Management of the County of Marin
San Rafael, California

In planning and performing our audit of the financial statements of the governmental activities, the business-type activities, the aggregate discretely presented component units, each major fund, and the aggregate remaining fund information of the County of Marin as of and for the year ended June 30, 2017, in accordance with auditing standards generally accepted in the United States of America, we considered the County's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the County's internal control. Accordingly, we do not express an opinion on the effectiveness of the County's internal control.

However, during our audit we became aware of other matters that are opportunities to strengthen your internal control and improve the efficiency of your operations. Our comments and suggestions regarding those matters are summarized below. We previously provided a written communication dated January 30, 2018, on the entity's internal control. This letter does not affect our report on the financial statements dated January 30, 2018, nor our internal control communication dated January 30, 2018.

**Windows / Active Directory**

Observation

The County uses the Windows / Active Directory as the gateway to its resources. The Group Windows / Active Directory policy enforces the following password requirements:

- Minimum characters
- Complexity of password
- Password history
- Change frequency
- Unsuccessful login attempts before action is taken

Risk

Unauthorized or malicious activity may be performed on the County's technical infrastructure due to unauthorized workstation access that remains undetected for an extended period.

Recommendation

Windows / Active Directory Group policy should enforce the following password requirements:

- 10-12 minimum characters
- Complexity enabled
- 90 day change frequency

**Employee Terminations or Separations**

Observation

There is no formal process in place for reporting terminations or separations by the County's Human Resources Department to the County's Information Services and Technology (IST) Department.

Risk

Without appropriate notification for removal of terminated employees' access, there is an increased risk that the system could be used inappropriately since there is an open path to the organization's network.

Recommendation

All terminations or separations from County employment should trigger an event by Human Resources to notify IST to remove system access of terminated employee.

**Disaster Recovery Plan**

Observation

The County does not have a documented disaster recovery plan.

Risk

Although the County has taken various measures to address brief interruptions to systems processing (such as regular back-ups and redundancy), the lack of a plan in place does not address the recovery and resumption of critical systems and data in the event of an interruption due to changes in the environment and personnel. Such a disaster or major business interruption could prevent access to information systems and data.

Recommendation

The County should establish a disaster recovery plan to address its critical business processes, including the supporting computing and communications systems.

The Disaster Recovery Plan should address, at a minimum, the following key areas:

- **Performing a Business Impact Assessment** to determine the critical business processes and their maximum tolerable downtime
- **Developing a Recovery Strategy** to ensure recovery of the critical business processes within their maximum tolerable downtime
- **Developing Recovery Plans** to provide recovery, resumption, and restoration procedures for critical business processes
- **Implementing the Recovery Strategy and Recovery Plans** to enable emergency preparedness of pre-determined critical business processes and their supporting communications and computing systems

- **Developing and implementing Testing and Maintenance Programs** for periodic review and updating of the business continuity plan to ensure its viability

The plan should be tested on a regular basis to ensure its effectiveness. Tests should simulate a disaster or some aspect of a disaster and use the steps in the plan to restore continuity.

We will review the status of these comments during our next audit engagement. We have already discussed many of these comments and suggestions with various entity personnel, and we will be pleased to discuss them in further detail at your convenience, to perform any additional study of these matters, or to assist you in implementing the recommendations.

This communication is intended solely for the information and use of management, the Board of Supervisors, and others within the entity, and is not intended to be, and should not be, used by anyone other than these specified parties.

CliftonLarsonAllen LLP

**CliftonLarsonAllen LLP**

Roseville, California
January 30, 2018