

Legal Position

2025:1



Date 2025-12-10

FI Ref. 25-31002

Finansinspektionen
Box 7821
103 97 Stockholm
Tel +46 8 408 980 00
finansinspektionen@fi.se
www.fi.se

2025:1 Internal control over the protective security manager

Summary

A protective security manager as referred to in Chapter 2, section 7 of the Protective Security Act (2018:585) is a function in an undertaking's operational activities. The requirements on internal control of the operational activities that apply to the undertaking are therefore also applicable to the protective security manager.

This position targets undertakings within Finansinspektionen's scope of supervision pursuant to Chapter 8, section 1 of the Protective Security Ordinance (2021:955).

Question

In this legal position, Finansinspektionen discusses the relationship between the protective security manager and an undertaking's internal control functions. Is a protective security manager as referred to in Chapter 2, section 7 of the Protective Security Act a function in an undertaking's operational activities that is subject to the requirements on internal control and the internal control functions' responsibility?

Governing law

The Protective Security Act applies to actors in the public and private sector that to any extent conduct business that is of importance for Sweden's security or subject to a, for Sweden, mandatory international commitment regarding protective security. Pursuant to Chapter 2, section 7, first

paragraph of the Protective Security Act, there should be a protective security manager in a business that is subject to the law, unless such a manager is obviously not necessary. According to the second paragraph of the section, the protective security manager **shall** lead and coordinate the protective security work and control that the business is being conducted in accordance with the Protective Security Act and the regulations issued in conjunction with it.

In the commercial legislation on the financial market, there are also requirements of varying degrees on different types of undertakings to establish separate control functions that should monitor that the operational activities (which are often referred to as the first line of defence) are being conducted in accordance with applicable regulations. The control functions that do not report directly to the undertaking's board of directors (for example, the risk control and compliance functions) are often referred to as the second line of defence. An internal audit function that reports directly to the board of directors is often called the undertaking's third line of defence.

An example of extensive regulation related to undertakings' internal governance and control are the regulations that apply to credit institutions and are set out in the Banking and Financing Business Act (2004:297) and Finansinspektionen's regulations and general guidelines (FFFS 2014:1) on governance, risk management and control in credit institutions. Here, requirements are placed, for example, on credit institutions to establish risk control, compliance and internal audit functions that are to be independent from the functions and areas they will monitor.

Assessment

That the protective security manager leads and coordinates the protective security work at an undertaking entails, according to the Government's preparatory works for the Protective Security Act, that the protective security manager must be active and operational and not only passively monitor the protective security work ex ante (Bill 2020/21:194 p. 126). The regulation in Chapter 2, section 7, second paragraph of the Protective Security Act therefore entails that the protective security manager is a function in an undertaking's operational activities.

This means that the requirements on internal control of the operational activities that apply to an undertaking also apply in relation to the protective security manager. For example, if a credit institution is included in the scope

of the Protective Security Act, this means that the protective security manager and its work should be monitored, controlled and reviewed by the undertaking's risk control, compliance and internal audit functions.

Finansinspektionen notes that the person at an undertaking who will work with the internal control of the protective security manager may need to read protective security-classified information or have access to security-sensitive activities in general to be able to perform their tasks. This means that such an officer may be considered to be authorised to receive the information or access the activities assuming that even the other conditions set out in Chapter 2, section 2 of the Protective Security Ordinance are met.

This legal position applies until further notice.