# Chapter 1: Introduction

## Terminology

Attack vector: Path/Means which vulnerabilities can be exploited.

Principle of easiest Penetration:

Attacker can use any means and do not behave the way it is expected. System is as strong as the weakest link. E.g. Remote Access Trojan(RAT) Havex

## Trinity of Trouble

Connectivity

Consequence: Mirari Malware, P2P.

Extensibility

Complexity

## Security Management

Human: Need clear mgm. Technology: Need to keep up to date. Process: System to identify threats

## Security Goals

Integrity: Unauthorized modification

Confidentiality: Unauthorized access

Availability: Unauthorized access

Non-Repudiation: Unauthorized sender

Possession: Ownership/Control

Utility: Usefulness of information

Authenticity: Authorship of piece of information

## Network/Internet Security

Network Sec: Focus on network layer protocol. Internet Sec: Security issues from internet applications eg. Browsers, botnet, DoS attacks.

## Advantage of attackers

1)Sitting duck Syndrome 2) Moving goal post 3) One way 4) Only need to succeed once 5) Cost to defend is high 6) System complexity helps attacker

# Chapter 2: Info sec, gov & law

## Purpose of Controls

Preventive: Authentication Based Access

Detective: Intrusion detection, recognize attacks

Corrective: Restore data, dmg control

## Nature of Control

Physical: Determine Access, data center

Procedural: Codify control types, incident response process

Technical: tech soln, user authentication

Legal & Regulatory: privacy laws, GDPR

## Defense in Depth/ Layered Security

Layered Security: Multiple layers protecting one point. Defense in depth: Defense multiple points with layered security. Buys reaction Time.

# Chapter 2.2: Standards and Guideline

## Purpose:

Articulate Requirements and Specifications: Eradicates ambiguity, Actionable. Eg. ISO/IEC 18031:2011, ISO/IEC 2700-series

## Common Criteria

CC: Guide to define security needs, develop, evaluate & procure products standards. Enables independent, consistent cert, gives global recognition. One of the properties is Privacy. Eg. ISO/IEC15408-1:2009.

IT product evaluation only meaningful if: [1] Specific properties were evaluated. [2] Evaluation assurance level is stated.

# Chapter 2.3: Laws and Regulations

## Challenges of law @ international level:

[1] Jurisdiction [2] Heterogeneous & even contradictory laws. Eg. Microsoft hand over overseas email, against EU laws. [3] Conflict of Interests.

Soln: Budapest Convention on Cybercrime 2001: Harmonizing national laws and increase coopn among nations.

## Singapore

### Banking act

### Monetary Authority of Sg (MAS)

- Comprehensive tech risk

- Single point of failure and fragility in functional design and specs: [1] Periodic Testing [2] Backup & offline Storage

- Three internal security principles:

[1] Defense in depth [2] Need to know [3] Least privilege

### Personal Data Protection Act(PDPA)

[1] PDPC: Personal data protection commission [2] Develop and implement policies and practices [3] DPO: Oversee data protection respn & ensure compliance with PDPA

### Cybersecurity Bill 2017

[1] License Agreement [2] Harmonize requirements for critical info infras (CII)

### GDPR

[1] Revenue based fines

[2] Data breach Notification

[3] Right to be forgotten

# Chapter 2.3: (GRC)

## Governance (G)

Mgm approach by senior executive to direct & control org.

[1] Align Security Objs w biz goal and legal obligations [2] Internal Policies and self-regulation. [3] Ensure that resources allocated & responsibilities assigned.

## Risk Management (R):

Process to identify, analyze and act to min(risk).

[1] Same as (G)

## Compliance (C):

Conforming w Stated Requirements

[1] Set out internally. [2] Through extrinsic requirements (law, reg, contract)

## Chapter 2.4: IT Security Audit

[1] Audit Planning and Preparation [2] Establish audit Obj [3] Carry out review/audit

### Performance Metrics

# Chapter 3: Risk Analysis and Assessment

Dilemmas: How much resource for each type of control, complacency, how much is good enough, fallacy of relative privation, compliance out of compulsion

# Chapter 3.1: Risk analysis

Desired Outcomes: Minimize exposure while providing functionality/usability

# Chapter 3.2: Risk analysis Process:

[1] Info gathering: process and policy, input from advisor, repository of known vulnerabilities

[2] Vulnerability Analysis: Determine current exposure, Penetration Testing.

[3] Categorize vulnerability: Severity & Exposure

[4] Threat Analysis: Human vs non-Human

[5] Risk identification and analysis of acceptable risk: risk urgency & interdependencies

Framework: NIST Special Publication

# 3.3: Qualitative vs Quantitative Analysis

### Qualitative Analysis:

No proper financial analyses to justify budget

Pros: [1] Simple to analyze & convey, [2] Flexible, [3] cover wider set of issues

Cons: [1] Subjective, [2] Ambiguous: Difficult to compare results.

### Quantitative Analysis:

Attempts to assign independently objective monetary values to components of risk and potential loss. Derived from cost/benefits.

Pros: [1] Justifiable cost that uses cost/benefits: Easy to understand. [2] More credible, [3] supports budget decisions

Cons: [1] Complex/Inapplicable: Lots of guesswork & Unable to tell secondary effects. ALE cannot tell btw high-freq, low impact vs low-freq, high impact. [2] False sense of accuracy.

# Chapter 3.4 Actualizing Risk Analysis

[1] Penetration Testing

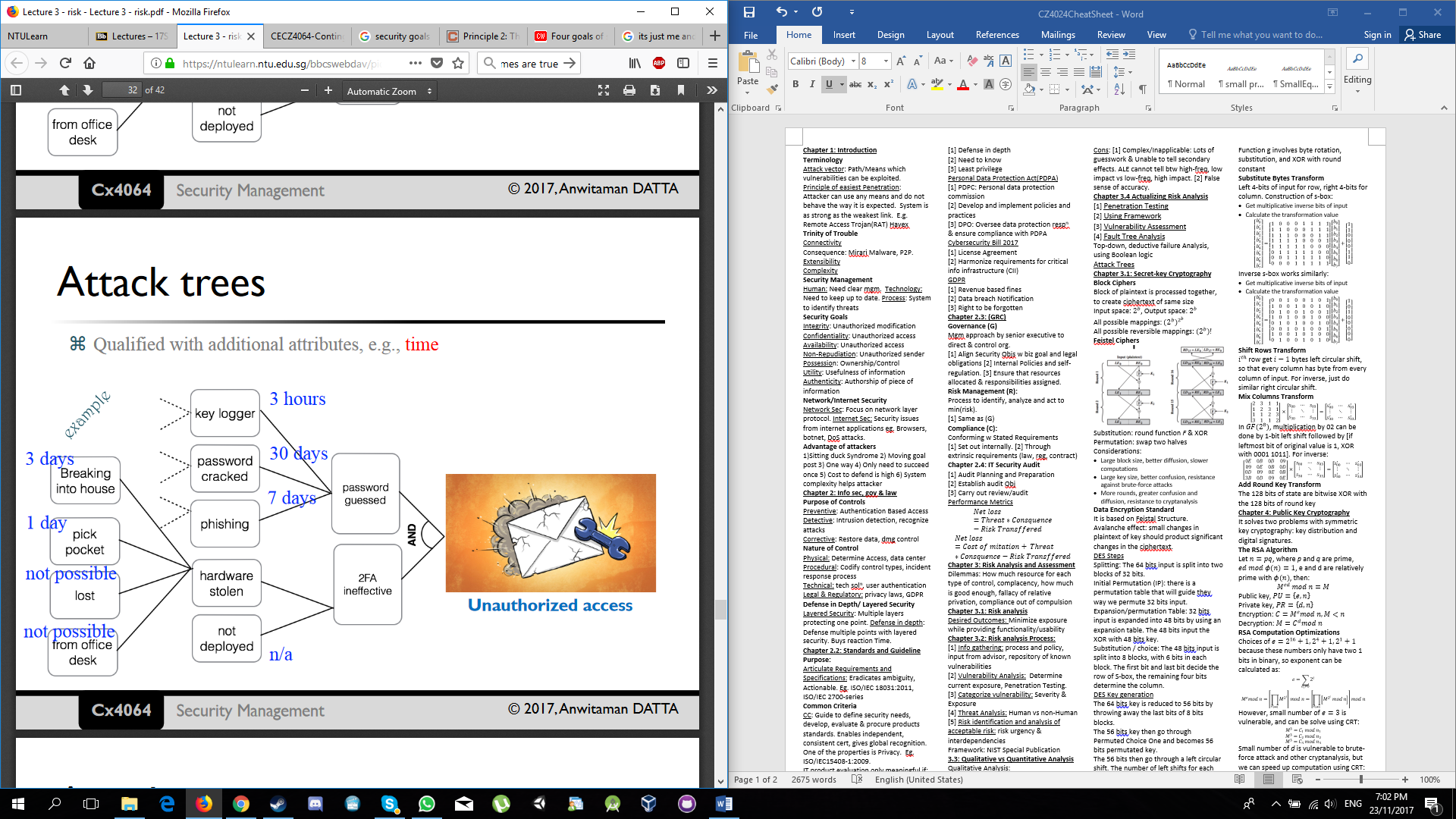
[2] Using Framework

[3] Vulnerability Assessment

[4] Fault Tree Analysis

Top-down, deductive failure Analysis, using Boolean logic

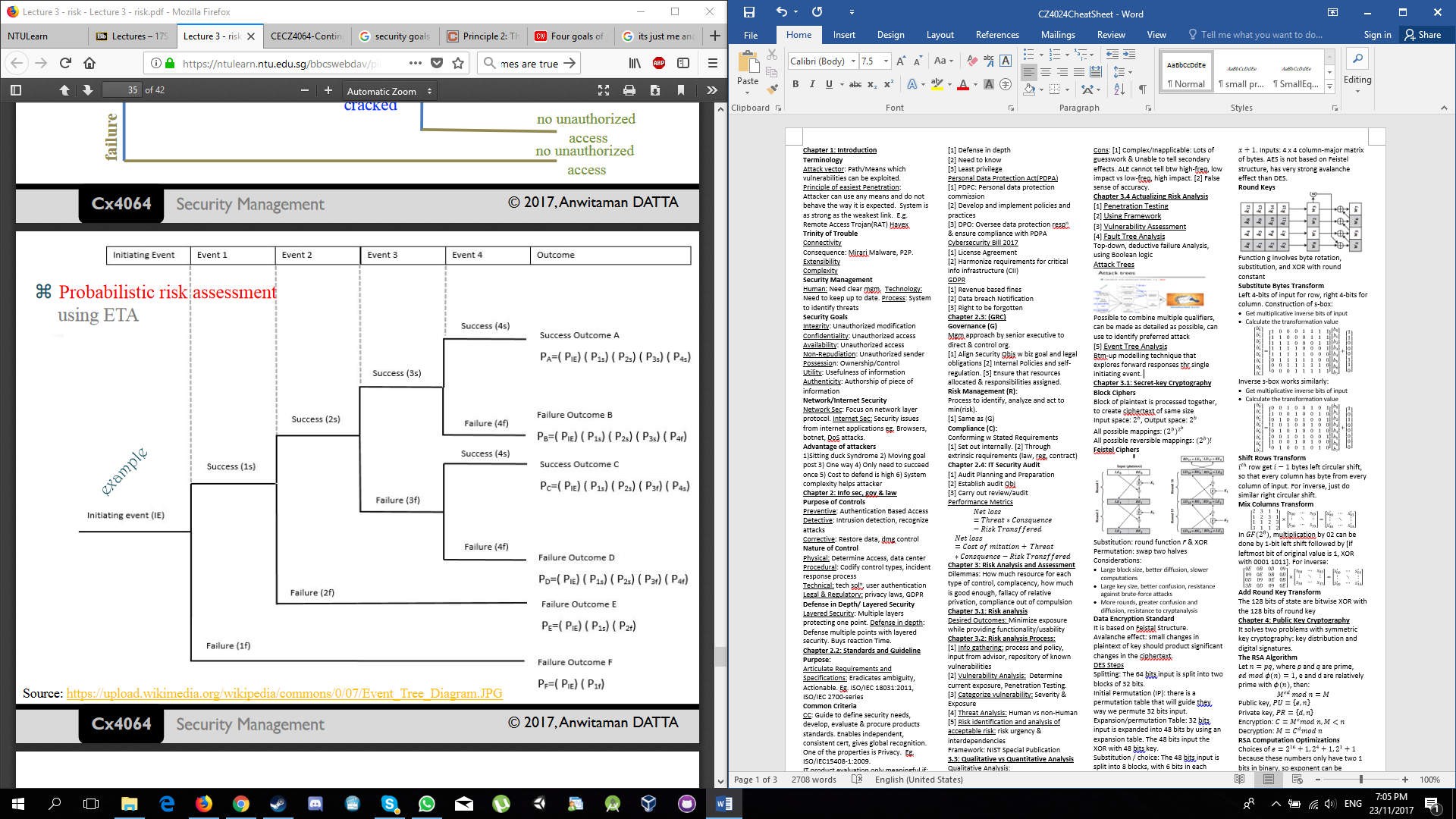
Attack Trees



Possible to combine multiple qualifiers, can be made as detailed as possible, can use to identify preferred attack

[5] Event Tree Analysis

Btm-up modelling technique that explores forward responses thr single initiating event.



[6] FMEA

Inductive reasoning single point of failure analysis: To review as many components, subsystems as possible. To identify failure modes, causes and effects.

# Chapter 4: Contingency Planning & mgm

## Contingency:

Why: [1] Economics of Info Sec [2] No perfect system [3] Emergence [4] To stay functional

## Biz Continuity:

To ensure that orgs are able to withstand any disruption to normal functioning.

[1] Emergency Reponses: Time critical [2] Crisis Mgm: Strategic Direction [3] Biz recovery: Phased recovery of biz-critical process & disaster recovery

How:

[1] Conduct BIA & RA: Establish biz recovery prioties & timescale, min req

[2] BC Strategy Formulation: Options for meeting priorities, timescale, mini req

[3] BCP Production: Plans, org, resp, logisitics, detail action task list

[4] BCP Test: Test strategy, plans, testing, evidence

[5] BC awareness: Awareness

Ongoing BCP Maintenance: Maintenance activity

## Biz Impact Analysis (BIA)

[1] Determine Critical Biz Process, services, products. [2] Identify activities that support provision of crit-biz, processes, services and products.

[3] Asses impacts over time of not performing these activities

[4] Set prioritized timeframes for resuming activities

[5] Identify dependencies and supporting res for these activities. (+ 3rd party dependencies)

### Key Considerations: [1] Policy & regulatory compliance req. [2] Customer impact analysis. [3] 3rd party dependencies. [4] System impact analysis [5] Recovery Req.

## Recovery Requirements

Recovery Time obj (RTO): duration from pt of disruption to restored

Recovery pt obj (RPO): Acceptable amt of data loss for IT system.

### Recovery Options:

Common approaches

[1] Hot, cold, semi hot sites [2] Shared services/mutual support [3] Amortize res

[1] Virtualization [2] Cloud services [3] Re-purposing existing services.

## Contingency Planning:

Process which biz develop a strategy to deal with unanticipated events that would impede daily/normal ops.

# Chapter 5: Model, Framework & Approach

# Chapter 5.1: Approaches

## Military Approach

[1] Info classification: Ranking of info and sensitivity; Hierarchical requirement. [2] Need to know principle: determines and limit info; non-hierarchical. [3] Uses Bell-Lapadula(BLP) model which defines MAC policy that enforces [1] and [2]. [4] Principle of least privilege (need to hold): enforces that user doesn’t access more than what they need to know.

Drive: [1] National security at stake [2] Complete protection [3] Cost of security embedded in IT systems and infrast.

Focus: [1] Enforcement of need to know, classification, clearance, least privilege. [2] Ensure proper classification, personnel security clearance, system security evaluation certification [3] System complies with CC specifications.

Performance: [1] Determine by completeness of functionality & assurance of correctness and accuracy of implementation. [2] Security measure by level of assurance eg.CC

Outcomes: [1] High cost [2] Slow to evolve and adapt: Unable to capitalize new tech. [3] Tight coupling: Interoperability suffers. [5] No perfect security.

## Commercial Approach

[1] Less strict and hierarchical structured. [2] No system of security clearance: Rules decided by owner [3] uses DAC. [4] Principle of separation of duty: Reduce potential of abuse and prevent conflict of interest (brewer and Nash): A person can access any info so long the person has not access info from a different company in same conflict class. [5] Principle of weakest link and defense in depth: Defense in depth and [6] baseline Security: Ensure every IT component have minimum security. This covers weakest link.

Drive: [1] Compliance [2] Fear of increase incidents [3] Reactive actions to limit loss but unsustainable.

Focus: [1] Info classification [2] Implement best practice [3] Prevent known issues [4] Protect-detect-react

Performance: [1] Measure by compliance audit [2] Maybe supplemented by periodic security reviews

Outcomes: [1] Address only known & discoverable [2] Compliance-driven resourcing [3] Reactive to unplanned security events [4] Cost questionable if number of incidents rises. [5] Justification for security uncertain: Benefits cannot be seen clearly.

## Risk-based Approach

[1] Higher baseline [2] Consider other factors: Human, office polities. [3] Better defense in depth system. [4] Risk management: understanding tradeoff btw risk and available resources: Info security manager need to prioritize limited resources

Drive: [1] Cost management [2] Resource Prioritization [3] Align with biz understanding of risk [4] Regulators’ recognition of risk management discipline [5] ISO27001 Certification: Global Trust

Focus: [1] Risk Assessment [2] Risk Treatment- mitigation and remediation [3]ISO 27001- ISMS cycle, documentation, internal & external audits

Performance: [1] Quality and Quantity of risk issues. [2] Cost implications versus potential benefits [3] Closure of risk issues [4] ISO 27001- Attain & maintain certification

Outcome: [1] Address only known issues [2] Risk Assessment is subjective [3] Hidden plane of uncertainties [4] Compliance takes priority over risk management.

## Responsive Security

[1] Approach developed to address weakness of commercial security and risk-based approach. [2] Piezoelectric Theory: If org is prepared to respond to security event, it will incur less negative impact. Level of responsiveness is direct outcome of investment in readiness program. [3] Focus on 3 areas: Visibility of change, Situation awareness upon detection of sig changes, crit align as respond to re-align important value to new situation. [4] Social Techniques:

a. Stakeholder analysis and engagement, b. Dialectic Model of System Inquiry (DMSI): Understand system requirement & create solution model taking into considerations the ideal model and practical constraints in op env,

c. Five-Level Action Map(FLAM): Identify & organize program, projects, task and identify intra and inner-relationships with ongoing change events & technical systems,

d. Flood Four Window System view: evaluate outcomes from 4 different system thinking perspective.

[5] FMEA: technical technique to identify modes of potential failure in a given system, then apply FTA to identify fault.

Drive: [1] Recognize weak links prevail [2] Intro readiness as key to hidden & emerging risk [3] Readiness and responsiveness metric to demo state of readiness [4] Measure impact thru state of readiness metric

Focus: [1] 50% on a risk-based/isms program to address known issues and other to social-technical on the 3 focus areas. [2] Prepare, detect and respond [3] Action learning practices to understand & influence stakeholders.

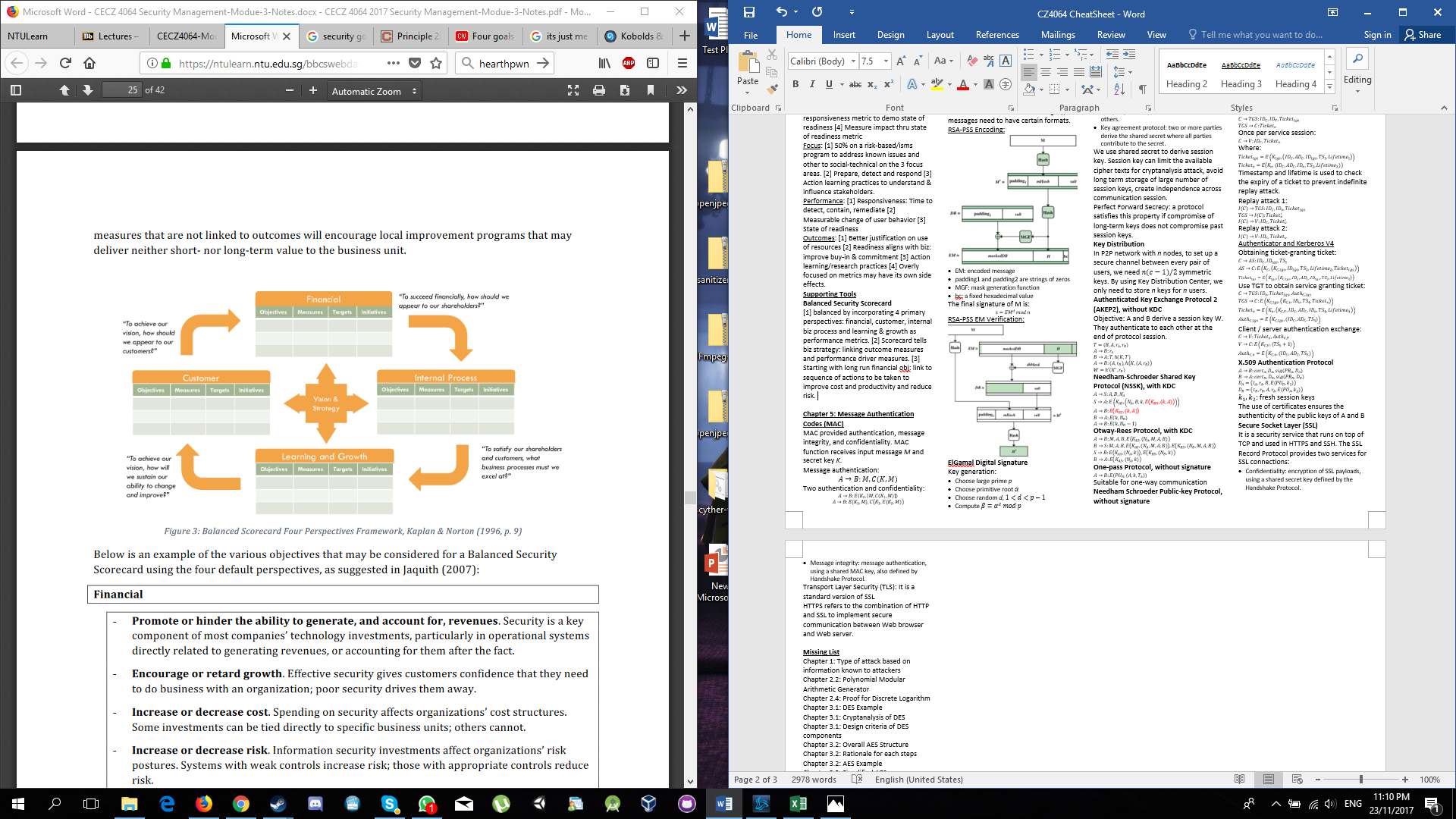
Performance: [1] Responsiveness: Time to detect, contain, remediate [2] Measurable change of user behavior [3] State of readiness

Outcomes: [1] Better justification on use of resources [2] Readiness aligns with biz: improve buy-in & commitment [3] Action learning/research practices [4] Overly focused on metrics may have its own side effects.

# Chapter 5.2: Supporting Tools

## Balanced Security Scorecard

[1] balanced by incorporating 4 primary perspectives: financial, customer, internal biz process and learning & growth as performance metrics. [2] Scorecard tells biz strategy: linking outcome measures and performance driver measures. [3] Starting with long run financial obj: link to sequence of actions to be taken to improve cost and productivity and reduce risk.



Drive: [1] provide natural extension [2] Means to align info security values with biz values. [3] Clear biz outcomes, measurable.

Focus: [1] Implement: Identify and measure appropriate driver’s measures for desired outcome. Metrics must show strong cause and effect linkages. [2] Execute [3] Reviews & updates: Strategic reviews made to govern executions and on-track progress to deliver measures.

Performance: [1] Overall demonstrated by outcome metrics [2] Individual/grp: shown by achieving performance driver in 4 perspectives.

Outcome: [1] Metric saturation may result [2] Could result in ambiguity [3] Limitation on measurement.

## Security Maturity Model

[1] Process-Oriented model: 1. Initial ->Managed -> Defined -> Controlled-> Optimized. [2] Security is result of continuous meeting/exceeding a set of obj [3] Incident means failure to achieve 1/+ mgm’s agreed biz and security obj. [4] Does not demand risk assessment-based approach.

Drive: [1] Benchmark against others [2] Justify spending [3] Determine if resources are used effectively.

Focus: [1] Determine current state of maturity. [2] Address capability gaps [3] Attaining next level up “Optimizing” state

Performance: [1] Overall based on measurement of status [2] Specific capability measures by related metrics: reflects performance [3] Adoption vs custom design and build.

Outcomes: [1] Improve visibility [2] May drive compliance culture [3] Process-oriented: May leave out human aspect [4] Risk on relying on benchmark.

# Chapter 6: Organization and people

Centralized: [1] All info sec staff report to single corporate grp. [2] Consistent people mgm policy and benefits [3] Facilitate allocation of mgm of resources.

Decentralized: Regional decentralization

Info Security Steering committee: [1] Coordinate security strategy across multiple functions: reduce duplication and risk [2] Common charter: policy review and approval [3] Factors influencing effectiveness: Leadership, Infosec/CISO role in committee, Membership, freq & duration of meeting.

External Relationship: [1] Contact w Authorities. [2] Key contacts: Law enforcement, cert org. [3] Info Sharing [4] Industry/Professional Org [5] Academic & research Institutions.

Stakeholders: [1] Infosec grp [2] Senior leaders and exec: Key decision makers. [3] Employees and partners’ associates [4] External Stakeholders: Law enforcement, gov officials, academia.

[5] Analysis: To identify key stakeholders, analyze position, and plan strategy to gain support.

## 6.1: Principles & policies

[1] Clearly defined duties [2] Separation of duties [3] Dual Control: Require combination of 2 people. [4] Rotation of duties/ Mandatory vacation policy: Avoid risk Habituation and reveal dishonesty. [5] Due care & due diligence [6] Establish Ethical Standards [7] Key man policies [8] Identity lifecycle process [9] Non-disclosure, non-competition and intellectual property protection agreements [10] Carrot and stick

## 6.2: Code of Ethics

[1] Preamble: Safety of commonwealth needs highest ethical standards of behavior [2] 4 Canons: -Protect society, commonwealth &infras, -Act honorably, honestly, justly, responsibly & legally, - Provide diligent and competent service to principals, - Advance and protect the profession

## 6.3: Infosec Professionals & practitioners

[1] Academic Qualifications [2] Professional Certification [3] Working Experience [4] Personality

## Programs

### Security Awareness Program

[1] Ensure awareness of general threat, security policies requirements and secure practices [2] Traditional Approach

Drive: [1] Low cost [2] easy implementation

Focus: [1] Identify messages to comm, [2] organize material and trainer [3] get consensus from mgm and deliver

Performance: [1] Quiz/test to measure understanding

Outcomes: [1] Mostly attend and forget overtime [2] Provide coverage but may not change behavior.

### Security Competency Program

[1] Ensure security related roles are trained to deliver services. [2] Practice oriented to develop specific skills.

Drive: [1] Targeted roles may be subjected to attacks therefore need to understand, detect and defend.

Focus: [1] Identify target roles and specific security skills needed.

Performance: [1] Measured by % of security escalations and severity of incidents. [2] Employee satisfaction

Outcomes: [1] Reduce errors [2] Improve Cooperation btw security f() & targeted job roles [3] Pre-requisite knowledge may be needed. [4] Higher cost [5] Only cover limited number of roles

### Security Readiness Program

[1] Based on principles of responsive security [2] Exposure to incident scenarios build capability and increase capacity to response.

Drives: [1] Responsiveness improved thru practices and measured scenario planning and exercises.

Focus: [1] Identify crit-roles and potential

crit-incidents scenarios [2] Establish facilities and systems to conduct forms of exercise required for each readiness outcomes

Performance: [1] Measured by level of readiness and responsiveness.

Outcome: [1] Change of behavior thru exercise [2] Improve insights on weakness, gaps. [3] measure efficiency, effectiveness, and reliability of multiple grp based on scope of incident scenarios.

# Chapter 7: Security Operations

Security operations: mgm of security services

Operation security: [1] increase awareness [2] reduce potential incidents

# Chapter 7.1: Scope of security Operations

## Client Management

[1] Client Requirement and expectation:

[2] Client Experience & satisfaction

[3] Executive relationship  
[4] Service level Agreement (SLA): [1] Comm tool [2] Expectations-managing mechanism [3] Conflict-reduction tool [4] Living document [5] Objective process for gauging service effectiveness

It is not : [1] mandate [2]used to get your way [3] complaint-stifling mechanism [4] Unilateral decision-making process [5] quick fix  
Service Metrics

## Operation management

[1] Service Ownership & responsibilities

[2] Cost management: [1] Ensure security op can be met. [2] Funding model- Corporate(centralized) vs Client (distributed) funding

[3] Efficiency, reliability, effectiveness, meaningfulness and fairness

[4] Performance metrics: [1] Cost Metrics [2] Workload and efficiency Metrics [3] Security/ Risk metrics

## Security Services Delivery

# Chapter 7.2: user & privilege mgm

[1] Provision of identity and access

[2] Password management: [1] Use of single-signon [2] Password Change Policy [3] Password Change Capability [4] Password Reset Tool

[3] Security Token mgm: [1] 2FA [2] Security token must be randomly generated [3] Smartcards [4] Activation process

[4] Privilege management: [1] Policy control: Separation of duties, Personnel Security, Security education, Duress procedure [2] Technical Controls: Security Monitoring, 2FA for admin level access

[5] Termination: [1] Pre-termination security check [2] briefing to remind of legal contract. [3] Recovery of computing devices.

# 7.3: Key management

[1] Hardware Security module(HSM): [1] Escrow and recovery of Root Key [2] Key gen [3] Destruction of key

[2] Application Specific requirements: [1] Secure Pin [2] Activation Code [3] Smartcard key gen

[3] PKI

# 7.4: Change Management:

[1] Access control mgm [2] Infras changes [3] Server & operating system changes [4] Application changes [5] User changes

# 7.5: Vulnerability management

Vuln mgm tool -> Vuln Scanner -> Network IDS -> managed Sec System -> back

# 7.6 Security Monitoring

## Monitoring and Detection System

[1] Real-Time Monitoring: [1] Using audit trail records/logs and network traffic and analyzing events to detect potential intrusion attempts.

Intrusion/Attack analysis: [1] Pattern- or signature based [2] Anomaly Based [3] Correlation Tools

# Chapter 8: Internet Control, Audit and Security

## 8.1: Committee of Sponsoring Organization of Treadway Commission

Definition of framework obj and internal control: [1] Effectiveness & efficiency of operations [2] Reliability of financial reporting [3] Compliance with applicable laws & regulations [4] Safeguarding of Assets

Framework: [1] Internal control is a process [2] Internal Control affected by people at every level [3] Internet control can be expected to provide only reasonable assurance [4] Internal control is geared to the achievement of objs with overlapping categories

Practices: [1] Control Self-Assessment [2] Automated/Semi-automated Checks [3] Internal Reviews [4] Security Metrics

Limitations: [1] Involve human actions: Possible in judgement error [2] Can be overridden by collusion or coercion by top management [3] Complxity of 3-D framework, many matrices, increase number of audits & related cost [4] Risk and control matrix might not fit framework.

## 8.2: COBIT

Concepts: [1] Framework for gov and mgm [2] Promote adoption of 5 principles and 7 Enablers [3] Embed controls into way of doing things in IT

Drives: [1] “Design-inn Control”: no surprises in undesirable events. [2] Cost of controls embedded in IT investments up front: No separate security investments

Focus: [1] Optimize IT investments & use

Performance: [1] Compliance w IT policies & control [2] Measure thru internal self-assessment and IT audits

Outcomes: [1] Compliance-driven culture [2] Compliance! = Security [3] Address what IT auditors and regulators’ concerns mostly

5 principles: [1] Meeting Stakeholder Needs [2] Covering Enterprise End to end [3] Applying a Single Integrated Framework [4] Enabling holistic Approach [5] Separating Gov from Mgm

7 enablers: [1] Principles, policies and Framework: comm infosec requirements and direction [2] Process: Describes specific/ detailed info sec activity [3] Organization Structure [4] Culture, Ethics and behavior [5] Info on sec [6] Service, infras and application [7] People, skills, competencies.

## 8.3. IT Audit

Internal: [1] Advisory & Monitoring role [2] Focus on effectiveness of controls [3] Report to op mgm/audit committee

External: [1] Effectiveness of internal control & audit [2] Regulatory mandate

General principles: [1] Compliance Test [2] Substantive Test [3] Control Analysis

\*[1] to [2] if [1] fails. [2] to [3] if [2] fails.

## 8.4. SOC reports and Purposes

SOC 1 (SSAE-16): Report on controls at service organization that may be relevant to user entities’ internal control over financial reporting

SOC 2: Evaluate org’s info system relevant to security, availability, processing integrity confidentiality or privacy

SOC 3: Similar to 2 except don’t detail testing

Benefits: [1] Provide assurance via trusted 3rd party: For service consumers [2] A means to demonstrate continuous compliance to internal policy: For service providers [3] Leverage for providing required assurance without conducting another audit.

Limitations: [1] Attestation based on org’s internal policies which might not align with international standard [2] Costly undertaking

## 8.5: Application Security

[1] Implements and enforces biz rules to prevent, detect and respond to potential attacks. [2] Secure itself against attempts to compromise application security to bypass biz rules &/ breach security of data processed by application

ISC Approach –The CSSLP: [1] Based Credential [2] Professional Cert program [3] Holistic approach to security in software cycle [4] Test candidate’s knowledge, skills, abilities to significantly mitigate the sec concerns

Purpose: [1] Address building security throughout the entire software lifecycle

[2] Provide credential to prove person’s ability

## 8.6 Cloud Computing

Characteristics/benefits: [1] On-demand self-service [2] Broad network access [3] Resource Pooling [4] Rapid Elasticity [5] measured Service

Changed: [1] Cloud takes control of operation instead of customer taking control [2] Improve flexibility and speed [3] Multi-tenancy

Not-Changed: [1] Admin access [2] Personnel Security [3] Transparency of security measures and incidents [4] Shared tech infras [5] Only 3rd party access [6] APIs security

Internal control can help: [1] Gain visibility of what’s at risk [2] Privacy Impact assessment: identify data at risk [3] Security monitoring at edge [4] Determine validity of cloud resources utilization [5] Compliance audit [6] Verification of security architecture [7] Internet security mgm & control over cloud security

\*Milkological Production!\*