Styrelsens för ackreditering och teknisk kontroll författningssamling

SWEDAC

ISSN 1400-4682

Utgivare: Gerda Lind

STAFS 2013:xx
Utkom från trycket
den xx månad 20XX

Föreskrifter om ändring i Styrelsens för ackreditering och teknisk kontroll (Swedac) föreskrifter och allmänna råd (STAFS 2007:20) om evalueringsorganisationer som utvärderar IT-säkerhet;

beslutade den xx månad 20XX.

Styrelsen för ackreditering och teknisk kontroll (Swedac) föreskriver med stöd av 3 § förordningen (2011:811) om ackreditering och teknisk kontroll att 1 och 3 §§ styrelsens föreskrifter och allmänna råd (STAFS 2007:20) om evalueringsorganisationer som utvärderar IT-säkerhet ska ha följande lydelse.

1 § Dessa föreskrifter tillämpas på evalueringsorganisationer som är eller ansöker om att bli ackrediterade av SWEDAC för utvärdering av IT-säkerhet hos IT-produkter, IT-system samt skyddsprofiler, Protection Profile (PP).

Föreskrifterna är ett komplement till SWEDAC:s föreskrifter och allmänna råd (STAFS 2010:10) om ackreditering samt SWEDAC:s föreskrifter och allmänna råd (STAFS 2011:33) om ackreditering av laboratorier.

3 § Enligt 3 § första stycket SWEDAC:s föreskrifter och allmänna råd (STAFS 2011:33) om ackreditering av laboratorier skall en evalueringsorganisation uppfylla kraven i standarden SS-EN ISO/IEC 17025:2005.

Evalueringsorganisationen skall ge SWEDAC möjlighet att vid nyackreditering och tillsyn granska metoder och genomförande av utvärderingsuppdrag.

Denna författning träder i kraft den 1 januari 2014.

På Swedacs vägnar

PETER STRÖMBÄCK

Roland Jonsson

Föreskrifter om ändring i Styrelsens för ackreditering och teknisk kontroll (Swedac) föreskrifter och allmänna råd (STAFS 2007:21) om organ som certifierar IT-säkerhet;

beslutade den xx månad 20XX.

Styrelsen för ackreditering och teknisk kontroll (Swedac) föreskriver med stöd av 3 § förordningen (2011:811) om ackreditering och teknisk kontroll att 1–3 §§ styrelsens föreskrifter och allmänna råd (STAFS 2007:21) om organ som certifierar IT-säkerhet ska ha följande lydelse och beslutar att de allmänna råden till 3 § ska följande lydelse.

1 § Dessa föreskrifter tillämpas på certifieringsorgan som är eller ansöker om att bli ackrediterade av SWEDAC för certifiering av IT-säkerhet hos IT-produkter, IT-system samt skyddsprofiler, Protection Profile (PP).

Föreskrifterna är ett komplement till SWEDAC:s föreskrifter och allmänna råd (STAFS 2010:10) om ackreditering samt SWEDAC:s föreskrifter och allmänna råd (STAFS 2013:5) om ackreditering av organ som certifierar produkter.

2 § I dessa föreskrifter gäller de definitioner som anges i

1. standarden ISO/IEC 17065:2012 – *Certifieringsorgan – Allmänna krav vid certifiering av produkter (ISO/IEC 17065:2012)*, och
2. SIS Handbok 550 - *Terminologi för informationssäkerhet.*

Dessutom avses i dessa föreskrifter med

Evalueringsorganisation	Organisation eller organisationsenhet som utför utvärdering. Evalueringsorganisation kan även benämnas som evalueringsenhet eller evalueringsföretag.
Evalueringsrapport (Evaluation Technical Report)	Detaljerad teknisk rapport över genomförd utvärdering som lämnas av evalueringsorganisation till ett certifieringsorgan.
Certifieringsrapport (Certification/Validation Report)	Rapport vilken ges ut av det ackrediterade certifieringsorganet. Dokumentet summerar resultaten från utvärderingen och intygar det sammanlagda resultatet. Det intygar även att evalueringsmetoder och procedurer har tillämpats på ett korrekt sätt.

3 § Enligt 6 § första stycket SWEDAC:s föreskrifter och allmänna råd (STAFS 2013:5) om ackreditering av organ som certifierar produkter skall den som ansöker om ackreditering visa att de kravspecifikationer mot vilka certifiering under ackreditering

skall göras, samt tillämpningsdokument och dokument för tillverkningskontroll eller motsvarande, är entydiga och allmänt tillgängliga. Enligt andra stycket skall berörda intressenter ha getts tillfälle att delta i arbetet med att ta fram kravspecifikationerna.

Allmänt råd till 3 §[1]

Kravspecifikationerna kan exempelvis vara en utgåva av standarden ISO/IEC 15408 eller den internationella standarden Common Criteria (CC).

Denna författning träder i kraft den 1 januari 2014. 2 § i äldre lydelse ska dock fortsätta gälla för de organ som med stöd av 2 punkten i övergångsbestämmelserna till styrelsens föreskrifter och allmänna råd (STAFS 2013:5) om ackreditering av organ som certifierar produkter tillämpar 3 § styrelsens föreskrifter och allmänna råd (STAFS 2007:12) om ackreditering av organ som certifierar produkter.

På Swedacs vägnar

PETER STRÖMBÄCK

Roland Jonsson

[1] Ändringen innebär bl.a. att andra och tredje styckena upphävs.

Konsekvensutredning: Förslag till föreskrifter om ändring i Swedacs föreskrifter och allmänna råd (STAFS 2007:20) om evalueringsorganisationer som utvärderar IT-säkerhet samt förslag till föreskrifter om ändring i Swedacs föreskrifter och allmänna råd (STAFS 2007:21) om organ som certifierar IT-säkerhet

1. Bakgrund

Enligt artikel 4.1 i Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 ska varje medlemsstat i EU utse ett enda nationellt ackrediteringsorgan. I Sverige har Styrelsen för ackreditering och teknisk kontroll (Swedac) utsetts att vara nationellt ackrediteringsorgan i enlighet med nyssnämnd EU-förordning, se vidare 2 § förordningen (2009:895) med instruktion för Styrelsen för ackreditering och teknisk kontroll och 4 § lagen (2011:791) om ackreditering och teknisk kontroll.

Som nationellt ackrediteringsorgan enligt förordning (EG) nr 765/2008 är det Swedacs uppgift att tillämpa förordningen och i övrigt agera utifrån kraven i dess bestämmelser. Ett krav är att Swedac ska tillhandahålla ackreditering enligt definitionen av detta begrepp i artikel 2.10:

> 10. ackreditering: en förklaring från ett nationellt ackrediteringsorgan om att ett organ för bedömning av överensstämmelse uppfyller kraven i harmoniserade standarder och, i förekommande fall, eventuella ytterligare krav, bland annat de som fastställs i sektorsspecifika program, för att utföra specifika bedömningar av överensstämmelse

Swedac ska alltså ackreditera enligt *harmoniserade standarder*. Detta begrepp förklaras på följande sätt i artikel 2.9 i förordning (EG) nr 765/2008.

> 9. harmoniserad standard: en standard som på grundval av en begäran av kommissionen i enlighet med artikel 6 i Europaparlamentets och rådets direktiv 98/34/EG av den 22 juni 1998 om ett informationsförfarande beträffande tekniska standarder och föreskrifter och beträffande föreskrifter för informationssamhällets tjänster *[fotnot borttagen]* antagits av ett europeiskt

standardiseringsorgan som upptas i bilaga I till det direktivet

Hänvisningar till harmoniserade standarder offentliggörs, efter att de antagits enligt proceduren ovan, i Europeiska unionens officiella tidning.

För produktcertifieringsorgans vidkommande fanns tidigare en harmoniserad standard med beteckningen EN 45011:1998. Kraven i den standarden var bindande för sådana certifieringsorgan enligt Swedacs föreskrifter och allmänna råd (STAFS 2007:12) om ackreditering av organ som certifierar produkter. Detta i enlighet med vad som föreskrivs i förordning (EG) nr 765/2008.

Den gamla standarden ersattes sedermera av en ny harmoniserad standard med den fullständiga beteckningen EN ISO/IEC 17065:2012 Bedömning av överensstämmelse – Krav på organ som certifierar produkter, processer och tjänster. Hänvisning till den nya standarden har offentliggjorts genom Kommissionens meddelande 2013/C 258/05 inom ramen för genomförandet av Europaparlamentets och rådets förordning (EG) nr 765/2008, beslut nr 768/2008/EG och förordning (EG) nr 1221/2009. I enligt därmed upphävdes de gamla föreskrifterna och ersattes med nya föreskrifter, STAFS 2013:5, som hänvisar till den nya standarden.

I 2 § STAFS 2007:21 om organ som certifierar IT-säkerhet finns emellertid hänvisningar kvar till definitionerna i den gamla standarden. Den gamla standarden nämns också i några allmänna råd. För undvikande av missförstånd ska hänvisningen i 2 § ersättas med hänvisningar till den nu gällande standarden. De berörda allmänna råden bör strykas. Även i ett annat avseende görs en justering av de allmänna råden innebärande att en mening stryks, som inte i strikt mening är ett allmänt råd enligt definitionen av detta begrepp i 1 § författningssamlingsförordningen (1976:725).

Det finns också i 1 § andra stycket några hänvisningar, upplysningsvis, till andra föreskrifter utfärdade av Swedac. Dessa andra föreskrifter har emellertid upphävts, varför dessa hänvisningar ska ändras till att avse de nu gällande föreskrifterna.

Vad gäller STAFS 2007:20 om evalueringsorganisationer som utvärderar IT-säkerhet finns i 1 § andra stycket hänvisningar, likaledes upplysningsvis, till numera upphävda föreskrifter. Dessa hänvisningar ska på motsvarande sätt ändras till att avse de nu gällande föreskrifterna.

2. Alternativ

Som nämnts upplysningsvis ska Swedac, som nationellt ackrediteringsorgan enligt förordning (EG) nr 765/2008, ackreditera enligt harmoniserade standarder. Swedac har inget alternativ till att ändra i sina föreskrifter så att hänvisning till en upphävd harmoniserad standard upphävs och ersätts med en hänvisning till den nya harmoniserade standarden. Detta gäller särskilt som den nya harmoniserade standarden har gjorts bindande genom redan gällande föreskrifter.

3. Berörda

Det finns tre organ som är ackrediterade för att certifiera IT-säkerhet. Dessa omfattas redan av de nya föreskrifterna (STAFS 2013:5) om ackreditering av organ som certifierar produkter. De omfattas således redan av ett krav på att uppfylla kraven i den nya standarden, låt vara att punkten 2 i övergångsbestämmelserna till de nyssnämnda föreskrifterna ger dessa organ till den 16 september 2015 att tillämpa de nya kraven (en övergångsperiod som även den föreskrivs i Kommissionens meddelande 2013/C 258/05 ovan).

Genom det här remitterade förslaget kommer definitionerna i den nya standarden att gälla vid tolkningen av STAFS 2007:21, som huvudregel. Genom en övergångsbestämmelse klargörs emellertid att de gamla definitionerna gäller de organ som med stöd av ovannämnd övergångsbestämmelse i STAFS 2013:5 tillämpar den äldre standarden.

Det finns två laboratorier som är ackrediterade evalueringsorganisationer enligt STAFS 2007:20. Det här remitterade förslaget innebär ingen ändring i sak för dem.

4. Kostnadsmässiga konsekvenser

Inga nya kostnader införs genom de här föreslagna föreskrifterna.

5. Överensstämmelse med EU-krav

Hänvisning till ny harmoniserad standard är en direkt konsekvens av kravet i artikel 2.10 i förordning (EG) nr 765/2008 att Swedac ska tillhandahålla ackreditering enligt harmoniserade standarder. Utpekandet av EN ISO/IEC 17065:2012 som harmoniserad standard följer av ett beslut från Kommissionen. Även övergångsperioden följer av Kommissionens beslut.

6. Ikraftträdande och informationsinsatser

Det finns endast fem ackrediterade organ, som ska få utkastet och konsekvensutredning på remiss. Även branschorganisationen Swetic ska få föreskrifter och konsekvensutredning på remiss. Därmed är alla berörda informerade. Som ovan nämnts finns sedan tidigare en övergångsperiod avseende den nya standarden. Föreskrifterna bör därför träda i kraft snarast efter att de beslutats, i praktiken ca en månad efter beslut.

7. Effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt

Enligt Swedacs mening har de här föreslagna föreskrifterna inte några effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt.

8. Ikraftträdande

Föreskrifterna föreslås träda i kraft den 1 januari 2014.

9 Yttrande från Regelrådet

Inhämtas i samband med remissrundan.

10. Kontakt

Följande personer hos Swedac kan kontaktas vid eventuella frågor och för närmare upplysningar kring föreskriftsförslaget.

Tekniska frågor: Helén Dahl, tfn 033-177774
helen.dahl@swedac.se

Juridiska frågor: Henrik Carlborg, tfn 08-406 83 70
henrik.carlborg@swedac.se