

PD-ABU-972
113678

USAID

OFFICE OF INSPECTOR GENERAL

**Audit of General Controls Over
USAID/Regional Services Center/Budapest's Computer
Systems**

Audit Report No. B-185-02-001-P

March 14, 2002



**U.S. Agency for International Development
Budapest, Hungary**

A



U.S. AGENCY FOR
INTERNATIONAL
DEVELOPMENT

RIG/Budapest

March 14, 2002

MEMORANDUM

FOR: Director, USAID/Regional Services Center/Budapest,
Hilda Arellano

FROM: Director, Audit Operations, RIG/Budapest, *[Signature]*
Nathan S. Lokos

SUBJECT: Audit of General Controls Over USAID/Regional Services
Center/Budapest's Computer Systems (Report No. B-185-02-
001-P)

This is our final report on the subject audit. In preparing the report, we considered your comments on the draft report and included them in their entirety in Appendix II.

The report contains five recommendations and we consider management decisions to have been made on all five recommendations. Furthermore, we consider Recommendation Numbers 1, 2, 3 and 4 closed upon issuance of the report. Please advise the Bureau for Management, Office of Management Planning and Innovation, Management and Innovation Control Division (M/MPI/MIC) when final action is complete.

I appreciate the cooperation and courtesy extended to my staff during the audit.

Table of Contents

Summary of Results	3
Background	3
Audit Objective	4
Audit Findings	4
Are USAID/Regional Services Center/Budapest's general controls over the computer-processing environment effective?	4
Need to Implement an Effective Security Program	5
Need for Better Surveillance Over Systems Software and Computer Operations	7
Need to Develop and Test an Adequate Contingency Plan	9
Management Comments and Our Evaluation	10
Appendix I - Scope and Methodology	11
Appendix II - Management Comments	13
Appendix III - GAO's Categorization of General Controls	17

Summary of Results

We examined the USAID/Regional Services Center/Budapest's (RSC's) general controls over its computer systems and determined that those controls did not adequately protect against serious threats including unauthorized access to Mission Accounting and Control System (MACS) programs, data, and other computer resources. However, as a result of two recently completed computer security reviews—Security Risk Assessment and Security Certification and Accreditation Review—the RSC has corrected many of the weaknesses identified by those reviews (page 4). While most of the weaknesses identified by those two reviews have been corrected, security vulnerabilities remain in the areas of: 1) Entity-wide Security Program Planning and Management (page 5); 2) System Software and Computer Operations (page 7); and 3) Service Continuity (page 9).

Consequently, in spite of the recent improvements made by the RSC to its computer system security environment, its operations continue to be vulnerable to both unauthorized access and the disruption of service in the event of computer failure. This report includes recommendations to address these vulnerabilities.

Background

General computer controls are the policies, procedures, and management structures that help protect an organization's computer systems and operations. The primary objectives of general controls are to safeguard data, protect computer application programs and system software from unauthorized access, and ensure continued computer operations in case of unexpected interruptions.

USAID places extensive reliance on information systems to process financial statement data. It is, therefore, critical that USAID maintain adequate internal controls over the systems that support its financial statements. Previous Office of Inspector General (OIG) audits found that USAID did not have effective general controls over computers hosting its financial systems. In response to OIG recommendations, USAID management has taken action to improve its general controls. For example, USAID has implemented an agency-wide Security Program, under which the security of each of its major applications and general support systems will be formally certified and accredited. Moreover, security has been improved in the Mission Accounting and Control System (MACS), which is the accounting system used by USAID's overseas missions.

MACS is a computer-based accounting and financial management system that provides information to mission management and to USAID/Washington. MACS defines the guidelines, procedures, and standards used to record, analyze, and report accounting data and contains computer programs that

perform and facilitate accounting and financial management. During Fiscal Year 2001, the USAID/Regional Services Center/Budapest's (RSC's) MACS processed transactions totaling more than \$402 million in net obligations and \$229 million in disbursements.

At the RSC, the Information Resources Management Division (RSC/IRM)—which is under the supervision of the RSC's Executive Office—is responsible for operating the Mission's computer systems. RSC/IRM is also responsible for: 1) establishing information system computer processing requirements and implementing an effective security program; 2) processing all requests for computer access to the system; and 3) providing information system computer services. The Controller's Office is the primary user of MACS and is responsible for its operation. It relies on MACS to support the Mission's accounting, budgeting, cash management, financial analysis, and financial reporting operations.

Audit Objective

This audit is part of a worldwide series of audits that are being conducted by USAID's Office of Inspector General (OIG) pursuant to the Government Management Reform Act of 1994. The Office of Regional Inspector General/Budapest performed this audit to review the RSC's computer operations and, specifically, to answer the following audit objective:

Are USAID/Regional Services Center/Budapest's general controls over the computer-processing environment effective?

The scope and methodology of this audit are detailed in Appendix I.

Audit Findings

Are USAID/Regional Services Center/Budapest's general controls over the computer-processing environment effective?

The USAID/Regional Services Center/Budapest's (RSC's) general controls over the computer-processing environment are not effective. The Mission needs to implement an effective computer security program and develop a service continuity (contingency) plan. In addition, the Mission should strengthen its surveillance over systems software and computer operations.

The RSC has implemented many effective management controls necessary to properly protect its computer systems. For example, the RSC:

- Maintains a visitors log for persons entering the computer center;
- Has configured its UNIX (MACS) and Windows NT software to comply with USAID standards; and

- Has assigned and implemented MACS user roles.

All of these controls were instituted as a direct result of the work performed by two USAID Information Resources Management (IRM) teams in May 2001. One of these teams conducted a Security Risk Assessment and the other, a Security Certification and Accreditation review. When these efforts identified numerous vulnerabilities, the RSC took quick action to address those areas. As a result, based upon the RSC's corrective actions, the IRM teams concluded that the overall security of the Mission's computer systems was much improved. However, these teams also noted that some problem areas still existed. Like the IRM teams, we also found remaining security vulnerabilities that the Mission should address. Those vulnerabilities—and our associated recommendations—are discussed below.

Need to Implement an Effective Security Program

The RSC's Executive Officer did not establish an organization-wide computer security program as required by Office of Management and Budget's (OMB) Circular A-130 and USAID's Automated Directives System (ADS). Such a program is a key management control because it provides the foundation on which effective computer security practices can be implemented. By establishing a framework for planning and managing activities to assess risks, develop and implement security procedures, and monitor the effectiveness of the procedures, such a security program helps assure that sensitive data and resources will be protected in a cost-effective manner. Without a security program, risks may not be clearly understood, controls may not be effective, and limited resources may be used to protect against low-risk threats.

The RSC does not currently have an effective security program protecting its general support systems (e.g. email, word processing, etc.) or the MACS. However, RSC officials have implemented several components of such a program, including: 1) assigning user identifications and passwords; 2) requiring backup copies of MACS data to be stored off-site; and 3) using encrypted password files and suppressed passwords. Moreover, the RSC is in the process of developing its first Mission-wide security plan. Nevertheless, the Mission's current security program does not meet the requirements of the Computer Security Act of 1987¹, OMB's Circular A-130², or ADS³ because of the three

¹ According to the Computer Security Act of 1987, Federal agencies with computer systems that process sensitive information are required to identify and develop security plans for these systems and to provide training to persons managing, using, and operating these systems.

² The Office of Management and Budget's (OMB) Circular A-130 establishes a minimum set of controls to be included in Federal automated information system security programs. These controls include preparing and maintaining security plans, establishing and testing of contingency plans, and periodic review of security controls.

weaknesses discussed below.

The major requirements and practices that the RSC has not fully implemented are:

- Documenting and maintaining current security plans for sensitive systems;
- Preparing and testing an adequate contingency plan (This issue is discussed in detail on page 9); and
- Monitoring and evaluating the effectiveness of its security program.

Consequently, risks threatening RSC computer systems may not be identified or clearly understood, controls may not be effective, and limited resources may be used to protect against low-risk threats.

Until the recently completed security risk assessment the RSC had not evaluated or monitored its computer security requirements. That is, the Mission did not systematically monitor the security program, because it relied on the system administrator to establish and maintain the computer security program with little or no Information System Security Officer (ISSO) oversight. The Executive Officer, who has ISSO responsibility for computer security, did not establish procedures for ensuring that controls were operating as intended or otherwise evaluate the effectiveness of the security program because: 1) she lacked ISSO training and therefore the knowledge to effectively oversee the RSC's computer security program and 2) she had other competing tasks that she focused on.

The RSC underwent its first security risk assessment in May 2001 and, as a result, is in the process of strengthening its security program. Mission staff reported that they are correcting weaknesses identified by the assessment and advised us of actions they had taken, or plan to take, addressing these deficiencies. However, we believe the following recommendations are necessary to ensure that an effective security program is implemented and managed.

Recommendation No. 1: We recommend that the Director, USAID/Regional Services Center/Budapest strengthen general controls over its computer systems by implementing a computer security program that includes: 1) conducting periodic risk assessments of computer operations; 2) documenting and maintaining current security plans; and 3) monitoring and evaluating the effectiveness of its security program.

³ The ADS, Chapter 545, Automated Information Systems Security, documents the Agency's security policies and procedures for information systems security and lists the specific headquarters and mission responsibilities.

Recommendation No. 2: We recommend that the Director, USAID/Regional Services Center/Budapest include a statement specifying Information System Security Officer responsibilities in the Annual Evaluation Form for the Executive Officer or other program manager designated as the Information System Security Officer.

Recommendation No. 3: We recommend that the Director, USAID/Regional Services Center/Budapest arrange training for the Mission's Information System Security Officer in Information System Security Officer responsibilities.

Need For Better Surveillance Over Systems Software and Computer Operations

U.S. General Accounting Office's (GAO) Federal Information System Controls Audit Manual states that because of the powerful capabilities of system software, its use should be monitored to identify any inappropriate or unusual activity. However, the RSC's ISSO did not ensure that audit logs were generated and reviewed for any inappropriate or unusual behavior, or that the RSC's computer systems complied with USAID's security configuration standards. As a result, the RSC does not know whether its system software has been misused and has not had the protection afforded by USAID's computer security configuration standards. This occurred because the ISSO lacked technical knowledge of information system security techniques. Additionally, the ISSO had many other competing tasks that had higher priority than computer system security, so in effect, the Systems Administrator became the defacto ISSO—which resulted in inadequate segregation of duties.

System software is a set of programs designed to operate computer equipment. Generally, one set of system software is used to support and control a variety of applications that may run on the same computer hardware. For example, Microsoft Word and MACS are application programs that are controlled by system software. Such software helps control and coordinate the input, processing, output, and data storage associated with all of the applications that run on a system.

Controls over access to—and modification of—system software are essential in providing reasonable assurance that operating system-based security controls are not compromised and that the system will not be impaired. For example, utility programs are a normal component of system software that are used to perform system maintenance during normal processing operations. However, these system utilities can aid individuals with fraudulent or malicious intent. Data

manipulation and query utilities or tools can often be used to access, view and manipulate data without leaving an audit trail. Therefore, because of such powerful capabilities, the use of system software should be monitored to identify inappropriate or unusual behavior. Such behavior may indicate unauthorized access or that an individual is improperly exploiting his or her access privileges. This principle is recognized in the GAO's Federal Information System Controls Audit Manual which states that because of the powerful capabilities at the disposal of those who have access to system software, its use should be monitored to identify any inappropriate or unusual behavior.

We noted that the ISSO did not regularly monitor the use of systems software and utilities. In fact, the necessary computer audit trails and reports were not generated. We also noted that the ISSO had not periodically verified that the RSC's computer configuration complied with USAID's standard configuration. As a result, RSC management does not know whether its system software has been misused and has not had the protection afforded by USAID's computer security configuration standards.

This situation arose because the ISSO (the Executive Officer) did not have the technical knowledge necessary to perform her computer security role. Additionally, as the Executive Officer, she had many other competing duties, that she focused on. As a result, those computer security duties fell to the Systems Administrator. However, the ISSO and the Systems Administrator should serve as a "check and balance" on one another, so having the Systems Administrator ultimately responsible for both computer security and computer operations was an inadequate segregation of those duties which negated the critical control provided by an ISSO.

To the RSC's credit, Mission officials and the two security review teams took swift action to correct most of the vulnerabilities identified by the IRM Risk Assessment and Accreditation teams. However, to guard against the risk of inappropriate or unauthorized access to systems software, the Mission still needs to fully implement the recommendations made by those teams. Furthermore, the Mission also needs to ensure that the ISSO is monitoring the Mission's computer systems for compliance with USAID's security configuration standards and that audit logs are being generated and personally reviewed by the ISSO. We believe the following recommendation and the previous Recommendation Number 3 to train the ISSO are necessary to ensure that an effective security program is implemented and managed.

Recommendation No. 4: We recommend that the Director, USAID/Regional Services Center/Budapest require that the Executive Officer/Information System Security Officer periodically verify that the Mission's system settings

comply with USAID security standards and that audit trails are maintained and personally reviewed.

Need to Develop and Test an Adequate Contingency Plan

To ensure that critical operations can continue in emergencies, OMB Circular A-130, Appendix III and USAID's ADS Chapter 545 require that Missions have a plan to cope with potential disruptions (a contingency plan) and to periodically test the plan. However because the ISSO did not have the necessary technical knowledge and because the ISSO had many other competing tasks, the required contingency plan was not prepared and tested, as required. Consequently, the RSC faces unnecessarily high risk that its operations will be seriously impaired should a major service disruption or disaster occur.

While backup and recovery mechanisms for the RSC's information systems exist, these mechanisms have not been routinely tested, nor are they formally documented. Moreover, because there is no formal information system contingency plan, the RSC does not have a strategy for overcoming the loss of key personnel. For example, the System Administrator maintains absolute oversight over the RSC's information systems and is the critical resource for sustaining information systems operation. Despite the critical importance of this individual to the ongoing operation of the RSC's information systems, there is no clear plan for overcoming the loss of this individual. Finally, the RSC is in the process of developing a formal contingency plan based on a Contingency Plan template provided by the Security Risk Assessment team in May 2001. In an effort to expedite the contingency plan implementation process, we are providing the following recommendation.

Recommendation No. 5: We recommend that USAID/Regional Services Center/Budapest strengthen its general controls over information technology systems by developing, implementing, and testing a service continuity or contingency plan for sustaining the systems in the event of an emergency.

Effective general controls require on-going, routine attention to maintain the integrity, availability, and performance of sensitive information systems in a complex computer environment. While the RSC has made significant progress in addressing the information system vulnerabilities identified by the recent Security Risk Assessment and Security Certification and Accreditation reviews, more needs to be done. If the RSC is to adequately protect sensitive data and systems from unauthorized access, disclosure, and loss, it must implement and maintain an effective computer security program.

**Management
Comments and
Our Evaluation**

In general, the USAID/Regional Services Center/Budapest (RSC) agreed with the findings, conclusions, and recommendations in our report. For some areas, the RSC provided additional information and/or suggestions. In instances where we agreed with the RSC response, we revised our report appropriately. For example, Recommendation No. 2 was revised to reflect RSC's concerns and will be closed upon issuance of this report.

One area in which we disagreed with the RSC concerned our audit objective. As stated in this report, this audit was conducted pursuant to the Government Management and Results Act of 1994 (GMRA), which requires that executive branch agencies of the U.S. Government—including USAID—produce audited financial statements. Our audit objective focused on the RSC's general controls over its computer-processing environment, which includes the financially related computer programs and databases, such as the MACS, that handle the RSC's financial functions. In order to emphasize that this audit was driven by GMRA-related requirements, we considered changing the focus of our audit objective from the RSC's "computer processing environment," to its "financial management systems."

The RSC took exception to this change, stating that the concept of a "computer-processing environment" differs significantly from the concept of "financial management systems." What the RSC did not mention is that the phrase "general controls" is a term of art that refers to a set of internal controls surrounding computer application programs. By necessity, since these general controls safeguard the overall computer processing environment, they also protect the financial management systems, such as the Mission Accounting and Control System (MACS), MACSTRAX and other applications software that the RSC uses to carry out its financial functions. Our contemplated change in the audit objective was, in fact, not a significant change as claimed by the Mission. It was simply a reflection that this audit of general controls was conducted pursuant to the GMRA—which focuses on financial statement reporting. Ultimately, however, we decided to retain our original audit objective because that original objective had been previously used in similar audit reports issued by other USAID Regional Inspector General offices.

**Scope and
Methodology**

Scope

The Office of Regional Inspector General/Budapest conducted this audit, in accordance with generally accepted government auditing standards, to determine if USAID/Regional Services Center/Budapest's (RSC) general controls over the computer-processing environment are effective. We examined the controls in place to determine whether they were designed and implemented properly. Specifically, we assessed five of U.S. General Accounting Office's (GAO) six control elements: the security program; access controls; segregation of duties; system software; and service continuity controls (see Appendix III). We did not evaluate the application software development and change controls because the Mission did not develop application software. The audit was conducted at USAID Regional Services Center in Budapest, Hungary from June 11 through September 17, 2001.

Methodology

We used the GAO's Federal Information System Controls Audit Manual to evaluate RSC's general controls over its computer systems. We identified and reviewed the information system's general control policies and procedures. We tested and documented the extent to which RSC implemented the controls. Through discussions with the Acting Executive Officer, Controller, and System Administrator, we determined what controls existed. We tested and observed the operation of controls to determine if they were designed and operating effectively.

We verified the accuracy of information reported in the following three security related assessments of the RSC and verified actions taken by the RSC to correct the weaknesses reported:

USAID Security Office Comprehensive Security Assessment of USAID/Budapest's Operations, February 25, 1999;

Draft USAID/RSC E&E Security Assessment, conducted by USAID Information Resource Management's Risk Analysis Team, May 10, 2001; and

Draft USAID Security Certification and Accreditation (C&A) Approval Package for the General Support System (GSS) and the Mission Accounting and Control System (MACS) at USAID/Budapest, July 5, 2001.

The results of these three assessments indicated weaknesses in the RSC's implementation of security procedures.

We also reviewed: 1) the report prepared by the RSC in accordance with the 1982 Federal Managers' Financial Integrity Act for FY 2000; and 2) the draft report on the Inspection of the Embassy at Budapest, Hungary, dated July 2001, performed by the Department of State Office of Inspector General. The purpose of the inspection was to assess strength and weaknesses of the Embassy post, office and function. These two reports did not discuss any information system security issues related to the RSC. In addition, we reviewed USAID's Automated Directives System, Chapter 545, Information Systems Security, the Computer Security Act of 1978, and the OMB Circular A-130.



**U.S. Agency for International
Development
Regional Services Center, E&E**

MEMORANDUM

DATE: March 7, 2002

TO: Director of Audit Operations/Budapest
Nathan S. Lokos

FROM: Director of USAID Regional Services Center/Budapest
Hilda Arellano

SUBJECT: Audit Response, Audit of General Controls over USAID/Regional Services Center/Budapest's Computer Systems (Report No. B-185-01-00X-P).

Thank you for your memorandum of February 25, 2002, and the attached draft report on the subject audit. I request that the report be finalized and published. This latest draft is nearly identical to the last draft but with some brief, although significant, changes. I would like to first address these changes before providing comments on the audit recommendations.

As regards your request for an additional signed representation letter, please refer to my previous letter dated December 21, 2001. The previous letter covered the matters that were audited.

The most significant change in the report involves changing the audit objectives and audit findings sections of the report. Per your prior report, the audit objective originally sought to answer whether or not RSC's "general controls over the computer-processing environment are effective." The findings concluded that they were "generally effective." The revised report significantly changes the objective to whether or not RSC's "general controls over the financial management systems (are) effective," and the findings concluded that they "are not effective." A comparison of the two

versions of the report reveals that the balance of the report remains unchanged, including the scope and methodology.

Per the GAO publication Government Auditing Standards, the first field work standard for government performance audits is that the audit be adequately planned. The first step in planning is to carefully define the audit objectives, clearly articulating what the audit is to accomplish, and that planning should be tailored to the specific audit objective.

I find it questionable that the audit objective was changed after completion of the initial draft audit report, without any corresponding adjustment in scope, methodology, or conduct of additional field work. The concept of a "computer-processing environment" differs significantly from the concept of "financial management systems." I suggest that the scope and methodology was defined for the original audit objective and is not necessarily compatible with the scope and methodology required for the revised objective.

A second aspect of the revised report that I find questionable is the repeated text that the Executive Officer "apparently believed competing tasks had higher priority" as regards overseeing RSC's computer security program. As presented in the report, the allegation appears to be pure conjecture unsupported by the evidence.

Historically, the Agency has had a very poor record as regards computer security. There were neither active programs nor training available for Agency managers for this critical component of Agency operations. It was not until recently, when computer security was assigned to the Office of Information Resources Management (M/IRM), that such a program was started and candidates sought for a pilot site. Under the direction of the RSC Director and Executive Officer, this mission actively sought improvements to its computer security environment and successfully brought the M/IRM pilot program to Budapest, making RSC one of the first in the world to have its systems tested, accredited, and certified. I request that all references to the objectionable text be deleted from the final audit report.

As regards the five audit recommendations, I request that recommendations 1, 3 and 4 be closed upon the issuance of the final audit report. Recommendation 2 should be dropped from the final report, and recommendation 5 should reflect that a management decision has been reached towards the correcting action requested. For each, I offer the following comments:

Recommendation No. 1.: We recommend that the Director, USAID/Regional Support Center/Budapest strengthen general controls over its computer systems by implementing a computer security program that includes: (1) conducting periodic risk assessments of computer operations; (2) documenting and maintaining current security plans; and (3) monitoring and evaluating the effectiveness of its security program.

USAID/Regional Services Center/Budapest has implemented a Security Program and Plan, effective July 16, 2001. This plan will be periodically updated and maintained as required. Periodic Risk Assessments and Review of Security Controls will be performed at specified intervals, as per the Security Program and Plan. A Risk assessment was performed as part of the mission's systems' Certification and Accreditation. It was produced following a standardized methodology that is part

of an Agency-wide Risk Assessment program. Monitoring and evaluation of the security program is accomplished through an independent review of security controls (including risk assessment) every three years. In addition the EXO will ensure internal security controls are evaluated internally on a continuing basis (as per the security plan). Security controls for the Budapest GSS and MACS application environment have been independently evaluated and tested as part of system Certification and Accreditation and found to be generally sound. I request that this recommendation be closed upon issuance of the final audit report.

Recommendation No. 2: We recommend that the Director, USAID/Regional Support Center/Budapest include a statement specifying Information System Security Officer responsibilities in the work objectives of the Executive Officer or Other Program manager designated as the information Systems Security Officer.

In consultation with the Executive Officer I respectfully disagree with this audit recommendation and ask that it be dropped from the final audit report. Per ADS 462, work objectives are defined as the "expectations for an employee established by management for a particular rating period." ISSO responsibilities are a continuing responsibility for the Executive Officer, as are the other EXO responsibilities such as GSO, Personnel, Motor Pool, Procurement, Property Management and Travel. Since ISSO responsibilities are a part of the role the EXO has in the organization they should not be in Section 3 (Work Objectives) of the Annual Evaluation Form, but rather in Section 2 (Role in the Organization).

Recommendation No. 3: We recommend that the Director, USAID/Regional Support Center/Budapest arrange training for the Mission's Information System Security Officer in Information System Security Officer Responsibilities.

The current EXO and designated ISSO, Alexander Bond, completed ISSO training in January 2002. I request that this recommendation be closed upon issuance of the final audit.

Recommendation No. 4: We recommend that the Director, USAID/Regional Support Center/Budapest require that the Executive Officer/Information Systems Security Officer periodically verify that the Mission's systems settings comply with USAID security standards and that audit trails are maintained and personally reviewed.

The Executive Officer will oversee periodic evaluations of the systems settings through use of the Security Configuration Checklists and, as deemed appropriate, assistance from M/IRM. Since the issuance of your last draft of this audit report, RSC invited M/IRM to Budapest to conduct an ad hoc assessment of our security environment and systems, including specific reference audit trails. Per the IRM team's report, RSC's security settings are all to Agency standard and functioning properly. The level of auditing is compliant with the M/IRM Server Security Checklist. Three audit log files are generated and been stored on the NT server. The system log has been active since January '01, the security log since June '00, and the applications log since June '01. Accordingly, I request that this recommendation be closed upon issuance of the final audit report.

Recommendation No. 5: We recommend that USAID/Regional Support Center/Budapest strengthen its general controls over information technology systems by developing, implementing, and testing a service continuity or contingency plan for sustaining the systems in the event of an emergency.

As part of the Security Program and Plan, USAID/RSC is preparing a contingency plan which will be completed and tested by March 31, 2002. I request that the final audit report reflect that a management decision has been made with respect to the preparation and testing of the contingency plan, and that Recommendation No. 5 be closed upon completion of contingency plan test.

Clearances:

Cecile Adams
Controller

Alexander Bond
Executive Officer

**GAO's
Categorization of
General Controls**

No.	Critical Elements	Description
1.	Security Program	Provides the framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related controls.
2.	Access Controls	Limits or detects access to computer resources. Thus, these controls protect the resources from unauthorized modification, loss, and disclosure.
3.	Application Software Development and Change Controls	Prevents unauthorized programs or modifications to an existing program from being implemented.
4.	Segregation of Duties	Policies, procedures, and an organizational structure established so that one individual cannot control key aspects of computer-related operations.
5.	System Software	Limits and monitors access to the powerful programs and sensitive files that (1) control the computer hardware, and (2) secure applications supported by the system.
6.	Service Continuity	Ensures that, when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.