The Background Screening Credentialing Council (BSCC) volunteer members drafted the accreditation tip for Clause 1.4 of the BSAAP Standard, version 2.0, effective April 6, 2018. This tip does not constitute a legal opinion of the BSCC.

The Background Screening Agency Accreditation Program's Accreditation Standard and Audit Criteria specifically require accredited firms to be in a position to both prevent, investigate and respond to data intrusions.

TITLE: Clause 1.4 - Intrusion and Data Security

Clause: CRA must have and follow procedures to prevent, detect, investigate and respond to an information system intrusion, including consumer notification and other breach notifications where mandated. At a minimum, procedures must meet all applicable legal and regulatory requirements.

A **Non-Conformity** sometimes identified for this clause is the absence of procedures and tools in place to prevent, detect, investigate and respond to an information system intrusion.

The Audit Criteria for Clause 1.4, of the BSAAP Standard with Audit Criteria, Version 2.0, Effective April 6, 2018 provides:

> *CRA must present proof of tools used to protect network, data, and consumer information. This may be third-party audit results, intrusion/detection testing results, firewall protections used, website security, or other recognized security protocols and devices. Auditor will seek evidence of adherence to policies and procedures.*
>
> *Process/procedure must include [sic] but is not limited to: 1) individual to contact in case of intrusion and his/her back-ups, 2) necessity of immediately stopping intrusion activity, if still occurring, 3) determination of notification requirements, 4) preparing notification/s, 5) obtaining necessary approvals of notification language, 6) communicating notification, and 7) de-brief to prevent future occurrences. Auditor will seek evidence of adherence to policies and procedures.*

As is detailed in the Measure & Documentation Typically Subject to Desk Audit and the Potential Verification for Onsite Audit columns associated with this Clause, the CRA must be able to produce procedures (including evidence of adherence to the same) for preventing, detecting, identifying and responding to information system intrusions, including consumer notice and other breach notice requirements.