

SÄKERHET, IT OCH BEREDSKAP

Bemästra Cybersäkerhetslagen NIS2

Gemensam kunskap för starkare riskhantering,
incidentberedskap och resiliens.

Fyra digitala moduler · cirka 1 timme · K3 eller SCORM



Identifiera

Bedöm

Åtgärda

Övervaka



Lagstiftningen gäller redan

Nu behövs ett gemensamt arbetssätt för cybersäkerhet i berörda verksamheter.

15 januari 2026

- Cybersäkerhetslagen och cybersäkerhetsförordningen trädde i kraft.
- Berörda verksamheter ska skydda nätverks- och informationssystem och rapportera betydande incidenter.
- NCSC anger systematiskt cybersäkerhetsarbete och utbildning av ledning och personal som centrala uppgifter.



Mindre risk. Större handlingskraft.

Kursen gör gemensamma förväntningar praktiska – från ansvar till vardagliga åtgärder.

Verksamhetsutmaning	Kursens bidrag
Otydliga riskprioriteringar	Tränar systematisk riskbedömning, allriskansats och proportionella åtgärder.
Olika beteenden vid hot	Gör phishing, ransomware, leverantörsrisker och incidentrespons konkreta.
Svår uppföljning av kompetens	Ger ett gemensamt underlag för tilldelning, test, dokumentation och repetition.

Beslutsnytta: en jämnare grundnivå som kan följas upp lokalt och skalas till hela organisationen.

En kurs för hela målgruppen

Gemensam riktning – med innehåll som gör skillnad i varje roll.



Ledning

Förstå ansvar, prioritera åtgärder och följa upp kompetens.



IT och säkerhet

Sätta risker, kontroller och lokala rutiner i rätt sammanhang.



Medarbetare

Känna igen hot och agera enligt verksamhetens vägledningar.



Administratörer

Tilldela, följa status och skapa underlag för kompetensarbetet.

Fyra moduler. En gemensam förmåga.

En koncentrerad kursresa från regelverk och risk till incidentberedskap och resiliens.

Modul	Fokus	Deltagaren blir tryggare i att
1	NIS2 i praktiken	förstå varför lagen och ansvaret berör verksamheten.
2	Riskhantering enligt NIS2	prioritera risker och arbeta med konkreta skyddsåtgärder.
3	Hot och incidenthantering	känna igen hot och agera strukturerat vid en incident.
4	Resiliens och träning	bygga förmåga genom övning, återhämtning och repetition.
Omfattning: cirka 1 timme, fördelad på fyra digitala 15-minutersmoduler.		

Riskhantering gör Artikel 21 konkret

Modul 2 översätter regelkrav till ett praktiskt, återkommande arbetssätt.

- **Allriskansats:** se hela hotbilden, inte bara kända risker.
- **Proportionella åtgärder:** koppla skyddet till storlek, exponering och konsekvens.
- **Riskmatris:** värdera sannolikhet och påverkan för att prioritera rätt.
- **Ledningens ansvar:** godkänn, följ upp och förbättra åtgärderna.



Autentisk kursbild från godkänd modul 2: riskmatrisen som praktiskt verktyg.

Målet är inte en engångsinsats – utan ett systematiskt sätt att prioritera och förbättra.

Praktiska scenarier tränar rätt beteenden

Igenkännbara situationer kopplar riskhanteringen till deltagarens vardag.



Autentisk kursbild: leverantörsangrepp och leveranskedjerisker.

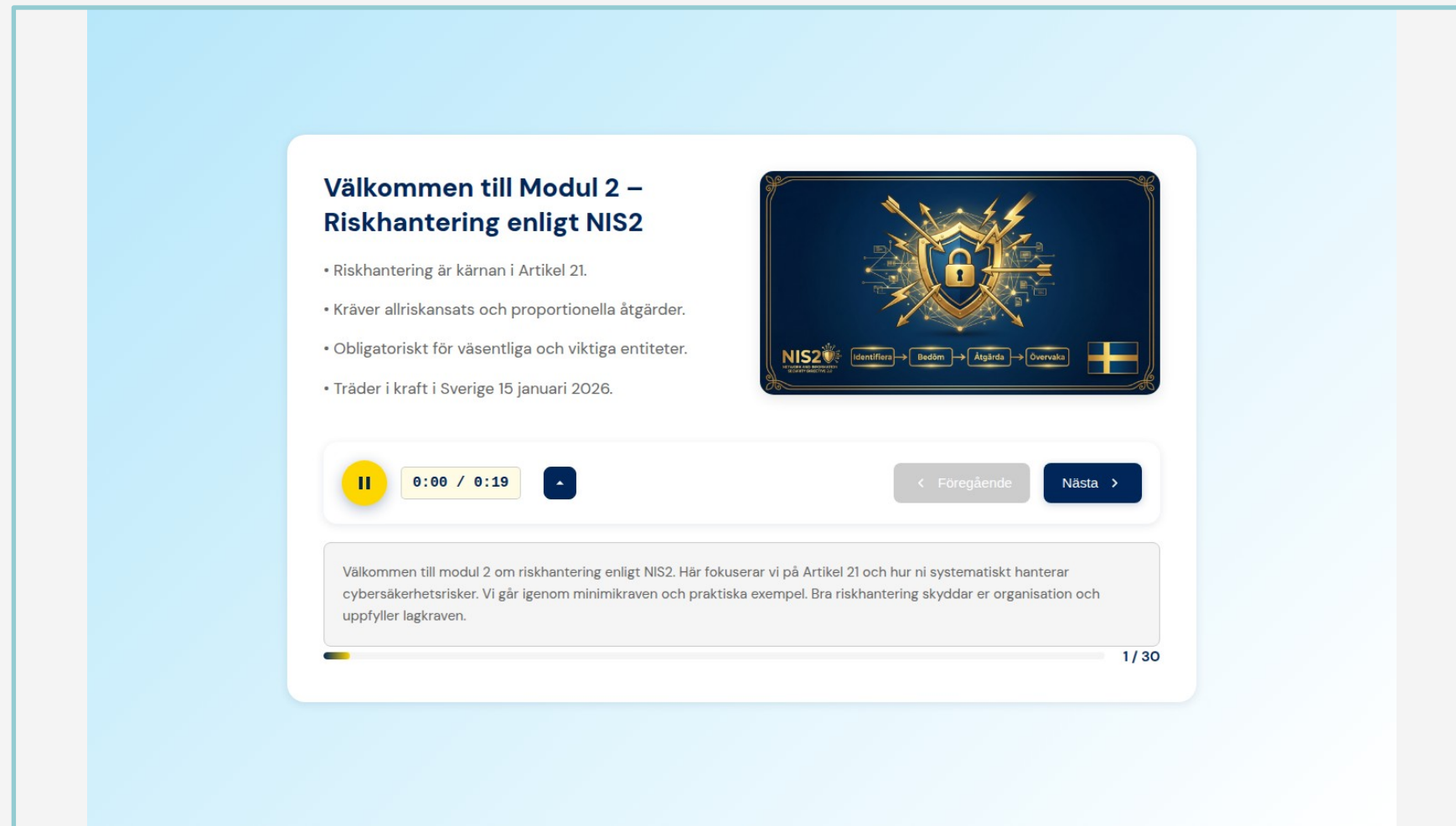
Exempel i kursen

- Phishing: från misstänkt e-post till rätt åtgärd.
- Ransomware: prioritera kritiska system och återställning.
- Leverantörsrisk: bygg krav, uppföljning och tydliga avtal.
- OT och dataläckage: begränsa spridning och skydda information.

Pedagogisk princip: teori, konsekvens, avgränsning och praktiskt exempel.

Deltagaren lär i ett tydligt flöde

Kursvyn gör det lätt att ta till sig innehållet, styra tempot och repetera.



Autentisk deltagarvy från den godkända SCORM-modulen.

- **Kursbild och stödtext** sätter situationen i sammanhang.
- **Spela/pausa och tidsvisning** låter deltagaren styra tempot.
- **Transcript** gör berättarrösten läsbar och tillgänglig.
- **Föregående, Nästa och förlopp** ger tydlig navigation och överblick.

K3 gör uppföljningen mätbar

Från tilldelning och kunskapskontroll till dokumentation och verifiering.



1. Tilldela

Rikta kursen till grupper, roller eller verksamheter.



2. Följ status

Se genomförande, kunskapskontroll och intyg.



3. Dokumentera

Godkänt sluttest kan ge ett certifikat från K3.



4. Verifiera

Unik kod kan kontrolleras publikt på verify.k3.io.

Ett K3-certifikat är ett verifierbart underlag för genomförd kurs – inte en yrkeslegitimation eller garanti för praktisk kompetens.

Inför på ett sätt som passar er

Välj leveransväg, målgrupp och uppföljning utifrån er organisation och era avtal.



Via K3

- Grupper, roller och riktade tilldelningar.
- Kunskapskontroller, intyg och status.
- Administrativ uppföljning i ett sammanhållet flöde.



Via eget LMS

- SCORM-kompatibelt kursformat.
- Leveransformat, metadata och uppföljning utreds mot er miljö.
- Tekniska möjligheter verifieras och avtalas före införande.

Kursens innehåll kan anpassas efter lokala instruktioner och kontaktvägar i K3.

Från behov till genomförd kompetens

Ett strukturerat införande bygger förankring, ger kontroll och gör repetition möjlig.



Kursen blir mest värdefull när den kopplas till verksamhetens egna rutiner, övningar och ansvar.

NÄSTA STEG

Gör cybersäkerhet till en gemensam förmåga.

Börja med en tydlig målgrupp, ett genomförbart upplägg och lokal uppföljning.

- Boka en behovsgenomgång.
- Välj målgrupp, leveransväg och pilot.
- Planera för tilldelning, test och repetition.

PUBLICERAT NORMALPRIS

2 990 kr

per deltagare
exkl. moms

Licens- och organisationsupplägg diskuteras
med Klick Data.