trusted computer system evaluation criteria

Trusted Computer System Evaluation Criteria: Understanding the Foundations of Secure Systems

trusted computer system evaluation criteria serve as the backbone for assessing the security and reliability of computer systems, especially those handling sensitive or classified information. In today's digital age, where cyber threats are increasingly sophisticated, organizations must ensure their systems meet rigorous standards to protect data integrity, confidentiality, and availability. These criteria not only guide developers and security professionals in building robust systems but also help users and regulatory bodies evaluate whether a system can be trusted to operate in secure environments.

Exploring these evaluation criteria reveals a fascinating blend of technical specifications, security policies, and assurance processes that collectively define what it means for a system to be "trusted." This article delves into the essential aspects of trusted computer system evaluation criteria, highlighting their significance, core components, and practical implications.

What Are Trusted Computer System Evaluation Criteria?

At its core, trusted computer system evaluation criteria refer to a set of standards and methodologies used to assess how well a computer system enforces security policies and withstands potential threats. These criteria emerged from the need to create a systematic approach to security evaluation, ensuring that systems claiming to be secure can be objectively tested and verified.

One of the most renowned frameworks in this domain is the Trusted Computer System Evaluation Criteria (TCSEC), also known as the Orange Book, developed by the U.S. Department of Defense in the 1980s. Though newer standards like the Common Criteria have since evolved, TCSEC laid the foundation for understanding how to categorize computer systems based on their security features and assurance levels.

The Purpose Behind Evaluation Criteria

Why do organizations need trusted evaluation criteria? The answer lies in the complexity of modern computing environments. Without clear standards, claims of security are often unverifiable, leaving systems vulnerable to exploitation. Trusted evaluation criteria provide:

- **Objective benchmarks** to measure security capabilities.
- **Guidance for system developers** to design secure architectures.
- **Confidence for users and administrators** that systems meet necessary protections.
- **A framework for certification and accreditation** processes.

Core Components of Trusted Computer System Evaluation Criteria

Understanding the key elements that make up these evaluation criteria helps in grasping how systems are judged for trustworthiness.

Security Policy

A fundamental requirement is a clearly defined security policy. This policy outlines how information is to be protected and who has access to what data. Trusted systems must enforce this policy consistently, preventing unauthorized access or data leaks.

For example, the Bell-LaPadula model focuses on maintaining confidentiality by enforcing access controls based on security levels. Trusted systems often incorporate such formal models to underpin their security policies.

System Architecture and Design

The design of the system plays a crucial role in trustworthiness. Evaluation criteria examine whether the system architecture supports security objectives such as separation of duties, least privilege, and secure communication.

Key design considerations include:

- **Modularity:** Systems designed in well-defined, isolated components reduce the risk of wide-ranging failures.
- **Trusted Computing Base (TCB):** This is the combination of hardware, software, and controls that enforce the security policy. A smaller, verifiable TCB is preferable as it minimizes the attack surface.
- **Reference Monitor Concept:** The system must have a mechanism that reliably enforces access controls and cannot be bypassed.

Assurance and Verification

Assurance refers to the confidence that the system's security features work as intended. Trusted evaluation criteria emphasize rigorous testing, formal verification, and documentation to provide evidence of compliance.

Assurance techniques include:

- **Code reviews and audits:** Identifying potential vulnerabilities in the system code.
- **Formal methods:** Using mathematical proofs to verify security properties.
- **Penetration testing:** Simulating attacks to uncover weaknesses.

The depth of assurance varies with the evaluation level, with higher levels requiring more stringent verification.

Levels of Trust in Evaluation Criteria

Trusted computer system evaluation criteria often categorize systems into different levels of trust, reflecting the degree of security assurance provided.

Understanding the Classification

Taking TCSEC as an example, systems were classified from D (minimal protection) to A1 (verified design). Each ascending level imposes stricter requirements:

- **D – Minimal protection:** Systems with little or no security features.
- **C1 and C2 – Discretionary protection:** Basic access controls and identification mechanisms.
- **B1, B2, B3 – Mandatory protection:** More sophisticated controls, auditing, and separation of functions.
- **A1 – Verified design:** Formal design and verification ensuring the highest assurance.

These gradations help organizations select systems appropriate for the sensitivity of the data they handle.

Modern Adaptations: The Common Criteria

Today, the Common Criteria (CC) is the international standard that supersedes older models like TCSEC. CC offers a flexible framework where products are evaluated against Protection Profiles (PP) and Security Targets (ST), allowing tailored assessments.

The CC introduces Evaluation Assurance Levels (EAL), ranging from EAL1 (functionally tested) to EAL7 (formally verified design and tested), providing a scalable approach to evaluate trustworthiness.

Practical Considerations When Applying Trusted Computer System Evaluation Criteria

While these criteria provide a robust framework, applying them in real-world scenarios involves thoughtful considerations.

Balancing Security and Usability

Highly secure systems often introduce complexity that can hinder usability. For trusted evaluation criteria to be effective, systems must find a balance where security controls do not overly burden users or impede operational efficiency.

For instance, strict access controls and multi-factor authentication enhance security but require user training and seamless integration to avoid frustration.

Contextual Relevance

Not all systems require the same level of trust. Evaluating systems based on their intended use and threat environment ensures resources are allocated appropriately.

A system handling classified government data demands rigorous evaluation, whereas a commercial website may prioritize other aspects like performance and user experience.

Continuous Monitoring and Re-evaluation

Achieving a trusted status is not a one-time event. As threats evolve, systems must be continuously

monitored, patched, and re-evaluated against current criteria to maintain trustworthiness.

Automated tools for vulnerability scanning and compliance checks aid in ongoing assurance.

Benefits of Adhering to Trusted Computer System Evaluation Criteria

Organizations that implement and adhere to trusted evaluation standards enjoy multiple advantages beyond just improved security.

- **Regulatory Compliance:** Many industries require adherence to recognized security standards.
- **Risk Reduction:** Identifying and mitigating vulnerabilities proactively reduces the likelihood of breaches.
- **Customer Confidence:** Demonstrating commitment to security builds trust with clients and partners.
- **Competitive Advantage:** Certified products stand out in markets where security is a key concern.

Encouraging a Security-First Mindset

Beyond technical measures, trusted evaluation criteria encourage organizations to foster a culture that prioritizes security at every level—from development teams to end-users. This holistic approach is vital to sustaining secure systems in dynamic environments.

Trusted computer system evaluation criteria remain an essential part of cybersecurity strategy, offering a well-founded approach to measuring and assuring system security. By understanding these criteria, stakeholders can better navigate the complex landscape of system trustworthiness, ensuring that

technology serves its purpose without compromising sensitive information or operational integrity.

Frequently Asked Questions

What is the Trusted Computer System Evaluation Criteria (TCSEC)?

The Trusted Computer System Evaluation Criteria (TCSEC), also known as the Orange Book, is a United States Department of Defense standard that sets basic requirements for assessing the effectiveness of security controls built into a computer system. It categorizes systems based on their ability to enforce security policies, particularly focusing on confidentiality.

What are the main security classes defined in the TCSEC?

TCSEC defines security classes ranging from D to A, where D represents minimal protection and A represents verified protection. The main classes are D (Minimal Protection), C (Discretionary Protection), B (Mandatory Protection), and A (Verified Protection), with each class having progressively stricter security requirements.

How does the TCSEC evaluate a system's security?

TCSEC evaluates a system’s security based on criteria such as identification and authentication, discretionary and mandatory access control, auditing, and assurance measures. Systems are assessed on how well they enforce access controls, protect data confidentiality, and provide mechanisms for accountability.

What is the significance of the TCSEC in modern computer security?

Although TCSEC was developed in the 1980s, it laid the foundation for formal security evaluation criteria and influenced later standards like the Common Criteria. Its significance lies in establishing a structured approach to evaluating security features and assurance in computer systems.

How does TCSEC differ from the Common Criteria?

TCSEC focuses primarily on confidentiality and access control within military and government systems, using a hierarchical classification system. The Common Criteria is an international standard that provides a more flexible and comprehensive framework for evaluating a wide range of security properties across various products and environments, allowing for more tailored evaluations.

Additional Resources

Trusted Computer System Evaluation Criteria: A Comprehensive Analysis

trusted computer system evaluation criteria serve as the backbone for assessing the reliability, security, and overall integrity of computer systems, especially those deployed in sensitive or mission-critical environments. In an era where cyber threats escalate daily and data breaches can have catastrophic consequences, understanding these evaluation criteria is fundamental for organizations, government agencies, and security professionals alike. This article delves into the primary frameworks and methodologies that define trusted computer system evaluation, shedding light on their significance, application, and evolution.

Understanding Trusted Computer System Evaluation Criteria

Trusted computer system evaluation criteria refer to the standardized benchmarks and processes used to measure the trustworthiness of computing environments. These criteria assess how well a system enforces security policies, protects data confidentiality and integrity, and resists unauthorized access or tampering. The goal is to provide stakeholders with confidence that the system can reliably perform its intended security functions under expected conditions.

Such evaluations are crucial for systems handling classified information, financial transactions, or critical infrastructure control. They help ensure compliance with regulatory requirements and establish

a common language for security assurance across vendors and users.

The Historical Context: The Orange Book and Beyond

The origin of trusted computer system evaluation criteria can be traced back to the Trusted Computer System Evaluation Criteria (TCSEC), colloquially known as the Orange Book, developed by the United States Department of Defense (DoD) in the 1980s. The Orange Book introduced a hierarchical classification system ranging from D (minimal protection) to A1 (verified design), outlining specific requirements for system architecture, access controls, and audit capabilities.

While revolutionary at the time, the Orange Book's focus was largely on military-grade security and specific hardware-software combinations. As technology evolved, so too did the need for more adaptable and internationally recognized evaluation frameworks.

Modern Evaluation Frameworks and Standards

Today, trusted computer system evaluation criteria encompass a variety of standards tailored to diverse applications and environments. The most prominent among these include the Common Criteria (CC), Federal Information Processing Standards (FIPS), and the Information Technology Security Evaluation Criteria (ITSEC).

Common Criteria (CC): The Global Standard

The Common Criteria, formally known as ISO/IEC 15408, represents the global standard for computer security certification. It offers a flexible, modular approach enabling evaluators to assess security properties based on Protection Profiles (PPs) and Security Targets (STs) specified by vendors or users.

Key features of the Common Criteria include:

- **Evaluation Assurance Levels (EALs):** Ranging from EAL1 (functionally tested) to EAL7 (formally verified design and testing), these levels indicate the depth and rigor of the evaluation.
- **Security Functional Requirements (SFRs):** Detailed security functionalities a system must implement, such as identification and authentication, access control, and cryptographic support.
- **Security Assurance Requirements (SARs):** Focus on assurance measures like configuration management, delivery, and vulnerability assessment.

Because it is internationally recognized, Common Criteria facilitates mutual recognition agreements (MRAs) among participating countries, streamlining certification acceptance worldwide.

Federal Information Processing Standards (FIPS)

FIPS are publicly announced standards developed by the National Institute of Standards and Technology (NIST) for use within U.S. federal agencies. Among these, FIPS 140 series is particularly relevant for trusted system evaluation, focusing on cryptographic modules.

FIPS 140-3, the latest iteration, specifies security requirements for cryptographic modules, ensuring they meet stringent criteria for physical security, key management, and operational environment. Systems reliant on cryptographic functions are often evaluated against FIPS standards to ensure compliance and trustworthiness.

Information Technology Security Evaluation Criteria (ITSEC)

Developed primarily in Europe, ITSEC offered a more flexible alternative to the Orange Book before the widespread adoption of Common Criteria. ITSEC allowed independent evaluation of functionality and assurance, enabling tailored certification. Though largely supplanted by Common Criteria, ITSEC contributed significantly to the evolution of evaluation methodologies.

Core Components of Trusted Computer System Evaluation

Despite differences in frameworks, several core components are consistently emphasized when evaluating trusted computer systems.

Security Policy Enforcement

A system's ability to enforce a defined security policy is paramount. This includes mechanisms to control access based on user identity, roles, or security clearance. The evaluation scrutinizes whether the system reliably implements mandatory access control (MAC), discretionary access control (DAC), or role-based access control (RBAC) as appropriate.

Identification and Authentication

Trusted systems must robustly identify and authenticate users or processes attempting to access resources. Evaluation criteria assess the strength and resilience of authentication mechanisms, such as multi-factor authentication, biometric verification, and cryptographic tokens.

Audit and Accountability

Audit capabilities that generate detailed logs of security-relevant events are critical for accountability and forensic analysis. Evaluators review whether the system records sufficient data, protects audit logs from tampering, and supports timely review and analysis.

System Integrity and Assurance

Integrity mechanisms ensure the system's software and hardware components are protected from unauthorized modification. Trusted system evaluation involves verifying the presence of trusted computing bases (TCBs), secure boot processes, and tamper-evident hardware features. Assurance measures also include rigorous development processes, testing, and vulnerability assessments.

Recovery and Continuity

Evaluation criteria often consider how systems handle failures or attacks. Trusted systems should support recovery procedures that restore secure operation without compromising sensitive data or security policies.

Challenges and Considerations in Applying Evaluation Criteria

While trusted computer system evaluation criteria provide a structured approach to security assessment, they are not without limitations. One ongoing challenge is balancing the depth of evaluation with cost and time constraints. High-assurance certifications, such as EAL6 or EAL7 under Common Criteria, require extensive formal methods and testing, which may be prohibitive for commercial products.

Moreover, the rapid pace of technological innovation, including cloud computing, virtualization, and Internet of Things (IoT) devices, complicates traditional evaluation models. Many frameworks are adapting to address these new paradigms, but gaps remain in evaluating dynamically changing environments or composite systems.

There is also the risk that certifications may be treated as checkboxes rather than genuine indicators of security posture. Effective security demands continuous monitoring and adaptation beyond initial evaluation.

The Role of Trusted Computer System Evaluation in Contemporary Security Landscapes

In today's interconnected world, trusted computer system evaluation criteria continue to play a vital role in establishing baseline security assurances. Governments rely on them to protect national security assets, while industries such as banking, healthcare, and telecommunications use these standards to safeguard sensitive information.

By providing a common language and methodology, these criteria enable informed decision-making when selecting and deploying technology solutions. They also foster competition among vendors to achieve higher assurance levels, driving innovation in secure design.

However, as cyber threats evolve, there is a growing recognition that trusted computing evaluation must be complemented by holistic security strategies incorporating threat intelligence, incident response, and user education.

Trusted computer system evaluation criteria remain a cornerstone of cybersecurity assurance, offering a rigorous framework to validate system trustworthiness. Their continued evolution and integration into

broader security ecosystems are essential to address the complexities of modern computing environments and the ever-increasing stakes of digital trust.

Trusted Computer System Evaluation Criteria

trusted computer system evaluation criteria: Department of Defense Trusted Computer System Evaluation Criteria United States. Department of Defense, 1985

trusted computer system evaluation criteria: Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria , 1994-03

trusted computer system evaluation criteria: Department of Defense Trusted Computer System Evaluation Criteria United States. Department of Defense, 1987

trusted computer system evaluation criteria: *Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria* , 1988 This document provides interpretations of the Department of Defense Trusted Computer System Evaluation Criteria (DoD 52O0.28-STD or TCSEC) for computer security subsystems. A computer security subsystem (subsystem) is defined, herein, as hardware, firmware and/or software which can be added to a computer system to enhance the security of the overall system. A subsystem's primary utility is to increase the security of a computer system. The computer system that the subsystem is to protect is referred to as the protected system in this Interpretation. When incorporated into a system environment, evaluated computer security subsystems may be very effective in reducing or eliminating certain types of vulnerabilities whenever entire evaluated systems are unavailable or impractical.--DTIC.

trusted computer system evaluation criteria: Computer Security Requirements , 1985

trusted computer system evaluation criteria: Department of Defense Trusted Computer System Evaluation Criteria , 1985 The trusted computer system evaluation criteria defined in this document classify systems into four broad hierarchical divisions of enhanced security protection. The criteria provide a basis for the evaluation of effectiveness of security controls built into automatic data processing system products. The criteria were developed with three objectives in mind: (a) to provide guidance to manufacturers as to what to build into their new, widely- available trusted commercial products in order to satisfy trust requirements for sensitive applications and as a standard for DoD evaluation thereof; (b) to provide users with a yardstick with which to assess the degree of trust that can be placed in computer systems for the secure processing of classified or other sensitive information; (c) to provide a basis for specifying security requirements in acquisitions. Two types of requirements are delineated for secure processing: (a) specific security feature requirements and (b) assurance requirements. Some of the latter requirements enable evaluation personnel to determine if the required features are present and functioning as intended.

trusted computer system evaluation criteria: Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria , 1987

trusted computer system evaluation criteria: Technical Rationale Behind CSC-STD-003-85, Computer Security Requirements , 1988

trusted computer system evaluation criteria: Trusted Network Interpretation of the Trusted

Computer System Evaluation Criteria. Version 1 , 1987 Part I of this document provides interpretations of the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) (DOD-5200.28-STD), for trusted computer/communications network systems. The specific security feature, the assurance requirements, and the rating structure of the TCSEC are extended to networks of computers rangings from isolated local area networks to wide-area internetwork systems. Part II of this document describes a number of additional security services (e.g., communications integrity, denial of service, transmission security) that arise in conjunction with networks. Those services available in specific network offerings, while inappropriate for the rigorous evaluation applied to TCSEC related feature and assurance requirements, may receive qualitative ratings.

trusted computer system evaluation criteria: Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria , 1993-06 Provides interpretation of the DoD Trusted Computer System Evaluation Criteria for computer security subsystems.

trusted computer system evaluation criteria: Department of Defense Trusted Computer System Evaluation Criteria Computer Security Center (U.S.), 1983

trusted computer system evaluation criteria: Trusted Computer System Evaluation Criteria Computer Security Center (U.S.), 1985

trusted computer system evaluation criteria: Department of Defense Trusted Computer System Evaluation Criteria Sheila Brand, 1985-06-01 Presents trusted computer system evaluation criteria providing a basis for the evaluation of effectiveness of security controls built into automatic data processing systems. Provides a standard to manufacturers as to what security features to build into new and planned commercial products, a metric with which to evaluate the degree of trust that can be placed in computer systems for the secure processing of classified and other sensitive information, and a basis for specifying security requirements in acquisition specifications. Includes appendices, glossary and references.

trusted computer system evaluation criteria: Trusted Computer System Evaluation Criteria Gerard Blokdyk, 2017-09-24 This exclusive Trusted Computer System Evaluation Criteria self-assessment will make you the dependable Trusted Computer System Evaluation Criteria domain auditor by revealing just what you need to know to be fluent and ready for any Trusted Computer System Evaluation Criteria challenge. How do I reduce the effort in the Trusted Computer System Evaluation Criteria work to be done to get problems solved? How can I ensure that plans of action include every Trusted Computer System Evaluation Criteria task and that every Trusted Computer System Evaluation Criteria outcome is in place? How will I save time investigating strategic and tactical options and ensuring Trusted Computer System Evaluation Criteria opportunity costs are low? How can I deliver tailored Trusted Computer System Evaluation Criteria advise instantly with structured going-forward plans? There's no better guide through these mind-expanding questions than acclaimed best-selling author Gerard Blokdyk. Blokdyk ensures all Trusted Computer System Evaluation Criteria essentials are covered, from every angle: the Trusted Computer System Evaluation Criteria self-assessment shows succinctly and clearly that what needs to be clarified to organize the business/project activities and processes so that Trusted Computer System Evaluation Criteria outcomes are achieved. Contains extensive criteria grounded in past and current successful projects and activities by experienced Trusted Computer System Evaluation Criteria practitioners. Their mastery, combined with the uncommon elegance of the self-assessment, provides its superior value to you in knowing how to ensure the outcome of any efforts in Trusted Computer System Evaluation Criteria are maximized with professional results. Your purchase includes access to the $249 value Trusted Computer System Evaluation Criteria self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows your organization exactly what to do next. Your exclusive instant access details can be found in your book.

trusted computer system evaluation criteria: *Trusted Computer System Evaluation Criteria a Complete Guide* Gerardus Blokdyk, 2018-04-09 Meeting the Challenge: Are Missed Trusted Computer System Evaluation Criteria opportunities Costing you Money? Is the scope of Trusted

Computer System Evaluation Criteria defined? What are the revised rough estimates of the financial savings/opportunity for Trusted Computer System Evaluation Criteria improvements? How are the Trusted Computer System Evaluation Criteria's objectives aligned to the organization's overall business strategy? How to Secure Trusted Computer System Evaluation Criteria? Defining, designing, creating, and implementing a process to solve a challenge or meet an objective is the most valuable role... In EVERY group, company, organization and department. Unless you are talking a one-time, single-use project, there should be a process. Whether that process is managed and implemented by humans, AI, or a combination of the two, it needs to be designed by someone with a complex enough perspective to ask the right questions. Someone capable of asking the right questions and step back and say, 'What are we really trying to accomplish here? And is there a different way to look at it?' This Self-Assessment empowers people to do just that - whether their title is entrepreneur, manager, consultant, (Vice-)President, CxO etc... - they are the people who rule the future. They are the person who asks the right questions to make Trusted Computer System Evaluation Criteria investments work better. This Trusted Computer System Evaluation Criteria All-Inclusive Self-Assessment enables You to be that person. All the tools you need to an in-depth Trusted Computer System Evaluation Criteria Self-Assessment. Featuring 633 new and updated case-based questions, organized into seven core areas of process design, this Self-Assessment will help you identify areas in which Trusted Computer System Evaluation Criteria improvements can be made. In using the questions you will be better able to: - diagnose Trusted Computer System Evaluation Criteria projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices - implement evidence-based best practice strategies aligned with overall goals - integrate recent advances in Trusted Computer System Evaluation Criteria and process design strategies into practice according to best practice guidelines Using a Self-Assessment tool known as the Trusted Computer System Evaluation Criteria Scorecard, you will develop a clear picture of which Trusted Computer System Evaluation Criteria areas need attention. Your purchase includes access details to the Trusted Computer System Evaluation Criteria self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows your organization exactly what to do next. Your exclusive instant access details can be found in your book.

trusted computer system evaluation criteria: Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria , 1988 This document provides interpretations of the Department of Defense Trusted Computer System Evaluation Criteria (DoD 52O0.28-STD or TCSEC) for computer security subsystems. A computer security subsystem (subsystem) is defined, herein, as hardware, firmware and/or software which can be added to a computer system to enhance the security of the overall system. A subsystem's primary utility is to increase the security of a computer system. The computer system that the subsystem is to protect is referred to as the protected system in this Interpretation. When incorporated into a system environment, evaluated computer security subsystems may be very effective in reducing or eliminating certain types of vulnerabilities whenever entire evaluated systems are unavailable or impractical.

trusted computer system evaluation criteria: Integrity-Oriented Control Objectives: Proposed Revisions to the Trusted Computer System Evaluation Criteria (TCSEC), DoD 5200.28-STD. , 1991 Control objectives, as they apply to automated information systems, express fundamental computer security requirements and serve as guidance to the development of more specific systems evaluation criteria. Within the DoD, the control objectives contained in the Trusted Computer System Evaluation Criteria (TCSEC), DoD 5200.28-STD, are of primary concern to the development of product evaluation criteria. The TCSEC's scope is currently confined to address only confidentiality protection of information. This document is intended to extend the scope of the TCSEC so that the control objectives, contained therin, will also address the protection of information and computing resource integrity. The document provides new and modified statements of control objectives along with discussion and rationale for their inclusion or revision. The revisions were initially determined as a result of an examination of various mechanisms and policy

abstractions that seemed focused on integrity. The revisions were further reinforced by an examination of Federal law and policy. The basis in Federal law and policy for the revised control objectives is discussed. A summary, key text, cross-references, and commentary notes of each law and policy used in the derivation of the revisions are provided. The document is intended to be used as a strawman to foster further debate and research leading to a new standard for evaluation criteria that encompasses both integrity and confidentiality.

trusted computer system evaluation criteria: Trusted Computer System Evaluation Criteria A Complete Guide Gerardus Blokdyk, 2018 Trusted Computer System Evaluation Criteria A Complete Guide.

trusted computer system evaluation criteria: Trusted computer system evaluation criteria United States Department of Defense, 1985

trusted computer system evaluation criteria: Department of Defense Trusted Computer System Evaluation Criteria United States. Department of Defense, 1987

Related to trusted computer system evaluation criteria

Find Your Next Travel Nurse or Allied Health Job | Trusted Health Trusted Health is the easiest, most intuitive way for clinicians to find travel jobs

TRUSTED Definition & Meaning - Merriam-Webster firm belief in the character, ability, strength, or truth of someone or something. : confident hope. : property held or managed by one person or organization (as a bank) for the benefit of another.

TRUSTED | definition in the Cambridge English Dictionary TRUSTED meaning: 1. deserving of trust, or able to be depended on : 2. deserving of trust, or able to be depended. Learn more

TRUSTED definition and meaning | Collins English Dictionary Definition of 'trusted' trusted in British English ('trʌstɪd) adjective regarded as honest and sincere

Trusted - definition of trusted by The Free Dictionary To have or place confidence in; depend on: only trusted his friends; did not trust the strength of the thin rope; could not be trusted to oversee so much money

65 Synonyms & Antonyms for TRUSTED | Find 65 different ways to say TRUSTED, along with antonyms, related words, and example sentences at Thesaurus.com

Trusted - Definition, Meaning & Synonyms | /'trʌsɪd/ /'trʌstɪd/ IPA guide Definitions of trusted adjective (of persons) worthy of trust or confidence synonyms: sure

What does trusted mean? - Trusted refers to someone or something that is believed to be reliable, good, honest, effective, or dependable. It usually implies a sense of confidence, safety and faith based on past

trusted - Dictionary of English to rely upon or place confidence in someone or something (usually fol. by in or to): to trust in another's honesty; trusting to luck. hope: Things work out if one only trusts. to sell merchandise

TRUSTED - Definition & Meaning - Reverso English Dictionary Trusted definition: considered reliable and deserving of trust by others. Check meanings, examples, usage tips, pronunciation, domains, and related words. Discover expressions like

Find Your Next Travel Nurse or Allied Health Job | Trusted Health Trusted Health is the easiest, most intuitive way for clinicians to find travel jobs

TRUSTED Definition & Meaning - Merriam-Webster firm belief in the character, ability, strength, or truth of someone or something. : confident hope. : property held or managed by one person or organization (as a bank) for the benefit of another.

TRUSTED | definition in the Cambridge English Dictionary TRUSTED meaning: 1. deserving of trust, or able to be depended on : 2. deserving of trust, or able to be depended. Learn more

TRUSTED definition and meaning | Collins English Dictionary Definition of 'trusted' trusted in British English ('trʌstɪd) adjective regarded as honest and sincere

Trusted - definition of trusted by The Free Dictionary To have or place confidence in; depend

on: only trusted his friends; did not trust the strength of the thin rope; could not be trusted to oversee so much money

65 Synonyms & Antonyms for TRUSTED | Find 65 different ways to say TRUSTED, along with antonyms, related words, and example sentences at Thesaurus.com

Trusted - Definition, Meaning & Synonyms | /ˈtrʌsɪɪd/ /ˈtrʌstɪd/ IPA guide Definitions of trusted adjective (of persons) worthy of trust or confidence synonyms: sure

What does trusted mean? - Trusted refers to someone or something that is believed to be reliable, good, honest, effective, or dependable. It usually implies a sense of confidence, safety and faith based on past

trusted - Dictionary of English to rely upon or place confidence in someone or something (usually fol. by in or to): to trust in another's honesty; trusting to luck. hope: Things work out if one only trusts. to sell merchandise

TRUSTED - Definition & Meaning - Reverso English Dictionary Trusted definition: considered reliable and deserving of trust by others. Check meanings, examples, usage tips, pronunciation, domains, and related words. Discover expressions like

Find Your Next Travel Nurse or Allied Health Job | Trusted Health Trusted Health is the easiest, most intuitive way for clinicians to find travel jobs

TRUSTED Definition & Meaning - Merriam-Webster firm belief in the character, ability, strength, or truth of someone or something. : confident hope. : property held or managed by one person or organization (as a bank) for the benefit of another.

TRUSTED | definition in the Cambridge English Dictionary TRUSTED meaning: 1. deserving of trust, or able to be depended on : 2. deserving of trust, or able to be depended. Learn more

TRUSTED definition and meaning | Collins English Dictionary Definition of 'trusted' trusted in British English ('trʌstɪd) adjective regarded as honest and sincere

Trusted - definition of trusted by The Free Dictionary To have or place confidence in; depend on: only trusted his friends; did not trust the strength of the thin rope; could not be trusted to oversee so much money

65 Synonyms & Antonyms for TRUSTED | Find 65 different ways to say TRUSTED, along with antonyms, related words, and example sentences at Thesaurus.com

Trusted - Definition, Meaning & Synonyms | /ˈtrʌsɪɪd/ /ˈtrʌstɪd/ IPA guide Definitions of trusted adjective (of persons) worthy of trust or confidence synonyms: sure

What does trusted mean? - Trusted refers to someone or something that is believed to be reliable, good, honest, effective, or dependable. It usually implies a sense of confidence, safety and faith based on past

trusted - Dictionary of English to rely upon or place confidence in someone or something (usually fol. by in or to): to trust in another's honesty; trusting to luck. hope: Things work out if one only trusts. to sell merchandise

TRUSTED - Definition & Meaning - Reverso English Dictionary Trusted definition: considered reliable and deserving of trust by others. Check meanings, examples, usage tips, pronunciation, domains, and related words. Discover expressions like

Find Your Next Travel Nurse or Allied Health Job | Trusted Health Trusted Health is the easiest, most intuitive way for clinicians to find travel jobs

TRUSTED Definition & Meaning - Merriam-Webster firm belief in the character, ability, strength, or truth of someone or something. : confident hope. : property held or managed by one person or organization (as a bank) for the benefit of another.

TRUSTED | definition in the Cambridge English Dictionary TRUSTED meaning: 1. deserving of trust, or able to be depended on : 2. deserving of trust, or able to be depended. Learn more

TRUSTED definition and meaning | Collins English Dictionary Definition of 'trusted' trusted in British English ('trʌstɪd) adjective regarded as honest and sincere

Trusted - definition of trusted by The Free Dictionary To have or place confidence in; depend on: only trusted his friends; did not trust the strength of the thin rope; could not be trusted to

oversee so much money
65 Synonyms & Antonyms for TRUSTED | Find 65 different ways to say TRUSTED, along with antonyms, related words, and example sentences at Thesaurus.com
Trusted - Definition, Meaning & Synonyms | /ˈtrʌsɾɪd/ /ˈtrʌstɪd/ IPA guide Definitions of trusted adjective (of persons) worthy of trust or confidence synonyms: sure
What does trusted mean? - Trusted refers to someone or something that is believed to be reliable, good, honest, effective, or dependable. It usually implies a sense of confidence, safety and faith based on past
trusted - Dictionary of English to rely upon or place confidence in someone or something (usually fol. by in or to): to trust in another's honesty; trusting to luck. hope: Things work out if one only trusts. to sell
TRUSTED - Definition & Meaning - Reverso English Dictionary Trusted definition: considered reliable and deserving of trust by others. Check meanings, examples, usage tips, pronunciation, domains, and related words. Discover expressions like

Related to trusted computer system evaluation criteria

Rainbow Series (PC Magazine6y) The Rainbow Series was a collection of freely distributed documents summarizing recommendations of agencies of the U.S. government. They were published in the 1980s and 1990s by the National Computer
Rainbow Series (PC Magazine6y) The Rainbow Series was a collection of freely distributed documents summarizing recommendations of agencies of the U.S. government. They were published in the 1980s and 1990s by the National Computer
Common Criteria (PC Magazine6y) The Common Criteria for Information Technology Security Evaluation (CC) is part of an international agreement for defining security objectives using agreed-upon terminology, for evaluating compliance
Common Criteria (PC Magazine6y) The Common Criteria for Information Technology Security Evaluation (CC) is part of an international agreement for defining security objectives using agreed-upon terminology, for evaluating compliance

Back to Home: https://lxc.avoiceformen.com