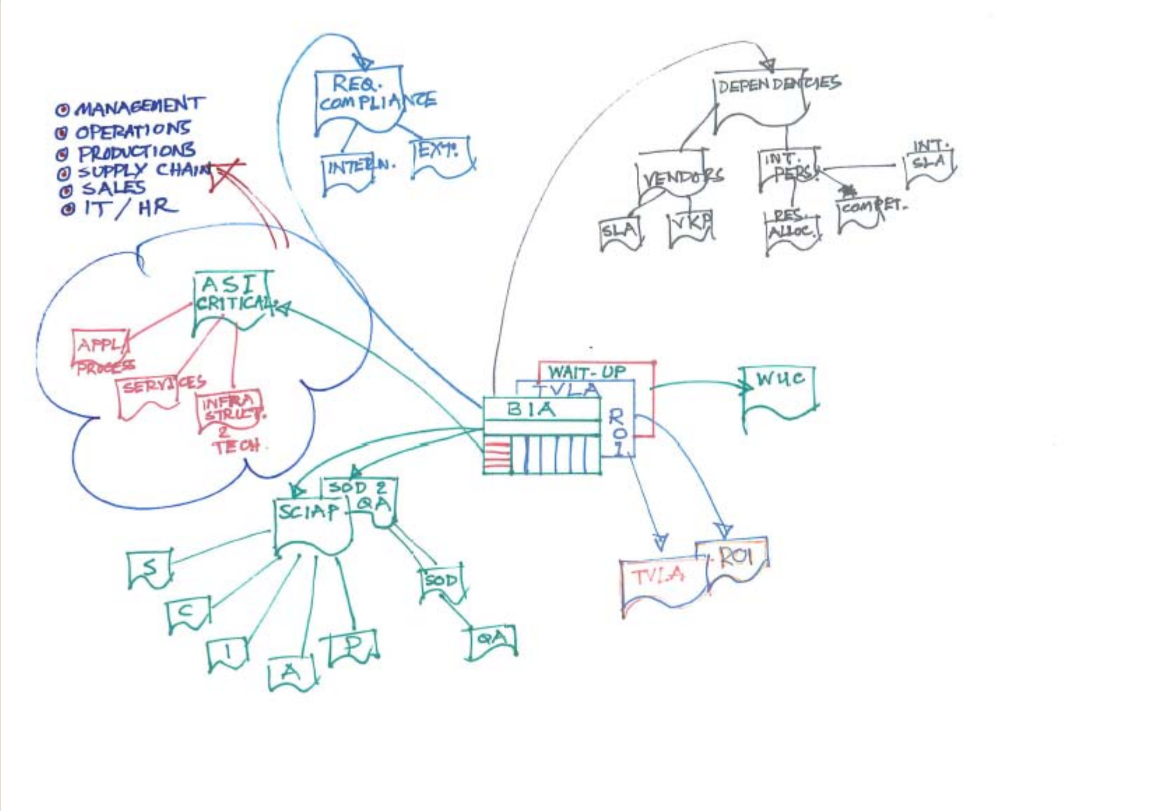
BIA OUTPUT



BIA OUTPUT



BIA OUTPUT



CONTACT INFO & CREDENTIALS

For further information, please contact:

Faruque Sayed
Team Consultants, Denmark
Telephone: +45 8681 6370
Mobile: +45 6172 5500
+45 2048 6370
Email: faruque@teamconsultants.dk

Credentials:
- M. A. (Econ) – University of Dacca
- B. A. (Information Technology), Aarhus
- Post Graduate (Info. Security Management), Royal Holloway, University of London
- Post Graduate (Business Continuity Management), University of Coventry
- MBCI, Business Continuity Institute, UK
- Lead Auditor, BS25999 (UKAS)
- CISM, CISA, CRISC & CGEIT, ISACA - IT Governance Institute