



# SECURITY POSTURE AND FRAMEWORK

Version: 0.20  
Date: 23 March 2001

---

Security Framework (Web)

Copyright © 2000, 2001 Radianz Limited.  
The information contained herein is proprietary to Radianz. Unauthorized use, duplication, or disclosure is strictly prohibited.

---

## TABLE OF CONTENTS

<b>1</b>	<b><i>Introduction</i></b> .....	<b>15</b>
1.1	Audience .....	15
1.2	Overview of Radianz Security .....	15
<b>2</b>	<b><i>Overview of Radianz Products and Services</i></b> .....	<b><i>Error! Bookmark not defined.</i></b>
2.1	RadianzNet.....	<b>Error! Bookmark not defined.</b>
2.2	Radianz Hosting Services .....	<b>Error! Bookmark not defined.</b>
<b>3</b>	<b><i>Security Principles and Posture</i></b> .....	<b><i>Error! Bookmark not defined.</i></b>
3.1	Radianz Security Leadership .....	<b>Error! Bookmark not defined.</b>
3.2	Radianz Impartiality and Neutrality .....	<b>Error! Bookmark not defined.</b>
3.3	Common Carrier .....	<b>Error! Bookmark not defined.</b>
3.4	Decentralized Security Organization .....	<b>Error! Bookmark not defined.</b>
3.5	Comprehensive Security .....	<b>Error! Bookmark not defined.</b>
3.6	Customer Privacy.....	<b>Error! Bookmark not defined.</b>
3.7	Confidentiality .....	<b>Error! Bookmark not defined.</b>
3.8	Least Privilege .....	<b>Error! Bookmark not defined.</b>
3.9	Segregation of Responsibility .....	<b>Error! Bookmark not defined.</b>
3.10	Individual Accountability .....	<b>Error! Bookmark not defined.</b>
3.11	Positive Default Action.....	<b>Error! Bookmark not defined.</b>
3.12	Secure Appearance .....	<b>Error! Bookmark not defined.</b>
3.13	Failsecure .....	<b>Error! Bookmark not defined.</b>
3.14	Minimum Function: Default Deny .....	<b>Error! Bookmark not defined.</b>

---

3.15	Defense in Depth .....	<b>Error! Bookmark not defined.</b>
3.16	Diversity of Defense .....	<b>Error! Bookmark not defined.</b>
3.17	Records of Security Events.....	<b>Error! Bookmark not defined.</b>
3.18	Security Controls .....	<b>Error! Bookmark not defined.</b>
3.19	Audits, Assessments, and Reviews.....	<b>Error! Bookmark not defined.</b>
3.20	Legal and Regulatory Compliance .....	<b>Error! Bookmark not defined.</b>
3.21	Security International Standards.....	<b>Error! Bookmark not defined.</b>
3.22	Continuous Improvement .....	<b>Error! Bookmark not defined.</b>
3.23	Universal Participation .....	<b>Error! Bookmark not defined.</b>
3.24	Risk Management Methodology.....	<b>Error! Bookmark not defined.</b>
3.25	Security Architecture .....	<b>Error! Bookmark not defined.</b>
<b>4</b>	<b><i>Radianz Security Program.....</i></b>	<b><i>Error! Bookmark not defined.</i></b>
4.1	Overview of the Radianz Security Program .....	<b>Error! Bookmark not defined.</b>
4.2	Radianz Security Posture and Framework.....	<b>Error! Bookmark not defined.</b>
4.3	Risk Management Framework.....	<b>Error! Bookmark not defined.</b>
4.4	RadianzNet Security .....	<b>Error! Bookmark not defined.</b>
4.5	Radianz Hosting Security .....	<b>Error! Bookmark not defined.</b>
4.6	Product Security.....	<b>Error! Bookmark not defined.</b>
4.7	Security Operations, Administration, and Management..	<b>Error! Bookmark not defined.</b>
4.8	Security Technical Architecture and Standards.	<b>Error! Bookmark not defined.</b>
4.9	Radianz Products and Services Security Policy	<b>Error! Bookmark not defined.</b>
4.10	Radianz Corporate Security Policy.....	<b>Error! Bookmark not defined.</b>

---

4.11	Personnel Security .....	<b>Error! Bookmark not defined.</b>
4.12	Privacy Policy .....	<b>Error! Bookmark not defined.</b>
4.13	Corporate Information Protection .....	<b>Error! Bookmark not defined.</b>
4.14	Employee Technology Acceptable Use Policy..	<b>Error! Bookmark not defined.</b>
4.15	Radianz Incident Management Capability .....	<b>Error! Bookmark not defined.</b>
4.16	Physical and Facilities Security .....	<b>Error! Bookmark not defined.</b>
4.17	Assessment, Audit, and Review .....	<b>Error! Bookmark not defined.</b>
4.18	Security Information Service .....	<b>Error! Bookmark not defined.</b>
4.19	Security Awareness, Education, and Training...	<b>Error! Bookmark not defined.</b>
4.20	Radianz Security Leadership Initiative.....	<b>Error! Bookmark not defined.</b>
<b>5</b>	<b><i>Radianz Security Organization.....</i></b>	<b><i>Error! Bookmark not defined.</i></b>
5.1	Chief Security Officer.....	<b>Error! Bookmark not defined.</b>
5.2	Corporate Security Group.....	<b>Error! Bookmark not defined.</b>
5.3	Security Operations.....	<b>Error! Bookmark not defined.</b>
5.4	Corporate IT Security .....	<b>Error! Bookmark not defined.</b>
<b>6</b>	<b><i>Risk Management Framework.....</i></b>	<b><i>Error! Bookmark not defined.</i></b>
6.1	Risk and Strategic Planning.....	<b>Error! Bookmark not defined.</b>
6.2	Risk Management Process .....	<b>Error! Bookmark not defined.</b>
6.3	Threat Scenario Planning.....	<b>Error! Bookmark not defined.</b>
<b>7</b>	<b><i>Radianz Security Policy.....</i></b>	<b><i>Error! Bookmark not defined.</i></b>
<b>8</b>	<b><i>Security Awareness, Education, and Training .....</i></b>	<b><i>Error! Bookmark not defined.</i></b>
<b>9</b>	<b><i>Security Operations.....</i></b>	<b><i>Error! Bookmark not defined.</i></b>
9.1	Security Operational Model.....	<b>Error! Bookmark not defined.</b>

---

9.2	Security Administration and Management .....	<b>Error! Bookmark not defined.</b>
9.2.1	Identity .....	<b>Error! Bookmark not defined.</b>
9.2.2	User Accounts.....	<b>Error! Bookmark not defined.</b>
9.2.3	Authenticity and Logon .....	<b>Error! Bookmark not defined.</b>
9.2.4	Authorization, Privileges, and Roles .....	<b>Error! Bookmark not defined.</b>
9.2.5	Privileged Accounts.....	<b>Error! Bookmark not defined.</b>
9.3	Configuration Management .....	<b>Error! Bookmark not defined.</b>
9.4	Change Management .....	<b>Error! Bookmark not defined.</b>
9.5	Continuous Improvement .....	<b>Error! Bookmark not defined.</b>
9.6	Security Event Monitoring and Management....	<b>Error! Bookmark not defined.</b>
9.7	Security Reviews .....	<b>Error! Bookmark not defined.</b>
<b>10</b>	<b><i>Network Security</i></b> .....	<i>Error! Bookmark not defined.</i>
10.1	Router and Firewall Security .....	<b>Error! Bookmark not defined.</b>
10.2	Packet Address Integrity (Antispoofing Controls) .....	<b>Error! Bookmark not defined.</b>
10.3	Network Route Integrity .....	<b>Error! Bookmark not defined.</b>
10.4	Network Secure Appearance .....	<b>Error! Bookmark not defined.</b>
10.4.1	Ping Sweeps.....	<b>Error! Bookmark not defined.</b>
10.4.2	Port Scans. ....	<b>Error! Bookmark not defined.</b>
10.4.3	Internet Control Message Protocol (ICMP).....	<b>Error! Bookmark not defined.</b>
10.4.4	ICMP Queries .....	<b>Error! Bookmark not defined.</b>
10.4.5	ICMP Error Messages.....	<b>Error! Bookmark not defined.</b>

---

10.4.6	Traceroute .....	<b>Error! Bookmark not defined.</b>
10.4.7	Simple Network Management Protocol (SNMP) ....	<b>Error! Bookmark not defined.</b>
10.5	Gateways and Peering .....	<b>Error! Bookmark not defined.</b>
10.5.1	Overview .....	<b>Error! Bookmark not defined.</b>
10.5.2	Gateway Security .....	<b>Error! Bookmark not defined.</b>
10.5.3	External Gateways .....	<b>Error! Bookmark not defined.</b>
10.5.4	Internal Gateways .....	<b>Error! Bookmark not defined.</b>
10.5.5	Internal Peering Points .....	<b>Error! Bookmark not defined.</b>
10.6	Network Component Access Controls .....	<b>Error! Bookmark not defined.</b>
10.8	Domain Name Service .....	<b>Error! Bookmark not defined.</b>
10.9	Remote Access .....	<b>Error! Bookmark not defined.</b>
<b>11</b>	<b><i>RadianzNet Security Architecture</i></b> .....	<b><i>Error! Bookmark not defined.</i></b>
11.1	Overview of RadianzNet Security Architecture	<b>Error! Bookmark not defined.</b>
11.2	RadianzNet Core Autonomous System .....	<b>Error! Bookmark not defined.</b>
11.3	RadianzNet Distribution Autonomous Systems	<b>Error! Bookmark not defined.</b>
11.4	Customer Premises Equipment .....	<b>Error! Bookmark not defined.</b>
11.5	Customer Connections .....	<b>Error! Bookmark not defined.</b>
11.5.1	Overview .....	<b>Error! Bookmark not defined.</b>
11.5.2	Level 1 High Security Customers .....	<b>Error! Bookmark not defined.</b>
11.5.3	Level 2 Medium Security Customers .....	<b>Error! Bookmark not defined.</b>
11.5.4	Level 3 Indeterminate Security Customers	<b>Error! Bookmark not defined.</b>

---

11.6	RadianzNet Autonomous System Interconnect LANs ....	<b>Error! Bookmark not defined.</b>
11.7	RadianzNet Network Component Access Controls.....	<b>Error! Bookmark not defined.</b>
11.8	RadianzNet Routing Information Integrity and Authenticity .	<b>Error! Bookmark not defined.</b>
11.10	RadianzNet Network Time Protocol.....	<b>Error! Bookmark not defined.</b>
<b>12</b>	<b><i>System Security</i></b> .....	<i>Error! Bookmark not defined.</i>
12.1	System Risk Categories .....	<b>Error! Bookmark not defined.</b>
12.2	System Access .....	<b>Error! Bookmark not defined.</b>
12.2.1	Access Authority.....	<b>Error! Bookmark not defined.</b>
12.2.2	User Accounts.....	<b>Error! Bookmark not defined.</b>
12.2.3	User Authentication and Login.....	<b>Error! Bookmark not defined.</b>
12.2.4	Passwords and Personal Identification Numbers.....	<b>Error! Bookmark not defined.</b>
12.2.5	Privileged Access.....	<b>Error! Bookmark not defined.</b>
12.2.6	Console Access.....	<b>Error! Bookmark not defined.</b>
12.2.7	Physical Access.....	<b>Error! Bookmark not defined.</b>
12.2.8	Remote Access.....	<b>Error! Bookmark not defined.</b>
12.2.9	Application Processes .....	<b>Error! Bookmark not defined.</b>
12.2.10	System Access Auditing .....	<b>Error! Bookmark not defined.</b>
12.3	Filesystem Access.....	<b>Error! Bookmark not defined.</b>
12.3.1	System Directories .....	<b>Error! Bookmark not defined.</b>
12.3.2	System Executables .....	<b>Error! Bookmark not defined.</b>

---

12.3.3	System Configuration Files .....	<b>Error! Bookmark not defined.</b>
12.3.4	System Device Files.....	<b>Error! Bookmark not defined.</b>
12.3.5	User Files and Directories.....	<b>Error! Bookmark not defined.</b>
12.3.6	Application Files and Directories .....	<b>Error! Bookmark not defined.</b>
12.3.7	Account Initialization Files and Scripts.....	<b>Error! Bookmark not defined.</b>
12.3.8	Executable File Search Path Environmental Variable ....	<b>Error! Bookmark not defined.</b>
12.4	Network Access .....	<b>Error! Bookmark not defined.</b>
12.4.1	Network Segmentation .....	<b>Error! Bookmark not defined.</b>
12.4.2	Network Services.....	<b>Error! Bookmark not defined.</b>
12.4.3	File Transfer Protocol (FTP).....	<b>Error! Bookmark not defined.</b>
12.4.4	Electronic Mail .....	<b>Error! Bookmark not defined.</b>
12.5	System Integrity.....	<b>Error! Bookmark not defined.</b>
12.5.1	System Change Management.....	<b>Error! Bookmark not defined.</b>
12.5.2	System Configuration Management .....	<b>Error! Bookmark not defined.</b>
12.5.3	Executable Files and Libraries.....	<b>Error! Bookmark not defined.</b>
12.6	System Monitoring and Auditing .....	<b>Error! Bookmark not defined.</b>
12.6.1	System Monitoring and Host Intrusion Detection ...	<b>Error! Bookmark not defined.</b>
12.6.2	System Integrity Auditing.....	<b>Error! Bookmark not defined.</b>
<b>13</b>	<b><i>Physical Security</i></b> .....	<i>Error! Bookmark not defined.</i>
<b>14</b>	<b><i>Threats and Countermeasures</i></b> .....	<i>Error! Bookmark not defined.</i>
14.1	Prevention of Distributed Denial of Service Attacks.....	<b>Error! Bookmark not defined.</b>

---

---

<b>15</b>	<b><i>Security Assessment, Audit, Review, and Monitoring.....</i></b>	<b><i>Error! Bookmark not defined.</i></b>
15.1	Monitoring and Assessing Radianz Security .....	<b>Error! Bookmark not defined.</b>
15.2	Security Assessment, Audit, and Review .....	<b>Error! Bookmark not defined.</b>
15.3	Security Audit Logging Service .....	<b>Error! Bookmark not defined.</b>
15.5	Network Intrusion Detection .....	<b>Error! Bookmark not defined.</b>
15.5.1	Network Intrusion Detection Scope and Objectives	<b>Error! Bookmark not defined.</b>
15.5.2	Network Intrusion Detection Operations and Architecture .....	<b>Error! Bookmark not defined.</b>
15.5.3	Network Intrusion Detection Audit and Detection Policy .....	<b>Error! Bookmark not defined.</b>
15.6	Host Intrusion Detection.....	<b>Error! Bookmark not defined.</b>
15.6.1	Host Intrusion Detection Scope and Objectives .....	<b>Error! Bookmark not defined.</b>
15.6.2	Host Intrusion Detection Operations and Architecture...	<b>Error! Bookmark not defined.</b>
15.6.3	Host Monitoring Audit and Detection Policy .....	<b>Error! Bookmark not defined.</b>
15.7	System Integrity Auditing.....	<b>Error! Bookmark not defined.</b>
15.7.1	System Integrity Audit Scope and Objectives .....	<b>Error! Bookmark not defined.</b>
15.7.2	System Integrity Auditing Operations .....	<b>Error! Bookmark not defined.</b>
<b>16</b>	<b><i>Incident Response and Management.....</i></b>	<b><i>Error! Bookmark not defined.</i></b>
16.1	Incident Management Constituencies .....	<b>Error! Bookmark not defined.</b>
16.2	Radianz Incident Management Organization ....	<b>Error! Bookmark not defined.</b>

---

---

16.3	Incident Classification .....	<b>Error! Bookmark not defined.</b>
16.3.1	Level 0 Indications.....	<b>Error! Bookmark not defined.</b>
16.3.2	Level 1 Notifiable Incidents .....	<b>Error! Bookmark not defined.</b>
16.3.3	Level 2 Monitored Incidents.....	<b>Error! Bookmark not defined.</b>
16.3.4	Level 3 Managed Incidents.....	<b>Error! Bookmark not defined.</b>
16.3.5	Level 4 Major Incidents .....	<b>Error! Bookmark not defined.</b>
16.4	Incident Governance .....	<b>Error! Bookmark not defined.</b>
16.5	Incident Management Process .....	<b>Error! Bookmark not defined.</b>
16.6	Incident Reporting .....	<b>Error! Bookmark not defined.</b>
<b>17</b>	<b><i>Radianz Security Information Service.....</i></b>	<b><i>Error! Bookmark not defined.</i></b>
17.1	Overview of Radianz Security Information Service.....	<b>Error! Bookmark not defined.</b>
17.2	Processes Using the Radianz Security Information Service...	<b>Error! Bookmark not defined.</b>
17.3	Security Information Consumers .....	<b>Error! Bookmark not defined.</b>
17.4	Security Intelligence Sources.....	<b>Error! Bookmark not defined.</b>
17.5	Security Information Publication.....	<b>Error! Bookmark not defined.</b>
<b>18</b>	<b><i>Radianz Security Leadership Initiative.....</i></b>	<b><i>Error! Bookmark not defined.</i></b>
18.1	Customer Security Advisory Council.....	<b>Error! Bookmark not defined.</b>
18.1.1	Purpose.....	<b>Error! Bookmark not defined.</b>
18.1.2	Membership and Organization.....	<b>Error! Bookmark not defined.</b>
18.1.3	Governance .....	<b>Error! Bookmark not defined.</b>
18.1.4	Meeting Schedule: .....	<b>Error! Bookmark not defined.</b>

---

18.1.5	Compensation of SAC members.....	<b>Error! Bookmark not defined.</b>
<b>19</b>	<b><i>Customer Demarcation and Terms of Engagement</i></b>	<b><i>Error! Bookmark not defined.</i></b>
19.1	Overview of Customer Demarcation .....	<b>Error! Bookmark not defined.</b>
19.2	Dimensions of Customer Demarcation.....	<b>Error! Bookmark not defined.</b>
19.3	Terms of Engagement with Radianz Customers	<b>Error! Bookmark not defined.</b>
19.4	Standard Customer Demarcation Configurations .....	<b>Error! Bookmark not defined.</b>
19.5	Establishing and Provisioning the Customer Demarcation ....	<b>Error! Bookmark not defined.</b>
19.6	Operating and Maintaining the Customer Demarcation ..	<b>Error! Bookmark not defined.</b>
19.7	Customer Acceptable Use Policy .....	<b>Error! Bookmark not defined.</b>

## FIGURES

Threat Scenario Planning .....	<b>Error! Bookmark not defined.</b>
Radianz Security Operations Org Chart .....	<b>Error! Bookmark not defined.</b>
Radianz Change Management .....	<b>Error! Bookmark not defined.</b>
Security Event Monitoring.....	<b>Error! Bookmark not defined.</b>
Radianz Security Span of Control.....	<b>Error! Bookmark not defined.</b>
RadianzNet Core Autonomous System .....	<b>Error! Bookmark not defined.</b>
RadianzNet Core Network.....	<b>Error! Bookmark not defined.</b>
RadianzNet Core Logical Topology .....	<b>Error! Bookmark not defined.</b>
RadianzNet Core.....	<b>Error! Bookmark not defined.</b>

RadianzNet Core and Distribution Network.....	<b>Error! Bookmark not defined.</b>
RXN Core Distribution.....	<b>Error! Bookmark not defined.</b>
RXN NTP Hierarchical Model .....	<b>Error! Bookmark not defined.</b>
Corporate Incident Management Capability.....	<b>Error! Bookmark not defined.</b>

---

## T A B L E S

Radianz Sample Courses.....	<b>Error! Bookmark not defined.</b>
Security Roles and Responsibilities.....	<b>Error! Bookmark not defined.</b>
Table of Security Reviews .....	<b>Error! Bookmark not defined.</b>
ICMP Query Table.....	<b>Error! Bookmark not defined.</b>
List of SNMP Community Prohibited Names .....	<b>Error! Bookmark not defined.</b>
Mandatory Gateway Types.....	<b>Error! Bookmark not defined.</b>
Gateway Security Requirements.....	<b>Error! Bookmark not defined.</b>
Customer Connection Trust Levels .....	<b>Error! Bookmark not defined.</b>
Service Package Security Requirements.....	<b>Error! Bookmark not defined.</b>
Risk Categories .....	<b>Error! Bookmark not defined.</b>
Minimum <i>setuid</i> and <i>setgid</i> Executable File Permissions .....	<b>Error! Bookmark not defined.</b>
System Directory Permissions .....	<b>Error! Bookmark not defined.</b>
Public Binary Executable File Permissions .....	<b>Error! Bookmark not defined.</b>
Administrative Binary Executable File Permissions .....	<b>Error! Bookmark not defined.</b>
Public Script Executable File Permissions .....	<b>Error! Bookmark not defined.</b>
Administrative Script Executable File Permissions.....	<b>Error! Bookmark not defined.</b>
System Configuration File Permissions.....	<b>Error! Bookmark not defined.</b>
System Device Files.....	<b>Error! Bookmark not defined.</b>
Disk, Tape, Network, and Memory Device File Permissions.....	<b>Error! Bookmark not defined.</b>
Terminal Device File Permissions .....	<b>Error! Bookmark not defined.</b>

---

Null Device File Permissions.....	<b>Error! Bookmark not defined.</b>
User Directory Permissions .....	<b>Error! Bookmark not defined.</b>
User Binary Executable File Permissions.....	<b>Error! Bookmark not defined.</b>
User Script Executable File Permissions .....	<b>Error! Bookmark not defined.</b>
Application Root and Executable Directory Permissions..	<b>Error! Bookmark not defined.</b>
Application Home Directory Permissions .....	<b>Error! Bookmark not defined.</b>
Application Binary Executable File Permissions .....	<b>Error! Bookmark not defined.</b>
Application Script Executable File Permissions.....	<b>Error! Bookmark not defined.</b>
Application Configuration File Permissions.....	<b>Error! Bookmark not defined.</b>
Account Initialization File Permissions .....	<b>Error! Bookmark not defined.</b>
Network Services Policy.....	<b>Error! Bookmark not defined.</b>
SMTP Packet Filtering Characteristics.....	<b>Error! Bookmark not defined.</b>
POP Packet Filtering Characteristics .....	<b>Error! Bookmark not defined.</b>
Network Denial-of-Service Attack Trait .....	<b>Error! Bookmark not defined.</b>
Safeguard and Summary Radianz Policy.....	<b>Error! Bookmark not defined.</b>
Radianz Security Methods .....	<b>Error! Bookmark not defined.</b>
Audit/Review Schedule .....	<b>Error! Bookmark not defined.</b>
Security Event Record Contents .....	<b>Error! Bookmark not defined.</b>
List of Events or Attacks.....	<b>Error! Bookmark not defined.</b>
System Risk Alarms.....	<b>Error! Bookmark not defined.</b>
Radianz Host Detection Intrusion Capability .....	<b>Error! Bookmark not defined.</b>
Radianz System Integrity Audit Policy.....	<b>Error! Bookmark not defined.</b>

---

Security Incident Governance.....**Error! Bookmark not defined.**

Incident Reporting .....**Error! Bookmark not defined.**

## **1 Introduction**

This document describes the Radianz posture, strategy, and framework for providing secure products and services. These include:

- RadianzNet;
- Radianz Hosting;
- Radianz products, such as real-time messaging, electronic mail, public key infrastructure, instant messaging, secure document transfer, managed firewalls, and virtual private networks; and
- supporting infrastructure, including operational support and management systems, billing support systems, network services, physical facilities, and customer service.

### **1.1 Audience**

This document is intended for both Radianz and its customers and prospects:

- This document provides Radianz customers and prospects a means to evaluate the security of Radianz products and services.
- For Radianz employees, this document specifies Radianz's strategy and approach for providing secure products and services.

### **1.2 Overview of Radianz Security**

Radianz offers a highly reliable, secure community of interest network over which members of the global financial community may conduct their business safely, reliably, and effectively.

Security is intrinsic to the Radianz brand. Security is the single major concern of Radianz customers, thus a major part of our value to them. Customers entrust to us their critical business transactions, delivery of their products, and a considerable portion of their sensitive information assets. Security is a fundamental business enabler and differentiator for Radianz.

***Security is Radianz's single most important differentiator.***

***150 Pages' Content Removed  
at Client's Request  
(Confidential Material)***

## GLOSSARY

**Access control** limiting use of some resource to authorized users.

**Access control list** a data entity associated with a resource that specifies the authorized users.

**Access control set** synonym for Access Control List; there may be some distinctions of significance between the two.

**Accountability** enables the reconstructing of events on a computer system or network. It allows a system or network administrator to follow the actual steps that occurred in a security incident and detect the individuals responsible.

**Administrator account** a default account on a Windows NT system that has high-level privileges.

**ANSI** a standards organization that issues standards for computer networking.

**Application gateway** a type of firewall that bases access decisions on the nature of the application's communication.

**Asymmetric cryptography** public key cryptography.

**Audit** to record events that might have security significance – for example, when access to resources occurred.

**Audit ID** an ID, used in constructing an audit trail, that is associated with each user.

**Authenticate** a determination of whether information is genuine or not.

**Authentication** reliably determining the identity of a communicating party.

**Authorization** permission to access a resource.

**Awareness** (in security) the knowledge in the user community about the importance of information security.

**Background authentication** automatic authentication when a user requests a service without the user having to do anything.

**Batch job** a procedure run on behalf of a particular user -- while the user need not be physically present at any terminal and no terminal is associated with the process.

**Block encryption** reversibly scrambling a fixed-size piece of data into a fixed size piece of cipher text.

**Call back** a security mechanism for dial-in connections to a network -- a user calls in, requests a connection, and hangs up. The system then calls him back and thus reliably knows the telephone number of the caller.

**Captive account** an account on a timesharing system that allows someone who uses that account to run only a single program which carefully controls access to system resources.

**Certificate** a message signed with a public key digital signature stating that a specified public key belongs to someone or something with a specified name.

**Certification authority (CA)** some entity trusted to sign certificates.

**Certification revocation list (CRL)** a digitally signed data structure listing all the certificates created by a given CA that have not yet expired but are no longer valid.

**Challenge** a number given to something so that it can cryptographically process the number using a secret quantity it knows and return the result (called the response). The purpose of the exercise is to prove knowledge of the secret quantity without revealing to an eavesdropper. This is known as challenge/response authentication.

**Change management** A defined process for the orderly management of change from one defined state to another.

**Checksum** a small, fixed-length quantity computed as a function of an arbitrary length message. It's computed by the sender of a message and recomputed and checked by the recipient of a message to detect data corruption.

**Chroot** a UNIX system call that allows the system administrator to change a particular directory to the root directory for a user (effectively limiting the user's ability to traverse the UNIX file system).

**Client** something that accesses a service by communicating with it over a computer network.

**Compromise** to invade by getting around its security.

**Confidentiality** the practice of preventing information from being divulged to unauthorized parties.

**Credential(s)** secret information used to prove one's identity in an authentication exchange.

**Data classification** the labeling of information according to its sensitivity.

**Data custodian** a trustee who has been given responsibility for the protection of a corporate information resource.

**Data encryption** protecting information by scrambling information that can only be unscrambled by the use of a special key.

**Data guardian** the person responsible for the protection of a corporate information resource.

**Data owner** the individual who has created or been given ownership of an information resource.

**Decipher** to decrypt.

**Decrypt** to reverse the encryption process.

**Delegation** giving some of your rights to another person or process.

**Denial of Service** an attack that attempts to deny corporate computing resources to legitimate users.

**Directory service** a service provided on a computer network that allows one to look up addresses (and perhaps other information) based on names.

**DNS** (Domain Name Service) the naming convention defined in RFC 1033. DNS names are often referred to as "internet addresses" or "internet names."

**DSS** (Digital Signature Standard) a public key cryptographic system of computing digital signatures.

**EDE** (encrypt/decrypt/encrypt) a method of making a secret key scheme more secure using multiple keys.

**Encrypt** scrambling information so that only someone knowing the appropriate secret can obtain the original information (through decryption).

**Escrow** to hold something in safe-keeping. Most uses of the word actually mean keeping the something safe from the owner as opposed to providing any safety for the owner.

**File access permissions** a set of flags that are used to determine whether or not to grant access to a file or directory.

**Filtering router** a router capable of performing packet filtering.

**Firewall** a computer system or network device that limits traffic between a trusted and untrusted network.

**Hash** a cryptographic one-way function that takes an arbitrary-sized input and yields a fixed-size output.

**Integrity** can also be called “correctness.” A system protects the integrity of data if it prevents unauthorized modification (as opposed to protecting the confidentiality of data, which prevents unauthorized disclosure).

**Integrity checks** a utility or task that reviews a computing environment for unauthorized modifications.

**Intermediary** something that facilitates communication between parties that wish to communicate.

**IP forwarding attack** a hacking technique used to attempt to pass TCP/IP packets to a protected network.

**ISO (International Standards Organization)** an international organization tasked with developing and publishing standards for everything from wine glasses to computer network protocols.

**Key** a quantity used in cryptography to encrypt or decrypt information.

**LAN (LAN)** a method of interconnecting multiple systems in such a way that all transmissions over the LAN can be listened to by all systems on the LAN.

**Mandatory access codes** an access control mechanism where the owner of data does not have full control over who may access the data.

**Masquerade (also “Spoof”)** to pretend to be “X” when you are not “X,” without “X’s” permission.

**Mutual authentication** when each party in a conversation proves its identity to the other.

**Overrun** when a network is taken over by a “bad guy.”

**Packet filtering** the limiting of TCP/IP traffic, based upon the type of traffic, source and destination IP addresses, ports or other information.

**Password cracking** a method seeking to discover passwords by passing a dictionary of terms through a password algorithm to compare the output to the encrypted password string.

**PIN (Personal Identification Number)** a short sequence of digits used as a password.

**Preauthentication** a protocol for proving you know your password before you are allowed access to a high quality secret encrypted with that password.

**Privacy** protection from the unauthorized disclosure of data.

**Private key** the quantity in public key cryptography that must be kept secret.

**Privileged user** a user of a computer who is authorized to bypass normal access control mechanisms, usually to be able to perform system management functions.

**Public key** the quantity in public key cryptography that is safely divulged to as large an extent as necessary or convenient.

**Public key cryptography** also known as asymmetric cryptography, a cryptographic system where encryption and decryption are performed using different keys.

**Revocation** taking back privileges, for example, as when an employee leaves a company.

**Risk analysis** the balancing of the exposure (risk) with the probability that it will occur.

**Risk assessment** sometimes called risk analysis – the analysis of controls (specifically their effectiveness).

**Routing attack** a hacking method that uses the IP source routing option to route packages to a destination where they can be manipulated.

**SSL** secure socket layer. Used for authentication and encryption between a client and a server.

**Secret key** the shared secret quantity in secret key cryptography that is used to encrypt and decrypt data.

**Secret key cryptography** also known as symmetric cryptography, a scheme in which the same key is used for encryption and decryption.

**Self assessment** an audit performed by a system administrator, user department or any group that is not independent. Often performed in anticipation of an audit.

**Sign** to use your private key to generate a digital signature as a means of proving you generated, or approve of, some message.

**Signature** a quantity associated with a message which only someone with knowledge of your private key could have generated, but which can be verified through knowledge of your public key.

**Simple Mail Transport Protocol (SMTP)** a protocol for sending electronic mail across a network, standardized by the IETF.

**Simple Network Management Protocol (SNMP)** a protocol for controlling systems across a network, standardized by the IETF.

**Spoof** (also masquerade) to pretend to be “X” when you are not “X,” without “X’s” permission.

**Strong authentication** authentication where someone eavesdropping on the authentication exchange does not gain sufficient information to impersonate the principal in a subsequent authentication.

**Superuser** an operating system concept in which an individual is allowed to circumvent ordinary security mechanisms. For instance, the system manager must be able to read everyone’s files for the purpose of doing backups.

**TCP/IP** a family of networking protocols and services based on IP (internet protocol).

**Token based authentication** authentication that is provided by the possession of a unique physical card or device that supplies one component of the authentication process.

**Trojan horse** a piece of code embedded in a useful program for nefarious purposes, for instance to steal information. Usually the term Trojan horse is used rather than virus when the offending code does not attempt to replicate itself into other programs.

**Trusted intermediary** a third party such as a KDC or CA that permits two parties to authenticate without prior configuration of keys between those two parties.

**Trusted server** something that aids in network authentication.

**Verify a signature** perform a cryptographic calculation using a message, a signature, and a public key to determine whether the signature was generated by someone knowing the corresponding private key signing the message.

**Virus** a piece of a computer program that replicates by embedding itself in other programs. When those programs are run, the virus is invoked again and can spread further.

**VPN** virtual private network. A technique that encrypts and protects traffic between two trusted networks.

**Worm** a self-contained program that replicates by running copies of itself – usually on different machines across a computer network.

## INDEX

Antispoofing Controls .....	59
ASIL .....	See Autonomous System Interconnect LANs
Audit and Accountability .....	59
Audits, Assessments and Reviews .....	25
and Regular Security Audits .....	121
and Thirdy Party Audits .....	25, 121
Authenticity and Logon .....	44
Authorization and Access control .....	36
Autonomous System Interconnect LANs .....	77, 84
British Standard BS7799 .....	36
Change Management	
approval .....	51
assess risk .....	49
change management group .....	51
change reviews .....	51
classification .....	51
customers .....	51
deployment .....	50
documenting .....	51
expedited changes .....	52
failure .....	50
final approval .....	50
identify need .....	48
initial approval .....	49

---

major changes.....	51
Operational Support Systems (OSS) .....	51
preapproval process.....	51
prior notification .....	51
propose change .....	49
recovery plan.....	51
records .....	51
review.....	50
rollback plan .....	51
scheduled changes .....	51
testing.....	50
unacceptable risk .....	51
Chief Security Officer .....	32
Command Line Programs .....	93
Common Carrier .....	21
Comprehensive Security .....	22
CONFIDENTIAL status .....	44
Configuration Management Group.....	49
Configuration Updates .....	59, 84
Console Access .....	93
Continous Improvement	
alerts and advisories .....	52
continous training .....	53
Radianz as leader .....	52
schedule of security reviews .....	53

---

---

vulnerabilities, sources of.....	52
Continuous Improvement.....	26, 52
opportunities for .....	53
Corporate Information Protection.....	29, 38
Corporate Security Group .....	32, 48
Customer	
confidentiality .....	22
privacy.....	22
<b>Customer Acceptable Use Policy.....</b>	<b>37</b>
chief characteristics of.....	157
examples of .....	156
purposes of .....	156
rights conferred to Radianz therein .....	157
Customer Connections .....	81
and Levels of Trust.....	81
and ways to connect .....	81
Level 1 High Security .....	82
Level 2 Medium Security.....	83
Level 3 Indeterminate Security.....	83
overview.....	81
Customer Contracts, Order Forms, and Service Level Agreements .....	37
Customer Demarcation .....	154
customer acceptable use policy .....	156
dimensions of customer demarcation.....	155
establishing and provisioning .....	156

---

---

operating and maintaining .....	156
overview .....	154
standard customer demarcation configurations.....	156
terms of engagement with radianz customers.....	155
Customer Management .....	38
Customer Premises Equipment .....	80
and Radianz Products and Services Security Policy .....	80
Customer Security Advisory Council	
membership and organization .....	153
Customer Service .....	39
Decentralized Security Organization.....	22
Defense in Depth .....	25
Director of Global Operations.....	42
Diversity of Defense.....	25
DNS .....	See Domain Name Service
Domain Name Service	
and administrative access .....	73
and dnssec.....	73
and modifications .....	73
and risk.....	73
DNS zone transfers .....	73
Dual Authorization.....	47
Echo Reply Packets.....	59
Electronic Mail .....	107
Employee Acceptable Use Policy .....	29, 37

---

Encryption	
account or user-identifiers .....	45
personal identifiers .....	45
single use or one-time passwords .....	45
static passwords.....	45
External Gateways	
and BGP Communities.....	71
and Layer 2 Bridging Firewall.....	71
and Two Tiers of Controls .....	71
Failed Login Attempts .....	46
Failsecure .....	24
Filesystem Access .....	95
account initialization files and scripts .....	104
application files and directories .....	100
executable file search path environmental variable.....	104
system configuration files.....	97
system device files .....	98
system directories .....	95
system executables.....	96
user files and directories .....	99
Five-Phase Risk Management Framework	
accept.....	33
assign.....	33
mitigate.....	33
Gateways	

---

external gateways .....	69
and minimum security requirements for .....	71
as high risk resources .....	71
GSO .....	42
Hackers.....	52
HOC's .....	40
Host Intrusion Detection	
for high and medium risk systems.....	130
host intrusion detection operations and architecture .....	130
host monitoring audit and detection policy .....	132
scope and objectives.....	130
Host Intrusion Detection Scope and Objectives	
types and sensitivity of .....	131
Host Monitoring Audit and Detection Policy	
list of events recorded .....	132
ICMP	
detection.....	66, 67
error messages .....	67
prevention .....	66, 67
queries .....	65
traffic .....	59
Identity .....	44
Identity And Authenticity .....	36
Impartiality and Neutrality.....	21
Incident Classification	

---

criteria of levels .....	142
levels of .....	142
Incident Management Process	
and indications .....	149
and Level 1 NOC .....	149
and monitored .....	150
and notifiables .....	149
Level 2 OSS .....	149
managed or major .....	150
Incident Reporting	
and centralized reporting .....	150
as generated by .....	150
Incident Response and Management .....	137
incident classification .....	142
incident governance .....	148
incident management process .....	148
incident reporting .....	150
level 0 indications .....	143
level 1 notifiable incidents .....	144
level 2 monitored incidents .....	145
level 3 managed incidents .....	146
level 4 major incidents .....	147
managing the life cycle of .....	137
incident management capability .....	138
incident management constituencies .....	140

---

---

incident management organization .....	140
Individual Accountability.....	23
Industry Best Practice .....	36
Intelligence.....	48
Internal Gateways .....	71
examples of.....	71
security controls .....	71
Internal Peering Points.....	72
security controls .....	72
Internet Control Message Protocol (ICMP) .....	64
Least Privilege .....	23
Legal and Regulatory Compliance .....	25
Level 1 Network Operators .....	41
Level 1 Notifiable Incidents .....	144
Level 2 Monitored Incidents .....	145
Level 2 Operational Security Manager (OSM) .....	55
Level 2 Operational Security Specialist (OSS).....	41
Level 3 Managed Incidents .....	146
List Of Events And Attacks.....	129
Manager of Global Security Operations .....	42, 48
Metrics .....	35
Minimum Function Default Deny .....	25
Monitoring And Auditing.....	36
Most Recent Activity .....	45
Network Access .....	104

---

---

electronic mail .....	107
file transfer protocol (ftp) .....	106
network segmentation .....	104
network services .....	106
Network and System Security Management .....	39
Network and System Security Practice .....	39
Network Engineering .....	48
Network Intrusion Detection	
audit and detection policy .....	128
list of events and attacks .....	129
maintaining disparate risk profiles .....	127
monitoring of .....	127
operations and architecture .....	128
scope and objectives .....	127
Network Management Console .....	55
and Level 1 Network Operator .....	55
and Level 2 Operational Security Manager .....	55
Network Operations .....	48
Network Operator .....	43
Network Risk Boundaries .....	59
Network Routers	
and customer sites .....	62
third party sources .....	62
unknown sources .....	62
Network Secure Appearance .....	63

---

---

attackers.....	63
detection.....	63
prevention .....	63
Network Security	
and ICMP queries .....	65
and reverse path forwarding.....	61
and TACACS+.....	60
antispoofing controls .....	61
controls.....	59
encryption.....	60
external gateways .....	71
gateway security .....	70
gateways and peering .....	68
internal gateways .....	69, 71
internal peering points.....	69, 72
network component access controls .....	72
network router integrity.....	62
network secure appearance .....	63
packet address integrity .....	61
passwords .....	60
port scans.....	64
remote access.....	73
router security controls .....	60
routers and firewalls .....	59
single network management protocol (SNMP).....	68

---

---

tracertool .....	67
Network Segmentation	
by risk profile .....	104
other measures .....	105
Network Services	
Radianz policy governing .....	106
New Employee Security Orientation .....	
and employee acceptable use policy .....	37
regular security awareness training .....	37
security orientation course .....	37
Operating System Shells .....	93
Operational Security Managers .....	43
Operational Security Specialists .....	43
Operations Security Manager .....	42, 46
Operations Security Specialist .....	41, 46-47
Overview of the Radianz Security Program	
information security .....	27
network security .....	27
physical security .....	27
product security .....	27
risk management .....	27
Passwords .....	36
Personnel Security .....	29
Physical And Facilities Security .....	30
Physical Security .....	110

---

---

five fundamental elements of .....	110
four level hierarchy of .....	111
objectives of operations and technical center .....	111
personnel identification system .....	112
specifications .....	111
visitor registration and temporary pass system .....	112-113
Ping Sweeps .....	63
detection .....	63
prevention .....	63
Port Scans .....	64
detection .....	64
prevention .....	64
Positive Default Action .....	24
Prevention of Distributed Denial of Service Attacks	
and attacker opportunities .....	113
approaches and mechanisms .....	114
safeguards and summaries .....	115
traits and postures .....	114
Privacy And Confidentiality .....	36
Privacy Policy .....	29, 37
Privileged Access	
and audits .....	93
and root commands .....	93
Product Security .....	28
Product Technology .....	48

---

---

Prosecution For Unauthorized Use .....	45
Public Database Security .....	36
Radianz Change Management Process .....	46-48
Radianz Corporate Development and security training courses.....	38
Radianz Corporate Security Policy .....	29, 36
Radianz Hosting Services	
Basic Hosting .....	19
Enhanced Hosting .....	20
Next Generation Hosting.....	20
Radianz Incident Management Organization	
and functional incident management cells.....	141
federal nature of .....	140
governance of accidents .....	141
Radianz Individual Product Security Policies .....	37
Radianz Operational Support Systems (OSS) and change management.....	51
Radianz Products and Services Security Policy.....	29, 36, 48
Radianz Security	
overview .....	18
security information service.....	151
overview .....	151
processes using.....	152
security information consumers.....	152
security information publication .....	153

---

---

security intelligence sources .....	152
Radianz Security Leadership Initiative .....	31, 153
compensation of sac members .....	154
customer security advisory council .....	153
governance .....	154
government initiatives .....	154
government initiatives .....	154
industry initiatives .....	154
meeting schedule .....	154
purpose .....	153
standards bodies .....	154
Radianz Security Operations	
roles and responsibilities .....	43
Radianz Security Policy .....	35
Radianz Security Posture and Framework .....	28
Radianz Security Program .....	27
overview .....	27
RadianzNet	
access customers .....	19
agent customers .....	19
broadcast customers .....	19
hosting customers .....	19
publishing customers .....	19
RadianzNet Core Autonomous System	
as open transit network .....	77

---

locations of .....	76
RadianzNet Distribution AS	
and routers .....	79
RadianzNet Distribution AS routers	
configurations .....	78
RadianzNet Network Component Access Controls .....	84
RadianzNet Network Time Protocol .....	86
RadianzNet Routing Information Integrity and Authenticity .....	85
RadianzNet Security .....	28
RadianzNet Security Architecture .....	75
autonomous system interconnect lans .....	84
core autonomous system .....	76
customer connections .....	81
customer premises equipment .....	80
distribution autonomous systems .....	77
overview .....	75
network component access controls .....	84
network time protocol .....	86
security monitoring and intrusion detection .....	86
RadianzNet Security Monitoring and Intrusion Detection .....	86
Records of Security Events .....	25
secure log .....	25
Remote Access	
and audits .....	74
and authorizations .....	74

---

---

as high risk resources .....	74
restrictions to .....	74
secure appearance of .....	75
Risk and Strategic Planning .....	32
Risk Management Framework .....	28, 32
Risk Management Methodology.....	26
five phase risk management framework.....	33
risk designations .....	26
threat scenario planning .....	33
Risk Measurement Proxies .....	35
Root User .....	See Superuser
Schedule of Operations Security Reviews	
annual .....	58
daily.....	58
monthly.....	58
quarterly .....	58
weekly .....	58
Secure Appearance .....	24
publicly available information .....	24
Secure Shell.....	See SSH
Security Administration And Management .....	44
Security Alerts.....	48
Security Architecture.....	27
Security Assessment, Audit, Review, And Monitoring.....	117
host intrusion detection .....	130

---

---

monitoring and assessing radianz security.....	117
network intrusion detection.....	127
physical intrusion detection .....	127
physical monitoring architecture.....	127
physical monitoring audit and detection policy .....	127
physical monitoring operations.....	127
physical monitoring scope and objectives .....	127
schedule of audits .....	121
security assessment, audit, and review.....	121
security audit logging service .....	125
summary of methods.....	118
<b>Security Audit Logging Service</b>	
and compliance with Radianz policy .....	126
as contained in logs .....	127
contained in logs .....	127
maintenance of.....	125
performance of .....	125
<b>Security Awareness, Education, and Training.....</b>	<b>30, 37</b>
continuous development and improvement.....	37
new employees .....	37
<b>Security Controls.....</b>	<b>25</b>
<b>Security Event Monitoring and Management .....</b>	<b>54</b>
and basic investigation .....	55
and security management consoles.....	54
corporate incident response team .....	55

---

generating, monitoring, detecting .....	54
incident .....	55
indication .....	55
Level 2 Operational Security Manager (OSM).....	55
major .....	55
managed .....	55
monitored .....	55
notifiable.....	55
pattern of events .....	55
security event .....	55
Security Events .....	55
Security Incident Management.....	36
Security Information Service .....	30
Security International Standards .....	26
Security Leadership .....	21
Security Operational Model	
HOC's.....	40
NOC's .....	41
Security Operations .....	32
Security Operations, Administration, And Management.....	28
Security Perimeters.....	59
Security Processes, Procedures, And Standards .....	See
Security Reviews .....	56
purposes .....	57
schedule.....	56

---

---

types of.....	58
Security System Administrators .....	43, 44
Security Systems Administrator .....	40
Security Technical Architecture And Standards .....	28
Security Training Courses.....	38
Security-By-Obscurity .....	48
Segregation Of Responsibility.....	23
Senior Security Engineer .....	43
Simple Network Management Protocol (SNMP)	
detection.....	68
prevention .....	68
Single Events .....	55
Source-Routed Packets .....	59
SSH .....	45
Standard Configurations .....	47
Strong Authentication.....	45
Successful Login.....	46
<i>Suid</i> And <i>Sudo</i> Commands.....	47
Superuser .....	46
Suspicious Activity .....	55
System Access .....	89
access authority .....	89
application processes.....	94
console access.....	93
passwords and pins .....	91

---

---

physical access .....	94
privileged access.....	92
remote access .....	94
system access auditing .....	94
user accounts.....	89
user authentication and login .....	89
System Access Auditing .....	94
System Administrator .....	45
System Administrators .....	44
System Integrity	
executable files and libraries .....	108
system change management .....	108
system configuration management .....	108
System Integrity Audit Scope and Objectives	
purposes of .....	135
the three functions of.....	134
System Integrity Auditing	
and recalculating of baselines .....	110
integrity audit and detection policy .....	136
operations .....	135
scope and objectives.....	134
selected systems.....	109
when audit.....	109
System Integrity Auditing Operations	
list with severity of .....	136

---

---

recalculating security baseline of .....	135
System Monitoring and Auditing .....	109
System Security .....	86
and mandatory minimum risk categories.....	88
radianz risk management methodology .....	88
system access.....	89
system risk categories.....	86
Threat Scenario Planning .....	35
Threats and Countermeasures .....	113
prevention of distributed denial of service attacks.....	113
Traceroute.....	67
detection.....	67
prevention .....	67
Triple DES Encryption.....	45
Twenty-Four Hours A Day.....	41
Two Factor Authentication .....	44
Unauthorized ICMP Traffic.....	59
Universal Participation .....	26
corporate security policy.....	26
radianz code of conduct .....	26
security awareness training.....	26
technology acceptable use policy.....	see acceptable use policy
US Securities and Exchange Commission Regulations for Alternative Trading Systems (RegATS) .....	36
User Accounts.....	36
User Accounts.....	See

---

---

User Identifier.....	44
Vendors .....	52