D. Status of recommendations made in *Energy 2023* (Report 5: 2023–24)

Strengthen information system controls	Status
1. With the evolving security threats and advancement in security controls and technology, we recommend that the energy sector entities: • limit the access to information systems provided to employees and third-party contractors to only what they need to perform their jobs • monitor activities performed by employees and third-party contractors who have access to sensitive data and can make changes within the system • fully assess the design and effectiveness of any new controls they implement to ensure they do not create control gaps in other parts of the information system security chain • update security settings in line with updated risk assessments, security policies, and better practices. We also recommend energy entities continue implementing the following recommendations, which we made in our *Energy 2020* report: • provide security training for employees so they understand the importance of maintaining strong information systems, and their roles in keeping them secure • implement strong password practices and multifactor authentication (for example, a username and password, plus a code sent to a mobile), particularly for systems that record sensitive information • encrypt sensitive information to protect it • patch vulnerabilities in systems in a timely manner, as upgrades and solutions are made available by software providers, to address known security weaknesses that could be exploited by external parties.	**Further action needs to be taken** While entities are implementing our recommendations to resolve the issues we reported to them last year, we identified similar internal control deficiencies this year.