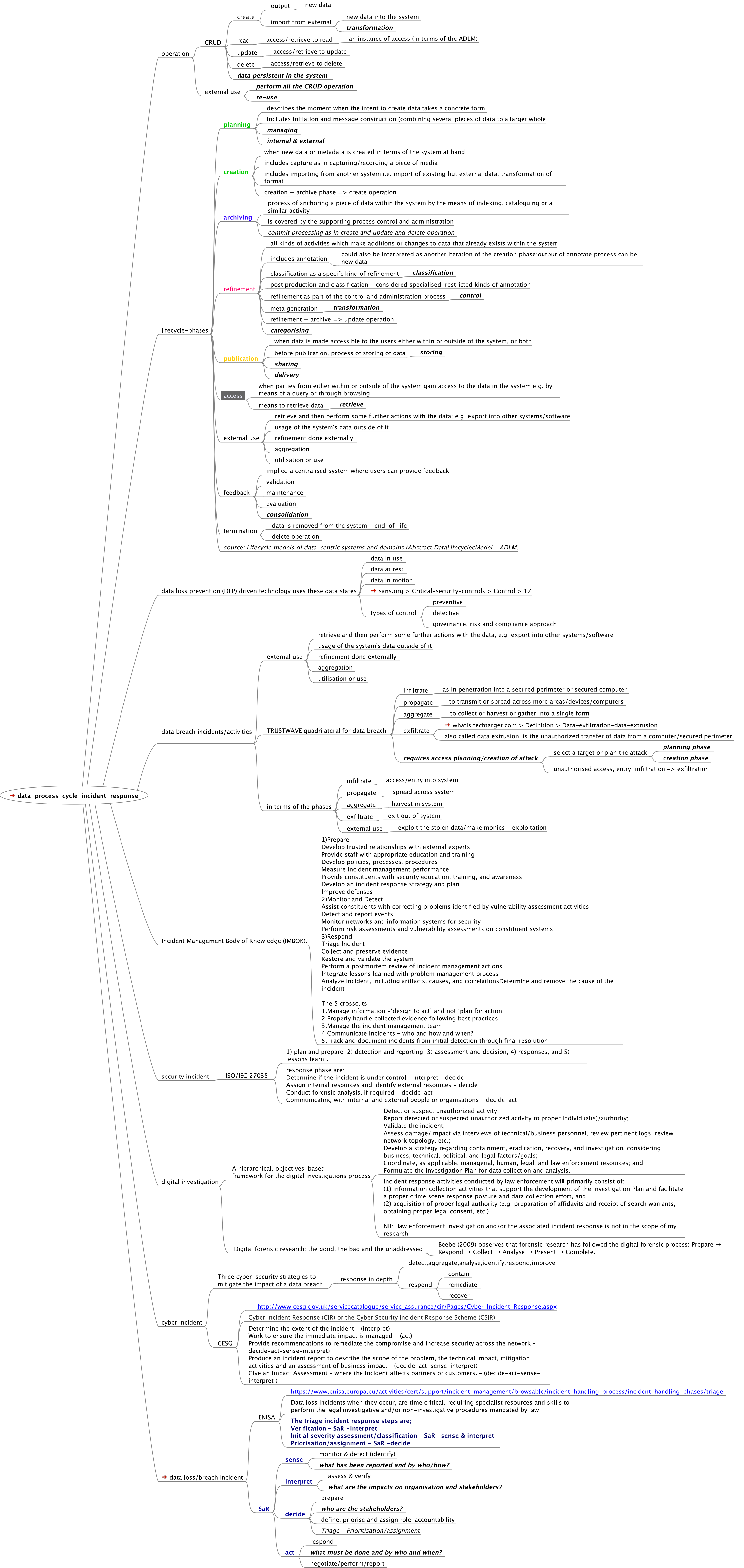

- ➜ **data-process-cycle-incident-response**
  - operation
    - CRUD
      - create
        - output
          - new data
        - import from external
          - new data into the system
          - ***transformation***
      - read
        - access/retrieve to read
          - an instance of access (in terms of the ADLM)
      - update
        - access/retrieve to update
      - delete
        - access/retrieve to delete
      - ***data persistent in the system***
    - external use
      - ***perform all the CRUD operation***
      - ***re-use***
  - lifecycle-phases
    - **planning**
      - describes the moment when the intent to create data takes a concrete form
      - includes initiation and message construction (combining several pieces of data to a larger whole
      - ***managing***
      - ***internal & external***
    - **creation**
      - when new data or metadata is created in terms of the system at hand
      - includes capture as in capturing/recording a piece of media
      - includes importing from another system i.e. import of existing but external data; transformation of format
      - creation + archive phase => create operation
    - **archiving**
      - process of anchoring a piece of data within the system by the means of indexing, cataloguing or a similar activity
      - is covered by the supporting process control and administration
      - *commit processing as in create and update and delete operation*
    - refinement
      - all kinds of activities which make additions or changes to data that already exists within the system
      - includes annotation
        - could also be interpreted as another iteration of the creation phase;output of annotate process can be new data
      - classification as a specifc kind of refinement
        - ***classification***
      - post production and classification - considered specialised, restricted kinds of annotation
      - refinement as part of the control and administration process
        - ***control***
      - meta generation
        - ***transformation***
      - refinement + archive => update operation
      - ***categorising***
    - publication
      - when data is made accessible to the users either within or outside of the system, or both
      - before publication, process of storing of data
        - ***storing***
      - ***sharing***
      - ***delivery***
    - access
      - when parties from either within or outside of the system gain access to the data in the system e.g. by means of a query or through browsing
      - means to retrieve data
        - ***retrieve***
    - external use
      - retrieve and then perform some further actions with the data; e.g. export into other systems/software
      - usage of the system's data outside of it
      - refinement done externally
      - aggregation
      - utilisation or use
    - feedback
      - implied a centralised system where users can provide feedback
      - validation
      - maintenance
      - evaluation
      - ***consolidation***
    - termination
      - data is removed from the system - end-of-life
      - delete operation
    - *source: Lifecycle models of data-centric systems and domains (Abstract DataLifecyclecModel - ADLM)*
  - data loss prevention (DLP) driven technology uses these data states
    - data in use
    - data at rest
    - data in motion
    - ➜ sans.org > Critical-security-controls > Control > 17
    - types of control
      - preventive
      - detective
      - governance, risk and compliance approach
  - data breach incidents/activities
    - external use
      - retrieve and then perform some further actions with the data; e.g. export into other systems/software
      - usage of the system's data outside of it
      - refinement done externally
      - aggregation
      - utilisation or use
    - TRUSTWAVE quadrilateral for data breach
      - infiltrate
        - as in penetration into a secured perimeter or secured computer
      - propagate
        - to transmit or spread across more areas/devices/computers
      - aggregate
        - to collect or harvest or gather into a single form
      - exfiltrate
        - ➜ whatis.techtarget.com > Definition > Data-exfiltration-data-extrusion
        - also called data extrusion, is the unauthorized transfer of data from a computer/secured perimeter
      - ***requires access planning/creation of attack***
        - select a target or plan the attack
          - ***planning phase***
          - ***creation phase***
        - unauthorised access, entry, infiltration -> exfiltration
    - in terms of the phases
      - infiltrate
        - access/entry into system
      - propagate
        - spread across system
      - aggregate
        - harvest in system
      - exfiltrate
        - exit out of system
      - external use
        - exploit the stolen data/make monies - exploitation
  - Incident Management Body of Knowledge (IMBOK).
    - 1)Prepare
      Develop trusted relationships with external experts
      Provide staff with appropriate education and training
      Develop policies, processes, procedures
      Measure incident management performance
      Provide constituents with security education, training, and awareness
      Develop an incident response strategy and plan
      Improve defenses
      2)Monitor and Detect
      Assist constituents with correcting problems identified by vulnerability assessment activities
      Detect and report events
      Monitor networks and information systems for security
      Perform risk assessments and vulnerability assessments on constituent systems
      3)Respond
      Triage Incident
      Collect and preserve evidence
      Restore and validate the system
      Perform a postmortem review of incident management actions
      Integrate lessons learned with problem management process
      Analyze incident, including artifacts, causes, and correlationsDetermine and remove the cause of the incident

      The 5 crosscuts;
      1.Manage information -'design to act' and not 'plan for action'
      2.Properly handle collected evidence following best practices
      3.Manage the incident management team
      4.Communicate incidents - who and how and when?
      5.Track and document incidents from initial detection through final resolution
  - security incident
    - ISO/IEC 27035
      - 1) plan and prepare; 2) detection and reporting; 3) assessment and decision; 4) responses; and 5) lessons learnt.
      - response phase are:
        Determine if the incident is under control - interpret - decide
        Assign internal resources and identify external resources - decide
        Conduct forensic analysis, if required - decide-act
        Communicating with internal and external people or organisations -decide-act
  - digital investigation
    - A hierarchical, objectives-based framework for the digital investigations process
      - Detect or suspect unauthorized activity;
        Report detected or suspected unauthorized activity to proper individual(s)/authority;
        Validate the incident;
        Assess damage/impact via interviews of technical/business personnel, review pertinent logs, review network topology, etc.;
        Develop a strategy regarding containment, eradication, recovery, and investigation, considering business, technical, political, and legal factors/goals;
        Coordinate, as applicable, managerial, human, legal, and law enforcement resources; and
        Formulate the Investigation Plan for data collection and analysis.
      - incident response activities conducted by law enforcement will primarily consist of:
        (1) information collection activities that support the development of the Investigation Plan and facilitate a proper crime scene response posture and data collection effort, and
        (2) acquisition of proper legal authority (e.g. preparation of affidavits and receipt of search warrants, obtaining proper legal consent, etc.)

        NB: law enforcement investigation and/or the associated incident response is not in the scope of my research
    - Digital forensic research: the good, the bad and the unaddressed
      - Beebe (2009) observes that forensic research has followed the digital forensic process: Prepare → Respond → Collect → Analyse → Present → Complete.
  - cyber incident
    - Three cyber-security strategies to mitigate the impact of a data breach
      - response in depth
        - detect,aggregate,analyse,identify,respond,improve
        - respond
          - contain
          - remediate
          - recover
    - CESG
      - http://www.cesg.gov.uk/servicecatalogue/service_assurance/cir/Pages/Cyber-Incident-Response.aspx
      - Cyber Incident Response (CIR) or the Cyber Security Incident Response Scheme (CSIR).
      - Determine the extent of the incident - (interpret)
        Work to ensure the immediate impact is managed - (act)
        Provide recommendations to remediate the compromise and increase security across the network - decide-act-sense-interpret)
        Produce an incident report to describe the scope of the problem, the technical impact, mitigation activities and an assessment of business impact - (decide-act-sense-interpret)
        Give an Impact Assessment - where the incident affects partners or customers. - (decide-act-sense-interpret)
  - ➜ data loss/breach incident
    - ENISA
      - https://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process/incident-handling-phases/triage-
      - Data loss incidents when they occur, are time critical, requiring specialist resources and skills to perform the legal investigative and/or non-investigative procedures mandated by law
      - **The triage incident response steps are;**
        Verification - SaR -interpret
        Initial severity assessment/classification - SaR -sense & interpret
        Priorisation/assignment - SaR -decide
    - **SaR**
      - **sense**
        - monitor & detect (identify)
        - ***what has been reported and by who/how?***
      - **interpret**
        - assess & verify
        - ***what are the impacts on organisation and stakeholders?***
      - **decide**
        - prepare
        - ***who are the stakeholders?***
        - define, priorise and assign role-accountability
        - *Triage - Prioritisation/assignment*
      - **act**
        - respond
        - ***what must be done and by who and when?***
        - negotiate/perform/report