FISSEA Workshop

16 Jul 08

Dr Timothy Mucklow

NSA/I924

t.mucklo@radium.ncsc.mil

Committee for National Security Systems

Senior policy making forum for discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems through the CNSS issuance system.

21 Voting Members

DHS	**Commerce**	**DIA**
GSA	**Energy**	**DOD**
NSC	**Justice**	**Army**
DNI	**Transportation**	**CIA**
OMB	**Treasury**	**NSA**
Navy	**Marine Corps**	**FBI**
State	**Air Force**	**JCS**

CNSS

SYSTEMS SECURITY FOR THE 21st CENTURY

Training and Education Standards

- **Series of rigorous role-based performance standards**
- **Collaboratively produced by and for the CNSS community**
- **Meet the unique requirements for protecting national security systems**

http://www.cnss.gov/instructions.html

CNSS 4000-Series Instructions

- Sought out and embraced by 170 CNSS-certified institutions in 42 states and the District of Columbia

- Basis for IA curriculum at:

-- 93 NSA/DHS National Centers of Academic Excellence

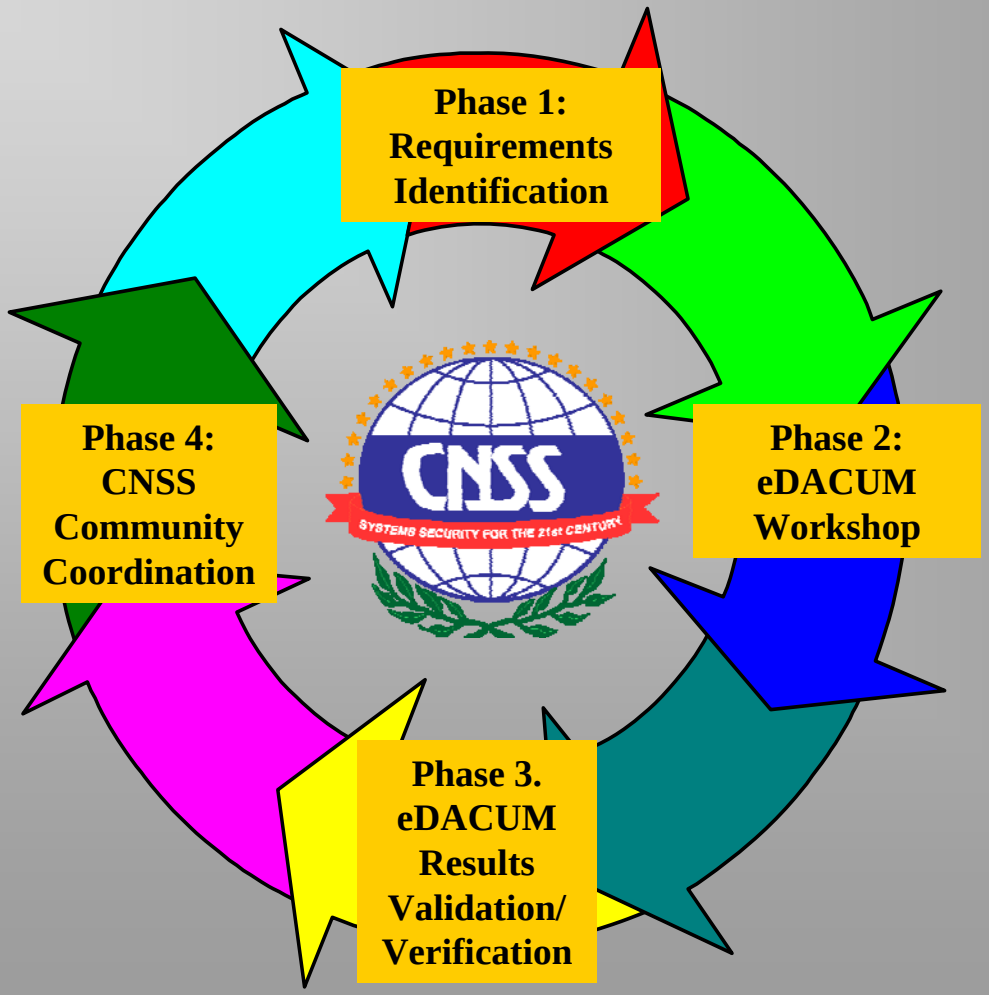
--Service Academies

--Military School Houses

CNSS 4000-Series Instructions

Producing a new generation of work-ready IA professionals from the ground up.

IA Training Standards Development Cycle



e D A CUM©

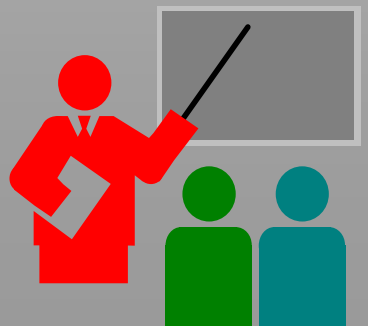
Electronic

Develop

A

Curriculum

A method of occupational analysis through involvement and consensus building to determine training needs as identified by skilled workers and professionals.



A joint CNSS, academia and private sector venture to produce CNSS Training Standards

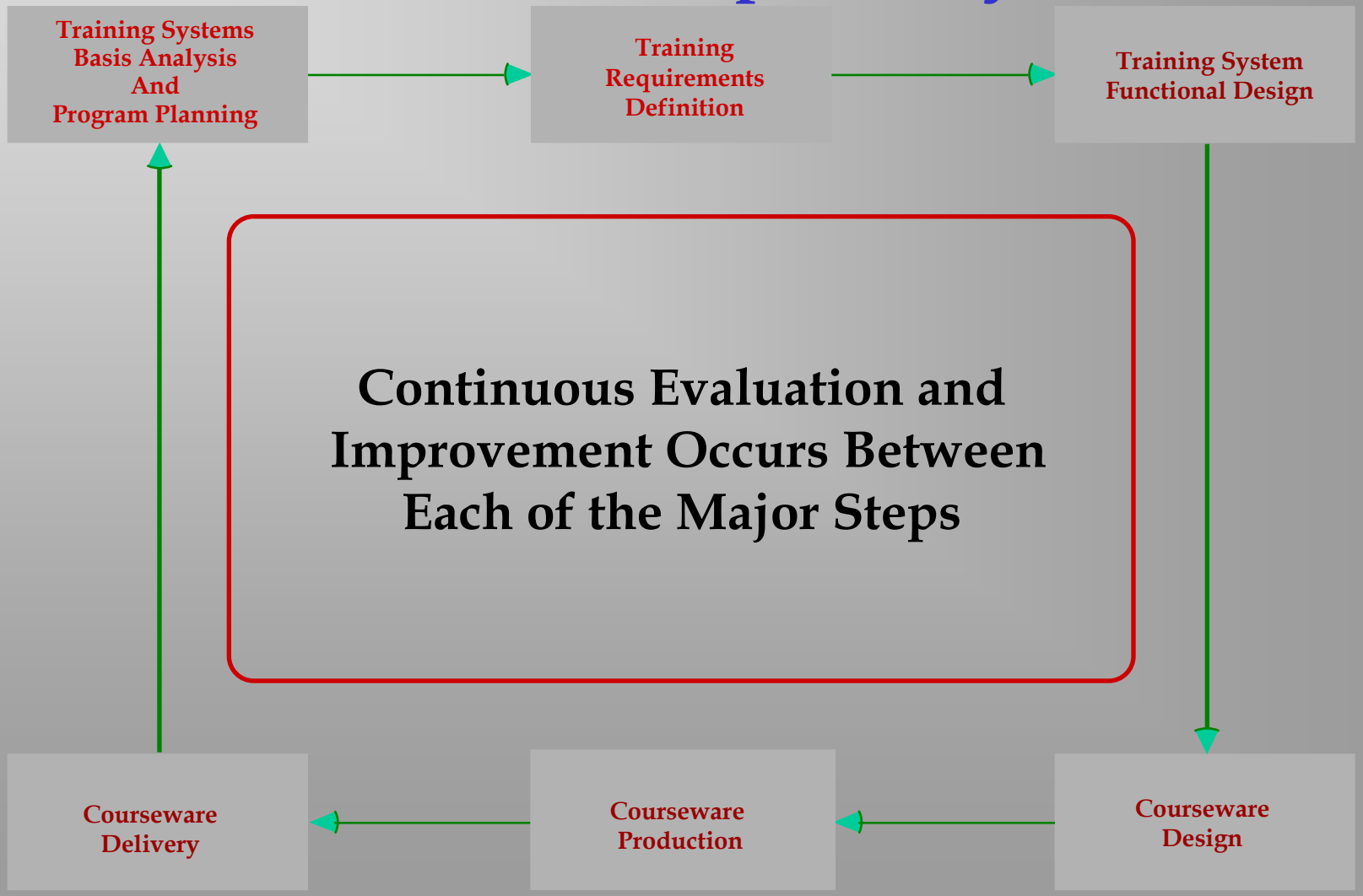
Definition

- **DACUM (day-kum)**
  - An abbreviation for Developing-A-Curriculum
  - An occupational analysis performed by expert workers in the occupation
  - An occupational skill profile which can be used for instructional program planning, curriculum development, training materials development, organizational restructuring, employee recruitment, training needs assessment, meeting ISO 9000 standards, career counseling, job descriptions, competency test development, and other purposes

Philosophy

- **The eDACUM© philosophy states that:**
  - Expert workers can describe and define their job more accurately than anyone else
  - An effective way to define a job is to describe precisely the tasks that expert workers perform
  - All tasks, in order to be performed correctly, demand certain knowledge, skills, tools, and worker behaviors

eDACUM© Supports All Instructional Models and Shortens Development Cycle



K S A

KNOWLEDGE: Broad comprehension of a subject that may not necessarily be applied immediately

SKILL: Comprehension of a subject that is/can be specifically applied to a job

ATTRIBUTE (ABILITY): Personality characteristics which are/can be developed to enhance job performance

KSA Examples

Knowledge Area

(f) Public Key Infrastructure (PKI)

Sub Knowledge areas

Public Key Infrastructure (PKI)
knowledge of how to operate an PKI system
users and managers what PKI is, and how/why it is used
components of PKI as it applies to system
PKI policies and procedures and explain their relevance to users
PKI management in a system
PKI methodology
specific PKI procedures for system IAW national/local policies
PKI Certificates
PKI operating procedures for a system
approved PKI technology
appropriate PKI system
differing public PKI methodologies
PKI process for a system
PKI management into overall system and procedures
PKI conflict with procedures and policies, and variances thereof
policy document
PKI supports security management requirements

Performance Item

KSA + Verb = Performance Item

Bloom's Taxonomy of Verbs

- Affective, Psychomotor and Cognitive

Verb Hierarchy

- Entry
- Intermediate
- Advanced

Examples of Verb Hierarchy

E – Define
E – Demonstrate
E – Describe
E – Identify
E – Outline
E – Use

Entry

I – Describe
I – Design
I – Manage
I– Prepare
I – Recommend
I – Implement

Intermediate

A – Compare
A – Evaluate
A – Integrate
A – Resolve
A – Revise
A – Verify

Advanced

IA Training Standard Excerpt

(f) Public Key Infrastructure (PKI)

E – Define Public Key Infrastructure (PKI)

E – Demonstrate knowledge of how to operate an PKI system

E – Describe to users and managers what PKI is, and how/why it is used

E – Identify components of PKI as it applies to system

E – Outline PKI policies and procedures and explain their relevance to users

E – Use PKI management in a system

I – Describe PKI methodology

I – Design specific PKI procedures for system IAW national/local policies

I – Manage PKI Certificates

I – Prepare PKI operating procedures for a system

I – Recommend approved PKI technology

I – Implement appropriate PKI system

A – Compare differing public PKI methodologies

A – Evaluate PKI process for a system

A – Integrate PKI management into overall system and procedures

A – Resolve PKI conflict with procedures and policies, and variances thereof

A – Revise policy document

A – Verify PKI supports security management requirements

Sample eDACUM© Participants

Government	***Industry***	***Academia***
NSA & NIST	ISI	AFIT
FBI	ISSA	Purdue
DISA	ISC2	CMU
DHS	EADS/NA	Cal Poly
GSA	MIS	Hampton University
DoD Services	Microsoft	MIT
State	CompTIA	University of Texas
Education	CISCO	NDU
FISSEA	NSTAC	Iowa State
Energy	Verizon	Mississippi St
Commerce	Honeywell	Navy PGS
HHS	Rockwell	EDUCAUSE
Treasury	Oracle	NCS
House of Reps	Mitre	University Washington
DIA		

A consortium of over 4,300 IA Professionals in Validation and Verification

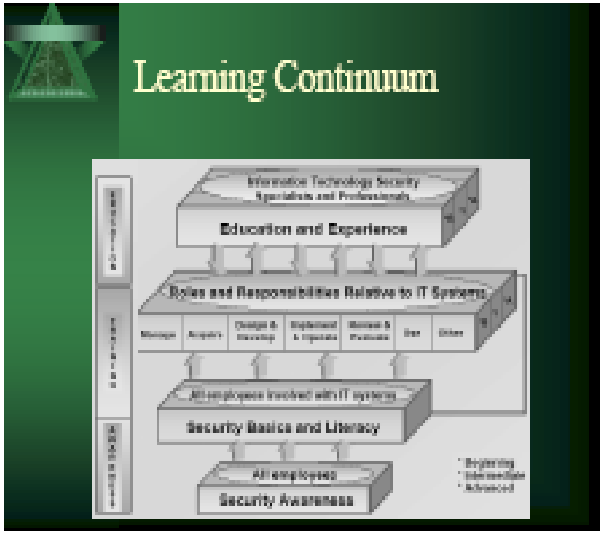
Validation

- All eDACUM© data are validated in Phase 3 Definition
  - The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements
  - Each eDACUM© has had average of
    - 16 active participants (Broad spectrum of participants)
    - 29 direct verification participants (Practitioners)
  - Cross-referenced to other standards
    - CompTIA, NIST, ISC2, ISSA

Cross-reference

- Definition
  - a reference at one place in a body of knowledge to information at another place
- Each CNSS standard has been cross-referenced to elements of CompTIA, NIST, ISC2, ISSA, etc
  - 800-16 originally shared the same database
  - CBK for ISC2 has been cross-referenced three times against emerging standards
  - For example, ISSA provided over 250 individuals to review original standards content

CNSS Standards and NIST



Corey D. Schou, William V. Maconachy, James Frost: Developing Awareness, Training and Education: A Cost Effective Tool for Maintaining System Integrity. (63-83 BibTeX). Presented at and Published by E. Graham Dougall (Ed.): Computer Security, Proceedings of the IFIP TC11, Ninth International Conference on Information Security, IFIP/Sec '93, Toronto, Canada, 12-14 May 1993. IFIP Transactions A-37 North-Holland 1993, ISBN 0-444-81748-4 BibTeX

Description of the model as taken from: NIST Special Publication 800-16, April 1998
(This model was modified from its original form to facilitate better display in this PowerPoint presentation)

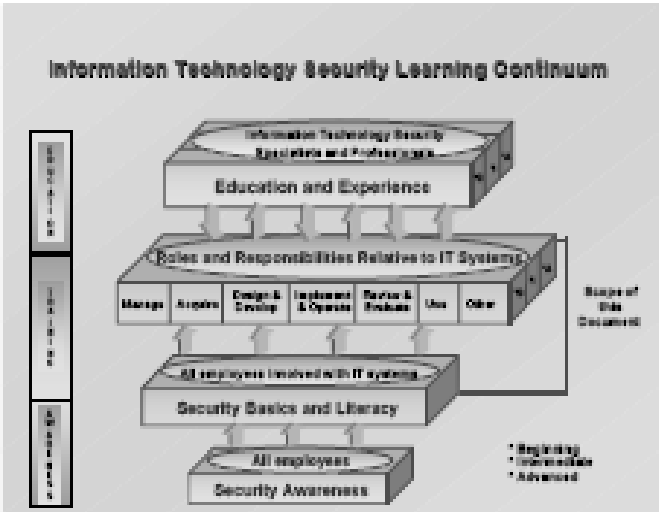
The model presented as Exhibit 2-1 is based on the premise that learning is a continuum. Specifically, learning in this context starts with awareness, builds to training, and evolves into education. This model provides the context for understanding and using this document.

Information Technology Security Training Requirements
Chapter 2. Learning Continuum 14

1992 eDACUM 2

CHAPTER 2. LEARNING CONTINUUM — MODEL AND OVERVIEW

Exhibit 2-1
IT Security Learning Continuum

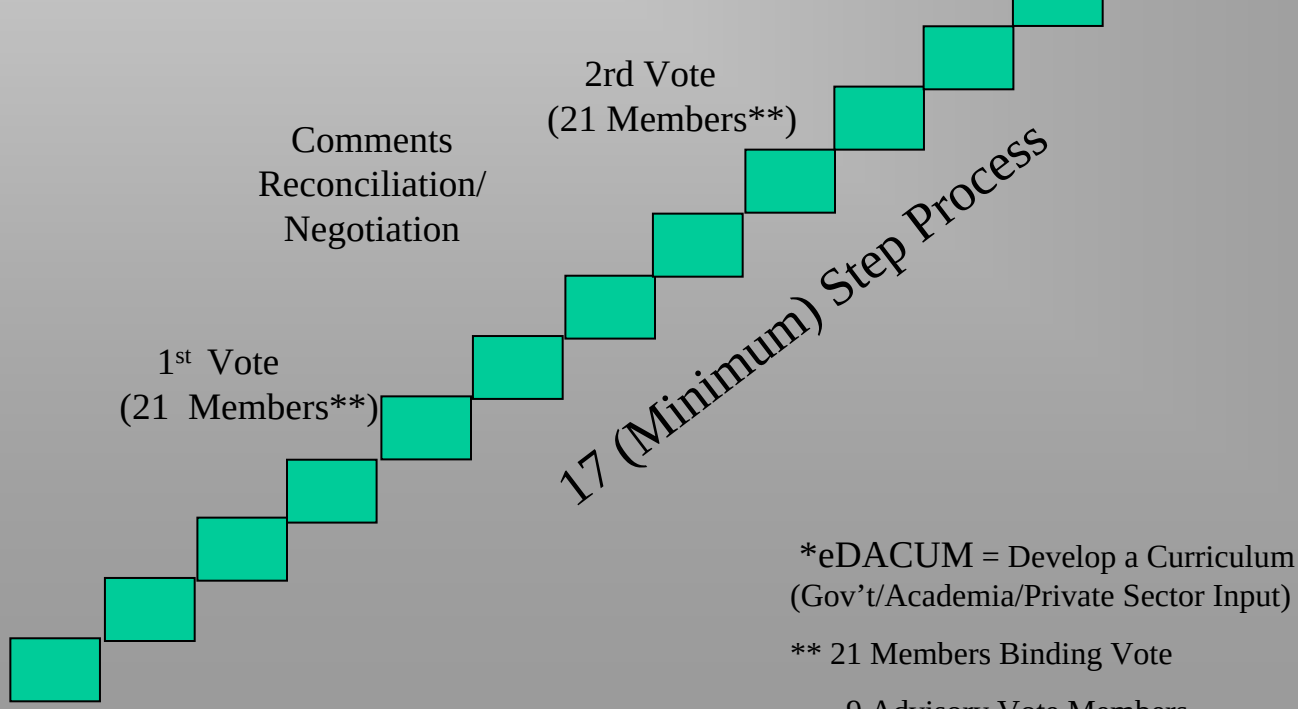


2.1 Introduction to the Model

The model presented as Exhibit 2-1 is based on the premise that learning is a continuum. Specifically, learning in this context starts with awareness, builds to training, and evolves into education. This model provides the context for understanding and using this document.

1998 NIST 800-16

CNSS Community Coordination Process



*eDACUM = Develop a Curriculum Process (Gov't/Academia/Private Sector Input)

** 21 Members Binding Vote

9 Advisory Vote Members

DACUM-Produced Training Standards Update in Progress

CNSSI 4011 IA Professional

CNSSI 4012 Senior Systems Managers

CNSSI 4013 System Administrators

CNSSI 4014 Information System Security Officers

NSTISSI 4015 System Certifiers

CNSSI 4016 Risk Analyst

DACUM-Produced Training Standards Under Development

CNSSI 40xx - Information Assurance Engineer/Architect
--Research completed
--Awaiting validation

CNSSI 40xx - Risk Management Function
--Research completed
--Validation completed

CNSSI 40xx - IA OPSEC Function
--Research completed
--Awaiting validation

CNSSI 40xx - Information Systems Security Manager

CNSSI 40xx - IA Forensics Function

CNSS
(Committee on National Security Systems)

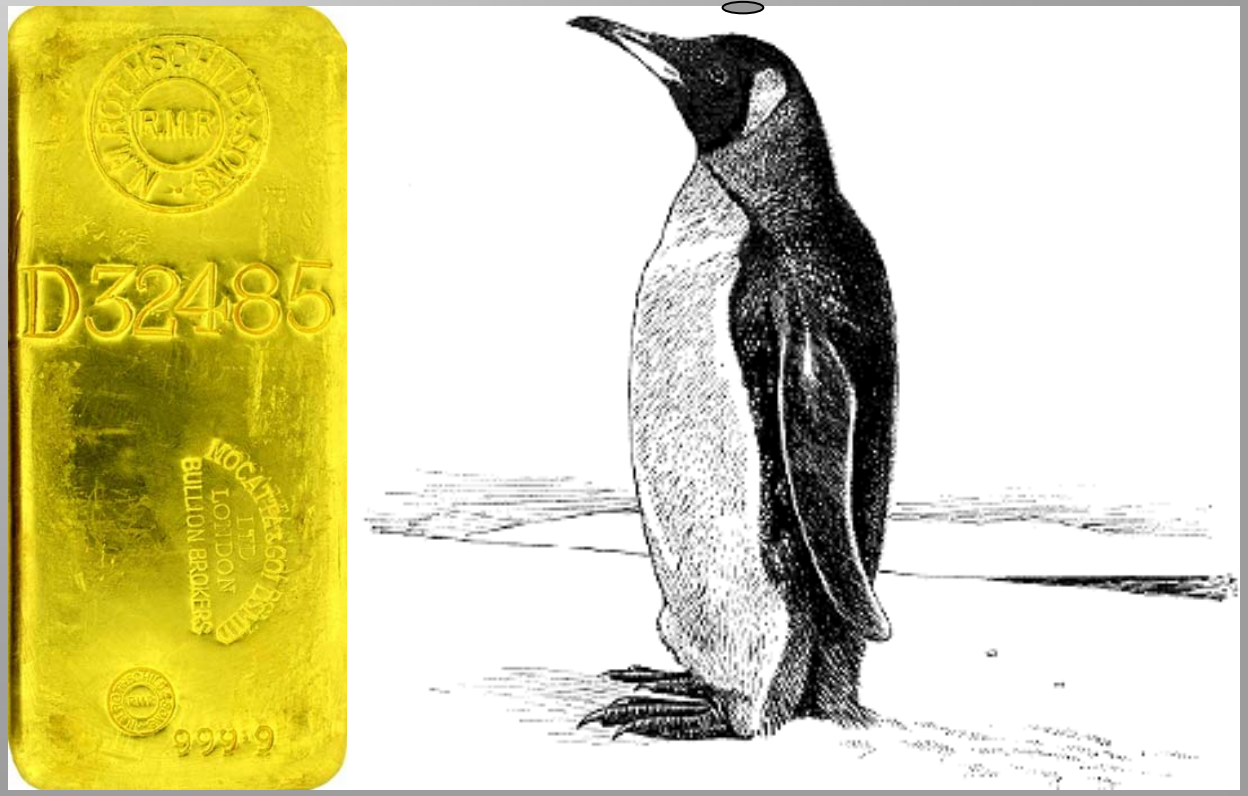
http://www.cnss.gov/

NIATEC

(National Information Assurance Training and Education Center)

- Grew out of a NIST/NSA Workshop in late 80s.
- Repository for IA training and education materials
- Free!!!
- **http://niatec.info/**

Questions ?


D32485
R.M.R
MOCATTA & GOLDSMID LTD
LONDON
BULLION BROKERS
999·9