

# [Information assurance essay sample](https://assignbuster.com/information-assurance-essay-sample/)

Abstract

Information  Assurance  (IA)  is  all  about  managing  the  risks  to  information  assets.  Saying  it  more  specifically,  IA  practitioners  seek  to  protect  the  confidentiality,  integrity,  and  availability  of  data  and  their  delivery  systems,  whether  the  data  are  in  storage,  processing,  or  transit,  and  whether  threatened  by  harmful  intent  or  accident.

Information  assurance  is  closely  related  to  information  security  and  the  terms  are  sometimes  used  interchangeably,  however  it  also  includes  reliability  and  lays  emphasis  on  strategic  risk  management  over  tools  and  tactics.  In  addition  to  defending  against  viruses  and  other  malicious  hackers,  IA  includes  other  corporate  governance  issues  such  as,  audits,  business  continuity,  disaster  recovery,  compliance  and  the  most  important  privacy.  Further,  while  information  security  draws  primarily  from  computers,  IA  is  interdisciplinary  and  draws  from  fraud  examination,  forensic  science,  military  science,  management  science,  systems  engineering,  security  engineering,  and  criminology  in  addition  to  computers.  Therefore,  IA  is  best  thought  of  as  a  superset  of  information  security.

Thus  briefly  IA  may  be  defined  as  “ Measures  that  protect  and  defend  information  and  information  systems  by  ensuring  their  availability,  integrity,  authentication,  confidentiality,  and  non  repudiation.  These  measures  include  provide  for  restoration  of  information  systems  by  incorporating  protection,  detection,  and  reaction  capabilities.

Introduction  to  Information  Assurance

Most  programs  delivering  capability  to  do  the  war  fighter  of  business  domains  will  use  information  technology  to  enable  or  deliver  that  capability.  For  those  programs,  developing  a  comprehensive  and  effective  approach  to  IA  if  a  fundamental  requirement  and  will  be  key  in  successfully  achieving  program  objectives.  IA  thus  can  be  said  is,  measures  that  protect  and  defend  information  and  information  system  from  malicious  threat  that  provides  availability  authentication.  Program  managers  and  functional  proponents  for  programs  should  be  familiar  with  statutory  and  regulatory  requirements  governing  information  assurance,  and  understand  the  major  tasks  involved    in  developing  an  IA  organization,  defining  IA  requirements,  incorporating  IA  in  the  program’s  architecture  ,  developing  an  acquisition  IA  strategy  (when  required),  conducting  appropriate  IA  testing,  and  achieving  IA  certification.  Thus  the  programmers  of  IA  aim  for  taking  steps  towards  effective  IA  defenses  in  depth  in  a  net-centric  environment.

Process  of  Information  Assurance

The  IA  process  typically  begins  with  the  classification  and  enumeration  of  the  information  technology  (IT)  assets  to  be  protected.  Next  step  of  this  process  is  that  the  IA  practitioner  will  perform  a  risk  assessment.  Basically  this  assessment  considers  both  the  probability  and  impact  of  the  undesired  events  like  malicious  hacking  or  threats.  The  probability  component  is  subdivided  into  vulnerabilities  and  threats,  and  may  be  measured  in  terms  of  annualized  rate  of  occurrence  (ARO).  The  impact  component  is  usually  measured  in  terms  of  cost,  specifically,  single  loss  expectancy  (SLE).  The  product  of  these  values  is  the  total  risk,  often  measured  in  terms  of  annual  loss  expectancy  (ALE).

This  can  be  expressed  as:

Annualized  Loss  Expectancy  (ALE)  =  SLE  \*  Annualized  Rate  of  Occurrence  (ARO)

Thus  an  IA  practitioner  will  develop  a  risk  management  plan  based  on  the  risk  assessment.  This  plan  proposes  measures  to  some  important  terms  like  eliminating,  mitigating,  accepting,  or  transferring  the  risks,  consider  prevention,  detection,  and  response.  A  framework,  such  as  ISO  17799,  is  a  typically  utilized  in  designing  this  risk  management  plan  successfully  and  efficiently.  Countermeasures  may  include  some  security  tools  such  as  anti-virus  and  firewalls  software,  policies  and  procedures  hardening  of  configuration  and  regular  backups,  and  some  trainings  like  (IA)  security  awareness  education,  or  reconstructing  such  as  forming  an  computer  security  incident  response  team(CSIRT)  or  computer  emergency  response  team  (CERT).  The  return  on  investment  (ROI)  of  each  countermeasure  is  carefully  considered.  Thus,  the  IA  practitioner  does  not  seek  to  eliminate  all  risks  and  malicious  occurrences,  were  that  possible,  but  to  manage  them  in  the  most  cost  effective-way.

After  the  implementation  of  risk  management  plan,  it  is  tested  and  then  further  evaluated,  perhaps  by  means  of  audits.  The  IA  process  is  cyclic  in  nature,  and  the  plan  involving  the  risk  management  and  assessment  are  regularly  improved  and  revised  on  the  basis  of  the  data  gained  from  the  evaluation.

Information  Assurance  Programs

The  mission  for  running  the  IA  programs  and  offering  variety  of  courses  like  IA  awareness  is  to  ensure  the  DOD’s  vital  information  resources  are  secured  and  protected  by  integrating  IA  activities  to  retrieve  a  secure  net-centric  GIG  operations  and  enabling  information  superiority  by  applying  a  deep  depth  defense  technology  which  includes  the  capabilities  of  people,  operations,  and  technology  to  establish  a  multi-layer,  and  multi  dimensional  protection  of  the  information.  Programs  like  IA  awareness  and  other  education  related  to  IA  have  played  a  very  important  role  in  defending  the  information  against  threats.  It  can  be  roughly  said  that  it  was  started  during  the  year  2003-2006  on  a  large  scale.  Nowadays  these  programs  are  running  in  large  scale  in  military  camps  and  in  several  other  federal  and  intelligence  services  where  the  protection  of  the  information  is  must.  Currently  there  are  a  number  of  universities  providing  the  bachelor  and  master  degrees  in  Information  Assurance  some  of  which  are  College  of  Business,  Idaho  State  University,  University  of  Dallas,  Florida  Institute  of  Technology  and  many  other  institutes  are  present  worldwide.  With  the  partnership  of  the  government  and  the  academia,  the  National  Information  Assurance  Education  and  Training  Program  (NIETP)  provides  a  wide  range  of  services,  it  operates  under  the  national  authority.  The  (IA)  programs  mainly  lay  stress  on  following  important  areas:

* Information  Awareness  Toolkit
* CNSS  Training  and  Education
* Cyber  Defensive  Exercise

Information  Awareness  Toolkit

This  part  basically  deals  with  the  encouragement  of  (IA)  education  and  training  with  federal  government,  the  idea  of  “ tool  kit”  was  developed  by  the  members  of  the  National  Information  Assurance  Education  and  Training  program  (NIETP).  The  kit  basically  includes  CDs,  videos  and  pamphlets  for  an  easy  user  interface  and  which  makes  this  very  useful  and  easy  for  everyone  to  understand  it.

CNSS  Training  and  Education

The  Committee  on  National  Security  continues  to  chair  the  committee  under  the  authority  established  by  NSD-42.  The  secretary  of  Defense  and  the  director  of  Central  Intelligence  are  responsible  for  developing  and  implementation  of  government-wide  policies,  principles,  standards,  and  guidelines  for  the  security  of  the  systems  with  national  security  information.  The  CNSS  provides  a  forum  for  the  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.  National  security  systems  contain  classified  information  for

* Involve  intelligence  activities
* Involve  cryptographic  activities  related  to  national  security
* Involve  command  and  control  of  military  forces
* Involve  equipment  that  is  an  integral  part  of  a  weapon  or  weapons  system  (is  critical  to  the  direct  fulfillment  of  military  or  intelligence  missions)
* Are  critical  to  the  direct  fulfillment  of  military  or  intelligence  missions

Cyber  Defensive  Exercise

The  Cyber  Defense  Exercise  (CDX)  serves  as  the  final  project  for  high-level  computer  science  majors  enrolled  in  the  United  States  Military  Academy  (USMA)  assuring  the  information.  The  main  aim  of  (CDX)  is  to  strengthen  the  knowledge  of  cadets  and  midshipmen  have  acquired  during  their  courses  that  addresses  the  defense  of  information  systems.  The  students  are  required  to  make  a  plan,  design  to  take  part  in  this  education  plan  including  applications,  and  various  operating  systems,  and  the  plans  must  address  the  issue  of  maintaining  integrity,  confidentiality,  and  availability  of  all  sources  and  services,  this  event  is  sponsored  by  The  National  Security  Agency’s  Director  of    Information  Assurance.  (CDX)  is  a  part  of  Defense-Wide  Information  Assurance  Program  (DIAP).  This  part  includes  various  trainings  and  tests  increasing  the  knowledge  of  the  person  about  Information  Assurance  and  other  systems  which  defend  information.

Information  Assurance  (IA)  Strategy

This  part  plays  a  very  vital  role  in  defense  of  information  using  (IA).  Information  Assurance  Strategy  basically  includes  10  important  steps  to  be  performed  which  are  necessary  for  building  a  safe  and  defense  the  information  from  various  malicious  threats,  so  the  following  steps  are  to  be  performed:

1. Program  Category  and  Life  cycle  Status:  Identify  the  Acquisition  category  of  the  program.  Identify  current  acquisition  life  cycle  phase  and  next  distant  decision.  Identify  whether  the  system  is  being  used  for  “ Mission  Critical  Information  System”  or  “ Mission  essential  Information  system”  in  accordance  with  DoD  Instruction  5000. 2,  enclosure  4.  Include  a  graphic  representation  of  the  program’s  schedule.
2. Mission  Assurance  Category  (MAC)  and  confidentiality  Level:  The  two  primary  steps  to  be  taken  are  that  determine  the  privacy  level  and  identify  the  system’s  MAC  in  the  applicable  capabilities  document,  or  as  determined  by  the  system  User  Representative  on  behalf  of  the  information  owner,  in  accordance  with  DoD  Instruction  8500. 2.
3. System  Description:  The  system  which  is  being  acquired  should  be  provided  with  a  high-level  overview.  Graphics  like  (block  diagram)  must  be  used  showing  major  elements  and  subsystems  that  are  the  part  and  make  up  the  system  or  service  being  acquired  and  also  showing  how  they  are  connected  to  each  other.  It  is  also  important  to  describe  the  system’s  function,  and  summarize  significant  information  exchange  requirements  (IER)  and  interfaces  with  other  IT  or  systems,  as  well  as  primary  databases  supported.
4. Threat  Assessment:  Methods  should  be  described  which  determine  threats  to  the  system  (such  as  System  Threat  Assessment),  and  whether  the  IT  was  included  in  the  overall  weapon  system  assessment.  In  the  case  of  an  AIS  application,  it  should  be  described  whether  there  were  specific  threats  unique  to  the  system  or  not.  For  MAIS  programs,  utilization  of  the  “ information  Operations  Capstone  Threat  Capabilities  Assessment”  (DIA  Doc  #  DI-1577-12-03)  is  required  by  DoD  Instruction  5000. 2.
5. Risk  Assessment:    Plans  including  projects  for  regimen  of  risk  assessments  should  be  mentioned,  including  a  summary  of  how  many  completed  risk  assessments  were  conducted.
6. Information  Assurance  Requirements:  Identify  the  applicable  sets  of  Baseline  IA  Controls  from  DoDI  8500. 2  that  will  be  implemented.  Whether  any  specific  IA  requirements  are  identified  in  the  approved  governing  requirements  documents  (e. g.  Capstone  Requirements  Document,  Initial  Capabilities  Document,  Capabilities  Design  Document,  or  Capabilities  Production  Document).  The  cost  of  IA  requirements  implementation  including  with  certification  should  be  described  and  also  the  overall  program  budget  should  be  shown.
7. Acquisition  Strategy:  A  summary  should  be  provided  showing  how  information  assurance  addressed  in  the  program’s  overall  acquisition  strategy  document.  The  Request  for  Proposal  (RFP)  for  the  System  Development  and  Demonstration  should  be  described.  In  addition,  describe  how  the  RPF  communicates  the  requirement  for  the  persons  that  are  trained,  and  appropriately  certified  in  accordance  with  DoDD  8570. 1,  in  IA.
8. IA  Testing:  In  this  part  it  is  discussed  that  how  IA  testing  has  been  integrated  into  the  program’s  test  and  evaluation’s  planning,  and  incorporated  into  program  testing  documentation,  such  as  the  Test  &  Evaluation  Master  Plan.
9. IA  Shortfalls:  Proposed  solutions  and  any  of  the  significant  IA  shortfalls  and/or  mitigation  strategies  must  be  identified  primarily.  Impact  of  failure  to  resolve  any  shortfall  or  malfunctioning  in  terms  of  program  resources  and  schedule,  inability  to  achieve  threshold  performance  and  system  or  war  fighter  vulnerability  should  be  specified.  A  recommendation  identifying  the  organization  with  the  responsibility  and  authority  to  address  the  shortfall  should  be  provided  which  will  be  responsible  for  taking  necessary  steps  while  the  malfunctioning  of  the  system  or  when  the  (IA)  is  not  working  properly.
10. Point  of  Contact:  The  name  and  contact  information  for  the  program  management  office  individual  responsible  for  the  acquisition  IA  Strategy  document  should  be  provided.

Information  Assurance  Technical  Framework  (IATF)

The  framework  of  the  Information  Assurance  defines  an  infrastructure  that  how  the  system  of  protecting  data  is  carried  away  safely  and  efficiently.  Most  important  feature  of  the  (IATF)  is  the  Wireless  Networks  Security  Framework;  this  section  is  incorporated  because  the  IATF  also  handles  many  security  concerns  and  secure  infrastructure  elements  that  also  affect  wireless  communications.  Exposure  of  wireless  communications  in  the  radio  frequency  (RF)  transmission  environment,  and  the  portability  of  computer  processing  and  storage  that  wireless  connectivity  provides,  add  another  set  of  vulnerabilities  to  the  vulnerabilities  of  wired  network  systems.  This  section  will  present  the  areas  of  security  where  wireless  communication  presents  additional  vulnerabilities,  different  customer  requirements,  and  different,  although  related,  security  concerns.

Information  Assurance  (IA)  Vulnerabilities

The  word  “ vulnerability”  defines  the  extent  of  damaging  a  thing  that  is  how  much  the  thing  is  safe  from  malicious  acts  or  any  other  threat  of  damaging.  Vulnerabilities  in  (IA)  can  be  explained  under  following  heads:

* Physical  Vulnerabilities
* Vulnerabilities  to  Electromagnetic  Attack  and,
* Cyber  vulnerabilities.

Physical  Vulnerability

Although  our  life  is  running  between  the  physical  and  cyber  dimensions  the  physical  dimensions  is  still  very  important.  Physical  attacks  against  key  nodes  with  disproportionate  effects  are  old  age  military  problems.  Protecting  these  primitive  weapons  can  still  be  the  most  effective.  Critical  network  nodes,  satellite  ground  stations,  and  other  dedicated  military  and  commercial  infrastructure  can  be  attacked  directly  with  high  explosives  or  other  physical  means  to  disrupt  the  operations  of  military.  Attacks  against  military  forces,  therefore,  can  be  mounted  in  areas  far  removed  from  the  location  of  operations.  Therefore  these  nodes  would  be  attractive  targets  and,  if  successfully  attacked,  their  vulnerability  may  have  a  disproportionate  effect  on  military  operations.  At  the  other  end  of  the  spectrum,  if  any  enemy  forces  capture  one  of  the  many  individual  computers  that  will  proliferate  the  future  battlefield  possibly  along  with  the  legitimate  user  adversaries  may  be  able  to  aces  the  battlefield  networks  and  use  that  access  to  disrupt  operations  of  the  military.

Electromagnetic  Vulnerabilities

The  term  “ electromagnetic  threats”  covers  a  wide  range  of  possible  weapons  that  includes  “ directed  energy”,  electromagnetic  pulse  (EMP),  and  electronic  warfare.  These  weapons  are  able  to  incapacitate  or  destroy  electronic  systems  without  physical  attack  or  explosives.  The  effects  of  one  form  of  directed  energy,  electromagnetic  pulse  (EMP),  were  firstly  observed  during  the  last  U. S.  atmospheric  nuclear  test  in  1962  (named  “ Starfish  Prime”),  which  severely  damaged  the  electrical  systems  in  Hawaii-800  miles  away.  EMP  of  this  type  is  generated  by  nuclear  weapons,  can  produce  a  large  electric  fields  over  significant  areas  (which  depends  upon  the  altitude  of  weapon  detonation)  and  has  been  recognized  as  a  threat  to  electronic  systems.  EMP  also  poses  threats  to  the  satellite.  Thus  it  can  be  concluded  that  EMP  of  strong  and  increased  power  and  can  really  damage  satellites,  electrical  systems,  electrical  components  and  other  components  like  microchip  and  other  circuit  devices  and  chips  used  in  the  computer  systems  and  various  other  equipments  thus  creating  a  hurdle  in  the  way  in  the  operations  of  the  military.  Advance  tools,  laser  pointers,  fax  machines,  printers,  and  other  scanners  all  use  a  form  of  directed  energy  thus  they  can  easily  be  affected  by  (EMP).

Cyber  Vulnerabilities

Attacking  through  cyber  technology  is  an  attractive  and  alternative  method  to  defeat  defense  technology  of  information  systems.  They  offer  the  attacker  the  potential  to  play  on  a  near  level  playing  field  and  the  effects  can  be  disproportionate  to  the  effort  involved.  The  attacker  can  be  a  hacker,  a  programmer,  an  insider,  a  terrorist,  a  hostile  nation  state,  or  a  combination  of  these.    When  considering  military  operations,  the  motive  for  cyber  attacks  can  range  from  creating  a  mischief,  to  hacking  into  sites  to  make  a  political  statement,  to  espionage,  to  the  disruption  of  operations.  Since  all  attackers  use  the  same  or  similar  techniques,  identification  of  the  motives  is  usually  very  difficult.  Additionally,  as  the  number  of  people  with  computer  skills  has  increased  the  tools  of  hacking  and  techniques  have  become  easily  available  to  anyone  with  access  to  the  internet,  the  degree  of  technical  sophistication  required  to  successfully  hack  into  a  system  has  been  reduced.  Law  enforcement  methods  for  investigating  intrusion  attempts  are  cumbersome  and  time  consuming  and  would  prove  unsatisfactory  in  time  of  war-especially  if  battlefield  systems  were  attacked.  Thus  a  programmer  is  required  which  monitor  each  and  every  small  change  and  which  is  able  to  fight  the  hacker  or  insider.