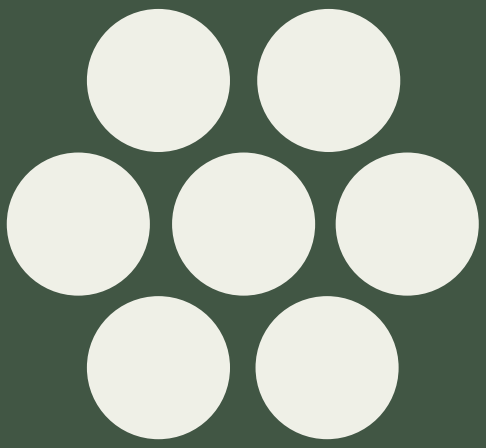
Anläggningar med förhöjd säkerhet och funktion

Bilaga 3. Metod för anläggningsanalys

Version 1.3



Anläggningar med förhöjd säkerhet

Innehåll

1 Metodöversikt

Nätägaren ska inom ramen för *Post och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster* ha genomfört risk- och sårbarhetsanalyser på anläggningstillgångar och förbindelser. Samtliga siter ska uppfylla PTS föreskrifter och inte ha några reståtgärder noterade.

För en nätägare är det viktigt att klargöra nedanstående frågor:

- Vilken/vilka säkerhets- och skyddsnivå(er) kan min anläggning erbjuda?
- Vilken/vilka säkerhets- och skyddsnivå(er) ska min anläggning kunna erbjuda?
- Vilka säkerhets- och skyddsåtgärder behöver jag komplettera anläggningen med?

För att ta fram lämpliga skydds- respektive säkerhetsnivåer används en process för anläggningsanalys enligt nedan.

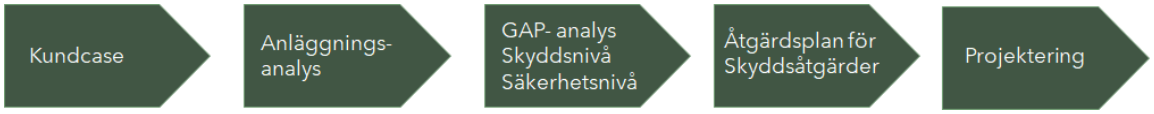


Bild. Metodik för analys av kundcase kopplad till anläggningsförmåga

Processen utgår från att det är kundbehov och kundkrav som ligger till grund för analysarbetet och där resultatet av analysen avgör de kompletteringar som krävs för att svara upp mot ställda krav. För att beskriva metoden används här ett fiktivt kundcase.

2 Kundcase – en aktörs behov av konnektivitet

En kund hyr idag förbindelser mellan två egna datacenters i Linköping respektive Norrköping (kundsite DL och DN). Dessa är backup för varandra och även ibland kompletterande och ska ses som en helhet.

Anläggning DL är genom ett gemensamt intag ansluten till två nätsiter. Anläggning DN är ansluten till två nätsiter genom separata intag. Framföringsvägen i nätet mellan DL och DN-anläggningarna är redundant men saknar diversitet

Kunden har behov av redundant högkapacitetsförbindelse för att klara 800Gbps mellan datacenters. De har också ett behov av förstärkt säkerhet och vill hyra en passiv förbindelse med hög säkerhet, hög skyddsnivå samt redundans genom diversitet i nätet mellan sina anläggningar då kritiska funktioner och kunder finns i datacentret.

Kunden står själv för den aktiva utrusningen och dess logiska konfiguration.

Säkerhets - och skyddsnivå

För en kund som bedriver verksamhet med krav på hög säkerhet krävs **skyddsnivå SA3** på kundens anslutning till nätet enligt *Bilaga 2 Fysiska förbindelser för anslutning av en kundsite med användare som bedriver verksamhet med krav på hög säkerhet*.

Kravet på framföringsvägen är att den ska vara redundant med diversitet genom nätet och att kundsiten ansluts till två separata siter som uppfyller säkerhetsnivå **S2 eller S3**. Intaget i respektive kundsite ska ske via separata intag med eller utan separata brunnar.

3 Nulägesanalys

3.1 Nätstruktur

Identifiera och dokumentera nätstrukturen för anläggningen som ska analyseras.

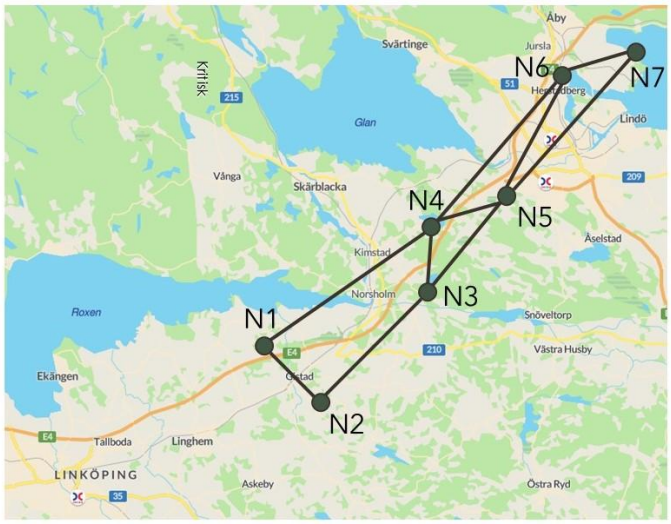


Bild. Befintlig nätstruktur

3.2 Förslag på framföringsvägar

Befintliga kundförbindelser ansluter till olika siter men framföringsvägen är den samma mellan orterna. I DL ansluter båda förbindelserna genom en gemensam anslutningspunkt. All kanalisation är etablerad enligt Robust fiber (RF).

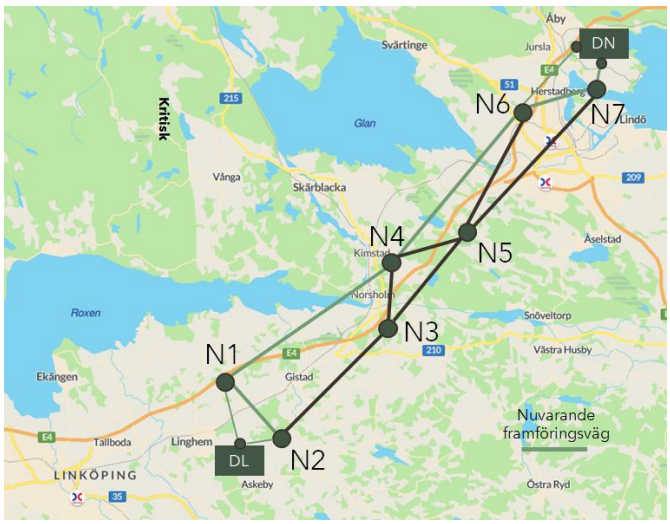


Bild. Befintliga kundanslutningar

Ta fram förslag till framföringsvägar för ordinarie förbindelse (OF) och redundant förbindelse (RF) mellan kundanläggningarna DL och DN.

För en kund som bedriver verksamhet med krav på hög säkerhet krävs skyddsnivå SA3 på vilket innebär att den ska vara redundant med diversitet genom nätet och att kundsiten ska anslutas till två separata siter som uppfyller säkerhetsnivå S2 eller S3. Intaget i respektive kundsite ska ske via separata intag med eller utan separata brunnar.

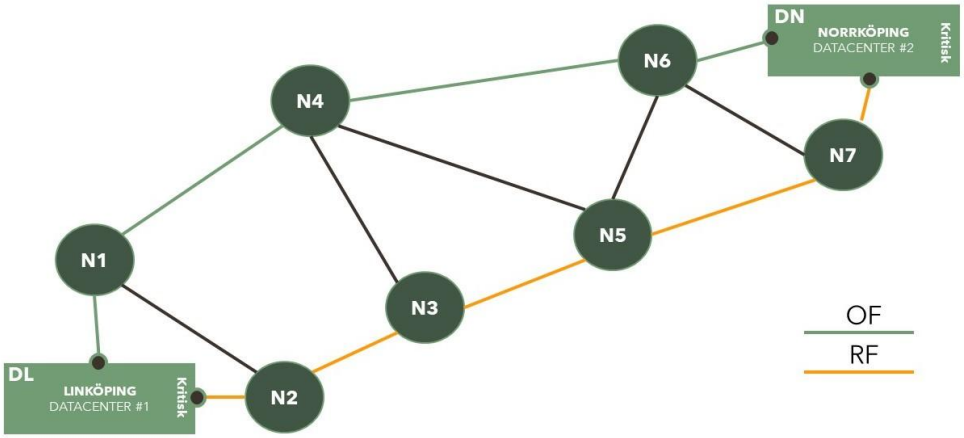


Bild. Förslag på framföringsvägar med kundanslutning

3.3 Nulägesanalys siter

Genomför en nulägesanalys enligt matrisen för skyddsåtgärder i Bilaga 1 Robust site för samhällsviktig digital infrastruktur avseende vilka säkerhetsnivåer som gäller för siterna i respektive framföringsväg. Sätt ett ID-nummer på förbindelserna mellan siterna.

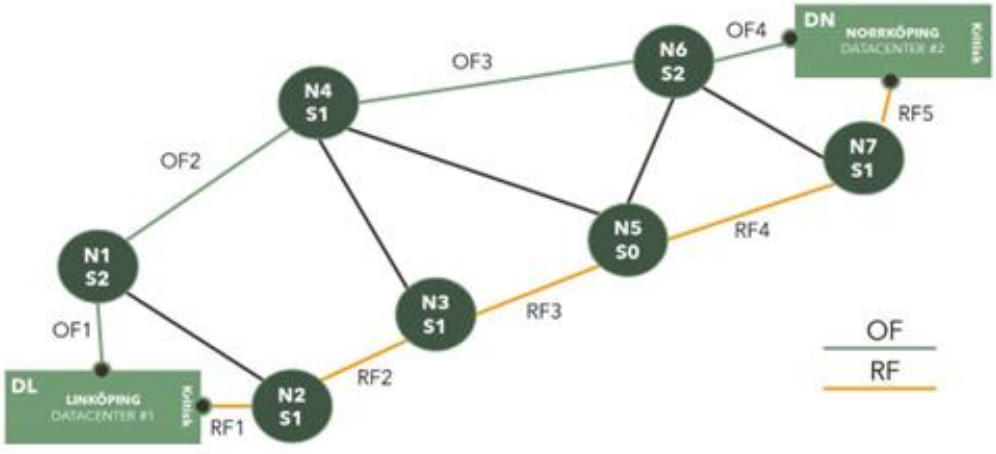


Bild. Förslag på framföringsvägar med kundanslutning

S1. Säkerhetsnivå för Siter med Stor lokal betydelse och krav på förhöjd säkerhet

S2. Säkerhetsnivå för Siter med stor betydelse och krav på hög säkerhet

S3. Säkerhetsnivå för Siter med avgörande betydelse och hög säkerhet

Skyddsåtgärder för Site	S1	S2	S3
5.1 Siteområde			
5.1.1 Områdesskydd			
- Mekaniskt områdesskydd	RSA	RSA	Ja
- Elektroniskt områdesskydd	Nej	RSA	Ja
-- Inbrottslarm	Nej	RSA	Ja
--- Larmsystem	Nej	Typ 1	Typ 2
-- Kameraövervakning	Nej	RSA	Ja
-- Tillträdeskontroll	Nej	RSA	Ja
5.2 Sitebyggnad			
5.2.1 Skalskydd			

Bildl. Utdrag från matrisen för skyddsåtgärder i Bilaga 1 Robust site för samhällsviktig digital infrastruktur

Resultatet från nulägesanalysen ger följande utfall:

Nuvarande säkerhetsnivå för siterna			
Site	**Uppfyller säkerhets-nivå**	**Site**	**Uppfyller säkerhets-nivå**
N1	S2	N5	S0
N2	S1	N6	S2
N3	S1	N7	S1
N4	S1		

3.4 Nulägesanalys av föreslagna förbindelse

3.4.1 Siter ordinarie förbindelse (OF)

Planerade förbindelser med siternas klassificering		
Förbindelse	**A-Site**	**B-Site**
OF1	DL*	N1 (S2)
OF2	N1 (S2)	N4 (S1)
OF3	N4 (S1)	N6 (S2)
OF4	N6 (S2)	DN**

*Utförande i enlighet med anvisningarna för robust fiber men saknar separata intag.
**Utförande i enlighet med anvisningarna för robust fiber och har separata intag.

3.4.2 Siter redundant förbindelse (RF)

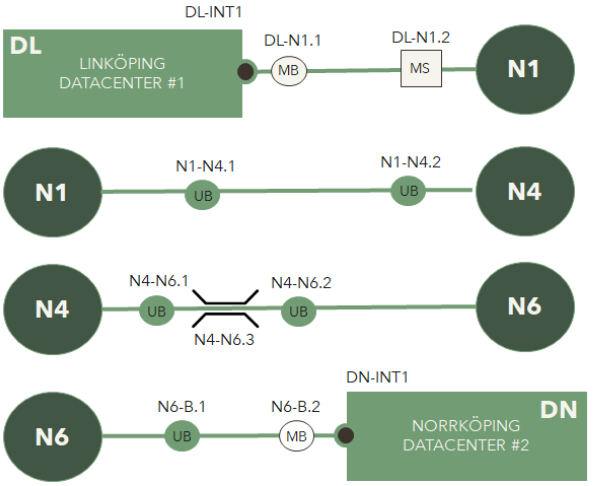
Planerade förbindelser, med siternas säkerhetsnivå		
Förbindelse	**A-Site**	**B-Site**
RF1	DL*	N2 (S1)
RF2	N2 (S1)	N3 (S1)
RF3	N3 (S1)	N5 (S0)
RF4	N5 (S0)	N7 (S1)
RF5	N7 (S1)	DN**

*Utförande i enlighet med anvisningarna för robust fiber men saknar separat intag.
**Utförande i enlighet med anvisningarna för robust fiber och har separata intag.

3.5 Nulägesanalys förbindelsernas framföringsväg

Genomför en nulägesanalys avseende det fysiska utförandet av delförbindelserna för respektive framföringsväg mellan siter och mellan siter och kundanläggningar.

Framföringsväg Ordinarie förbindelse (OF)



OF1
DL-INT1 Gemensamt intag
DL-N1.1 Markbrunn
DL-N1.2 Markskåp

OF2
N1-N4.1 Underjordsbrunn
N1-N4.2 Underjordsbrunn

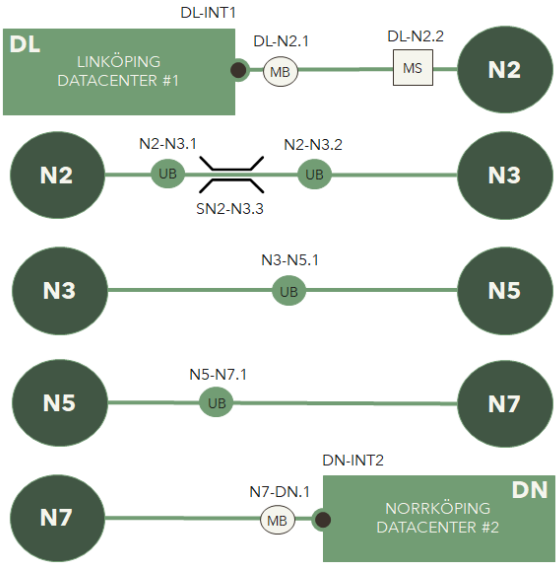
OF3
N4-N6.1 Underjordsbrunn
N4-N6.2 Underjordsbrunn
N4-N6.3 Bro med kanalisation

OF4
N6-DN.1
Underjordsbrunn
N6-DN.2 Markbrunn
DN-INT1 Separat intag

(1) Anläggningsanalys: nätinfrastruktur mellan A-B

Bild. Exempel på fysiska egenskaper på delsträckorna för ordinarie förbindelse

Framföringsväg Redundant förbindelse (RF)



RF1
DL-N2.1 Markbrunn
DL-N2.2 Markskåp
DL-INT1 Gemensamt intag

RF2
N2-N3.1 Underjordsbrunn
N2-N3.2 Underjordsbrunn
N2-N3.3 Bro med kanalisation

RF3
N3-N5.1 Underjordsbrunn

RF4
N5-N7.1 Underjordsbrunn

RF5
N7-DN.1 Markbrunn
DN-INT2 Separat intag

(1) Anläggningsanalys: nätinfrastruktur mellan A-B

Bild. Exempel på fysiska egenskaper på delsträckorna för redundant förbindelse

3.6 Sammanställning nulägesanalys

Dokumentera nuläget för delförbindelserna för respektive framföringsväg. Vid typidentifiering används bilaga 2.

3.6.1 Ordinarie förbindelse (OF)

Planerade förbindelser				
Förbindelse	**A-Site**	**B-Site**	**Spridningspunkter**	**Typ**
OF1	DL	N1 (S2)	DL-INT1 Gemensamt intag	RF
			DL-N1.1 Markbrunn	Typ 1
			DL-N1.2 Markskåp	Typ 1
OF2	N1 (S2)	N4 (S1)	N4-N4.1 Underjordsbrunn	Typ 1
			N4-N4.2 Underjordsbrunn	Typ 0 *
OF3	N4 (S1)	N6 (S2)	N4-N6.1 Underjordsbrunn	Typ 1
			N4-N6.2 Underjordsbrunn	Typ 0 *
			N4-N6.3 Bro, kanalisation under	RF
OF4	N6 (S2)	DN	N6-DN.1 Underjordsbrunn	Typ 0 *
			N6-DN.2 Markbrunn	Typ 1
			DN-INT1 Separat intag	RF

* Sökboll i brunnen

3.6.2 Redundant förbindelse (RF)

Planerade förbindelser				
Förbindelse	**A-Site**	**B-Site**	**Spridningspunkter**	**Typ**
RF1	DL	N2 (S1)	DL-INT1 Gemensamt intag	RF
			DL-N2.1 Markbrunn	Typ 1
			DL-N2.2 Markskåp	Typ 1
RF2	N2 (S1)	N3 (S1)	N2-N3.1 Underjordsbrunn	Typ 1
			N2-N3.2 Underjordsbrunn	Typ 0 *
			N2-N3.2 Bro med kanalisation	RF
RF3	N3 (S1)	N5 (S0)	N3-N5.1 Underjordsbrunn	Typ 0 *
RF4	N5 (S0)	N7 (S1)	N5-N7.1 Underjordsbrunn	Typ 0 *
RF5	N7 (S1)	DN	N7-N7.1 Markbrunn	Typ 1
			DN-INT2 Separat intag	RF

* Sökboll i brunnen

4 GAP-analys

4.1 Allmänt

Genomför en GAP-analys* genom att identifiera och dokumentera, i en GAP-rapport, skillnaderna mellan identifierade skydds-och säkerhetsnivåer och kraven angivna i Bilaga 1 Robust Site för samhällsviktig digital infrastruktur och Bilaga 2 Passiv säker fysisk förbindelse.

*GAP-analys är ett sätt att beskriva skillnaden mellan nuläge och ställda krav.

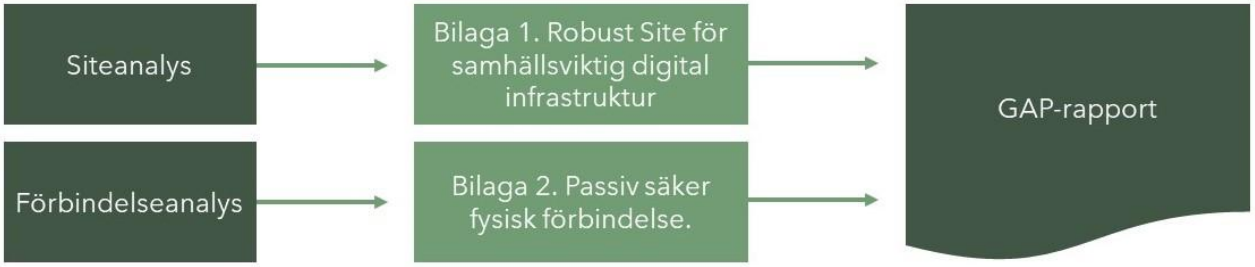


Bild. GAP-analys

4.2 Kravanalys

Jämför det fysiska utförandet av siter och delförbindelserna med kraven i säkerhetsmatriserna i Bilaga 1 Robust Site för samhällsviktig digital infrastruktur respektive Bilaga 2 Passiv säker fysisk förbindelse för respektive framföringsväg. Nuläge och identifierade krav dokumenteras i en GAP-rapport.

S1. Säkerhetsnivå för Siter med Stor lokal betydelse och krav på förhöjd säkerhet

S2. Säkerhetsnivå för Siter med stor betydelse och krav på hög säkerhet

S3. Säkerhetsnivå för Siter med avgörande betydelse och hög säkerhet

Skyddsåtgärder för Site	S1	S2	S3
5.1 Siteområde			
5.1.1 Områdesskydd			
- Mekaniskt områdesskydd	RSA	RSA	Ja
- Elektroniskt områdesskydd	Nej	RSA	Ja
-- Inbrottslarm	Nej	RSA	Ja
--- Larmsystem	Nej	Typ 1	Typ 2
-- Kameraövervakning	Nej	RSA	Ja
-- Tillträdeskontroll	Nej	RSA	Ja
5.2 Sitebyggnad			
5.2.1 Skalskydd			

Bild. Utdrag från säkerhetsmatriserna i Bilaga 1 Robust Site för samhällsviktig digital infrastruktur.

Fysiska skyddsåtgärder för elektronisk kommunikation	SF1 Utökad bas-säkerhet	SF2 Förhöjd Säkerhet	SF3 Hög säkerhet	SF1 Utökad bas-säkerhet	SF2 Förhöjd Säkerhet	SA3 Hög säkerhet
6.3 Skyddsåtgärder framföringsväg						
6.3.1 Redundans och diversitet						
Fysiska förbindelser med hög säkerhet och redundans med diversitet.			**X**			
Fysiska kundförbindelser med hög säkerhet och redundans med diversitet till skilda nätsiter.						***X***

Fysiska skyddsåtgärder för elektronisk kommunikation	SF1 Utökad bas-säkerhet	SF2 Förhöjd Säkerhet	SF3 Hög säkerhet	SF1 Utökad bas-säkerhet	SF2 Förhöjd Säkerhet	SA3 Hög säkerhet
6.4.4.1 Skyddsåtgärd underjordsbrunn (typ 1) Markförhållandena runt och över brunnen ska vara återställda så att brunnens placering visuellt inte kan identifieras.		**X**	**X**		**X**	**X**
Brunnen ska inte vara utrustad med sökbollar.		**X**	**X**		**X**	**X**

Fysiska skyddsåtgärder för elektronisk kommunikation	SF1 Utökad bas-säkerhet	SF2 Förhöjd Säkerhet	SF3 Hög säkerhet	SF1 Utökad bas-säkerhet	SF2 Förhöjd Säkerhet	SA3 Hög säkerhet
6.4.4.4 Skyddsåtgärder markbrunn (typ 2) Kraven för Markbrunn Typ 1 utgör baskrav för Markbrunn Typ 2.						
Brunnen ska vara säkerhetsklassad i enlighet med EN 1627 RC3.			**X**			**X**
Brunnen bör kompletteras med sensorer för övervakning av öppen/stängd lucka.			**X**			**X**

Bild. Utdrag från skyddsmatriserna i Bilaga 2 Robust säker fysisk förbindelse.

4.3 GAP-rapporter

GAP-rapport site

GAP-rapport - Siter			
Site	**Nuläge**	**Krav**	**Kommentar**
DL	RF	SA3	Saknar separat intag i anläggningen
N1	S2	S2	
N2	S1	S2	Reservkraftsystem - drifttid
N3	S1	S2	Skydd mot Elektromagnetisk störning
N4	S1	S2	Kameraövervakning (områdesskydd)
N5	S0	S2	Saknar mekaniskt områdesskydd med passagekontroll, släcksystem, redundant kylsystem, kameraövervakning (områdesskydd), skydd mot Elektromagnetisk störning, redundant elkraftsmatning och reservkraftsystem - drifttid
N6	S2	S2	
N7	S1	S2	Redundant kylsystem
DN	RF	SA3	

GAP-rapport förbindelse

GAP-rapport - Förbindelser			
Komponent	**Nuläge**	**Krav**	**Kommentar**
OF1		SA3	
DL-N1.1 Markbrunn	Typ 1	Typ 2	Markbrunn. Ej godkänd. Bytes till godkänd.
DL-N1.2 Markskåp	Typ 1		Markskåp. Ej tillåtet. Bytes till brunn typ 2
OF2		SF3	
N1-N4.1 Underjordsbrunn	Typ 1	Typ 1	Underjordsbrunn
N1-N4.2 Underjordsbrunn	Typ 0*	Typ 1	Underjordsbrunn. Sökbollen ska tas bort ur brunnen.
OF3		SF3	
N4-N6.1 Underjordsbrunn	Typ 1	Typ 1	Underjordsbrunn
N4-N6.2 Underjordsbrunn	Typ 0*	Typ 1	Underjordsbrunn Sökbollen ska tas bort ur brunnen.
N4-N6.3 Bro	RF		Ej godkänd. Ersättas med styrd borrning.
OF4		SA3	
N6-DN.1 Underjordsbrunn	Typ 0*	Typ 1	Underjordsbrunn. Sökbollen ska tas bort ur brunnen.
N6-DN.2 Markbrunn	Typ 1	Typ 2	Markbrunn. Ej godkänd. Bytes till godkänd.
RF1		SA3	
DL-N2.1 Markbrunn	Typ 1	Typ 2	Ej godkänd. Bytes till godkänd.
DL-N2.2 Markskåp	Typ 1		Markskåp. Ej tillåtet. Bytes till brunn typ 2
RF2		SF3	
N2-N3.1 Underjordsbrunn	Typ 1	Typ 1	-
N2-N3.2 Underjordsbrunn	Typ 0*	Typ 1	Sökbollen ska tas bort ur brunnen.
N2-N3.3 Bro			Ej godkänd. Ersättas med styrd borrning.
RF3		SF3	
N3-N5.1 Underjordsbrunn	Typ 0*	Typ 1	Sökbollen skall tas bort ur brunnen.
RF4		SF3	
N5-N7.1 Underjordsbrunn	Typ 0*	Typ 1	Sökbollen skall tas bort ur brunnen.
RF5		SA3	
N7-DN.1 Markbrunn	Typ 1	Typ 2	Ej godkänd. Bytes till godkänd.

* Sökboll i brunnen

5 Skyddsåtgärder

5.1 Allmänt

Fastställ vilken/vilka säkerhets- och skyddsnivåer anläggningen ska erbjuda, fastställ vilka säkerhets- och skyddsåtgärder anläggningen behöver kompletteras med och dokumentera detta i en åtgärdsplan.

Om åtgärderna innebär förändringar av anläggningen ska en revidering genomföras i enlighet med Post och telestyrelsen föreskrifter och allmänna råd om säkerhet i nät och tjänster.

Bild. Åtgärdsplan säkerhetsåtgärder

5.2 Skyddsnivå avseende skydd av elektronisk kommunikation

5.2.1 Siter

Analysera erforderliga åtgärder för att uppfylla kraven i *Bilaga 1 Robust Site för samhällsviktig digital infrastruktur*.

Åtgärdsanalys - Site			
Nr	**Åtgärd**	**Komponent**	**Kommentar**
1	Separata intag i anläggning	Datacenter #1 Linköping (DL)	
2	Reservkraftsystem - drifttid	N2, N5	
3	Skydd mot Elektromagnetisk störning	N3, N5	
4	Kameraövervakning (områdesskydd)	N4, N5	RSA
5	Mekaniskt områdesskydd	N5	
6	Passagekontroll (områdesskydd)	N5	
7	Släcksystem	N5	
8	Redundant Kylsystem	N5, N7	
9	Redundant elkraftsmatning	N5	

5.2.2 Förbindelser

Analysera erforderliga åtgärder för att uppfylla kraven i Bilaga 2 Passiv säker fysisk förbindelse för respektive framföringsväg.

Åtgärdsanalys - Förbindelser			
Nr	**Åtgärd**	**Komponent**	**Kommentar**
1	Byte av brunnar till godkända	DL-N1.1, N7-DN.1	
2	Byte av skåp till godkända brunnar	DL-N1.2, DL-N2.2	
3	Avlägsna sökbollar ur brunnar	N1-N4.2, N4-N6.2, N6-DN.1, N2-N3.2, N3-N5.1, N5-N7.1	Underjordsbrunnar
4	Styrd borrning	N4.N6.3, N2-N3.3	Ersätter broförläggning

5.3 Åtgärdsplan

Upprätta en åtgärdsplan för att hantera identifierade åtgärdsbehov enligt genomförda GAP-analyser. Åtgärdsplanen ska omfatta:

- Bakgrund till den genomförda analysen.
- Målet för införandet av identifierade åtgärder
- Beskrivning av respektive åtgärd:
    - Utförande
    - Risk- och konsekvensbedömning
    - Prioritet
    - Kostnadsbedömning
    - Tidplan för införandet
    - Ansvar för genomförandet
- Uppföljning av åtgärder

6 Projektering

Ta fram projekteringsunderlag, detaljprojektera och inför beslutad uppgradering av anläggningen.

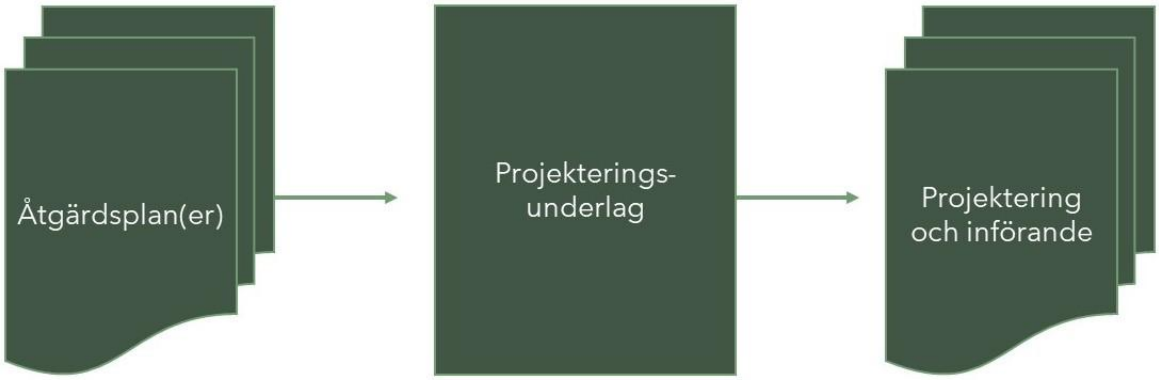


Bild. Projektering

För att genomföra projekteringen rekommenderas att följa anvisningen i *Robust fiber Bilaga 7 Anläggningsprojektering* alternativt befintlig projekteringsprocess.