# 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:<br>• limit the access to information systems provided to employees and third-party contractors to only what they need to perform their jobs<br>• monitor activities performed by employees and third-party contractors who have access to sensitive data and can make changes within the system<br>• 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<br>• update security settings in line with updated risk assessments, security policies, and better practices.<br>We also recommend energy entities continue implementing the following recommendations, which we made in our *Energy 2020* report:<br>• provide security training for employees so they understand the importance of maintaining strong information systems, and their roles in keeping them secure<br>• 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<br>• encrypt sensitive information to protect it<br>• 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**<br>Entities are implementing our recommendations to resolve the deficiencies we reported last year. This resulted in the resolution of recommendations for:<br>• user access management – 3<br>• system security – 1<br>• privileged user accounts – 1<br>• change management – 1.<br>Resolution of the following recommendations is ongoing:<br>• privileged accounts – 7<br>• user access management – 6<br>• system security – 3.<br>Within 2025–26, we have re-raised 10 previously resolved deficiencies in the following areas:<br>• privileged accounts – 3<br>• system security – 1<br>• user access management – 6.<br>While entities are implementing our recommendations to resolve the issues we reported to them last year, we continued to identify similar internal control deficiencies this year. Further details are provided in our report *Information systems 2026* (Report 4: 2026–27). |