DOMAIN 2, BOOKLET 2

CC in a Nutshell

Incident Response (IR), Business Continuity (BC), and Disaster Recovery (DR)

By BELKHiR Selma

Incident Response (IR)

Objective: Respond to abnormal operating conditions to keep the business running.

Main components:

Preparation: Plan for incidents before they occur.

Detection and Analysis: Plan for incidents before they occur.

Containment, Eradication, and Recovery: Limit the damage and restore systems.

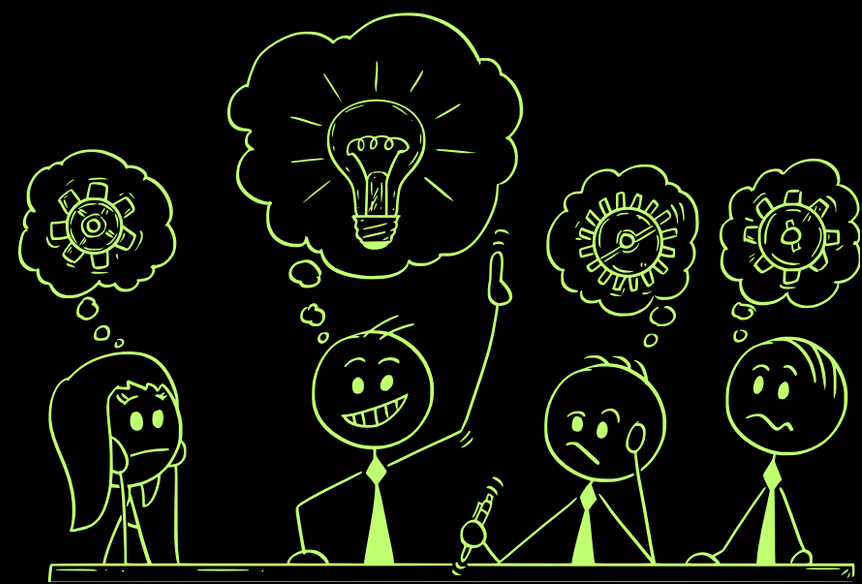
Post-Incident Activity: Review the incident and improve processes.

Incident Response Team (IRT)

ARE TYPICALLY A CROSS-FUNCTIONAL GROUP OF INDIVIDUALS WHO REPRESENT : MANAGEMENT, TECHNICAL, AND FUNCTIONAL STAFF.

THREE POSSIBLE MODELS FOR AN INCIDENT RESPONSE TEAM :

- LEVERAGED
- DEDICATED
- HYBRID



Business Continuity (BC)

OBJECTIVE: ENSURE THE ORGANIZATION CAN OPERATE DURING A CRISIS.

MAIN COMPONENTS:

-CONTACT METHODS FOR TEAM MEMBERS, INCLUDING BACKUP MEMBERS.

-IMMEDIATE RESPONSE PROCEDURES: CHECKLISTS FOR FIRE SUPPRESSION, EMERGENCY AGENCIES, ETC.

-NOTIFICATION SYSTEMS: CALL TREES TO ALERT PERSONNEL.

-GUIDANCE FOR MANAGEMENT: INCLUDING DESIGNATION OF AUTHORITY.

-CONTACT NUMBERS FOR THIRD-PARTY PARTNERS, VENDORS, AND EMERGENCY PROVIDERS.

Disaster Recovery (DR)

Objective: Restore operations to normal as quickly as possible after major failures

Main Components:

- **Executive Summary:** High-level overview of the plan.
- **Department-Specific Plans:** Tailored to each department's needs.
- **Technical Guides:** For IT personnel to manage critical systems.
- **Full Copies of the Plan:** For critical disaster recovery team members.
- **Checklists:** For individuals responsible for specific tasks.

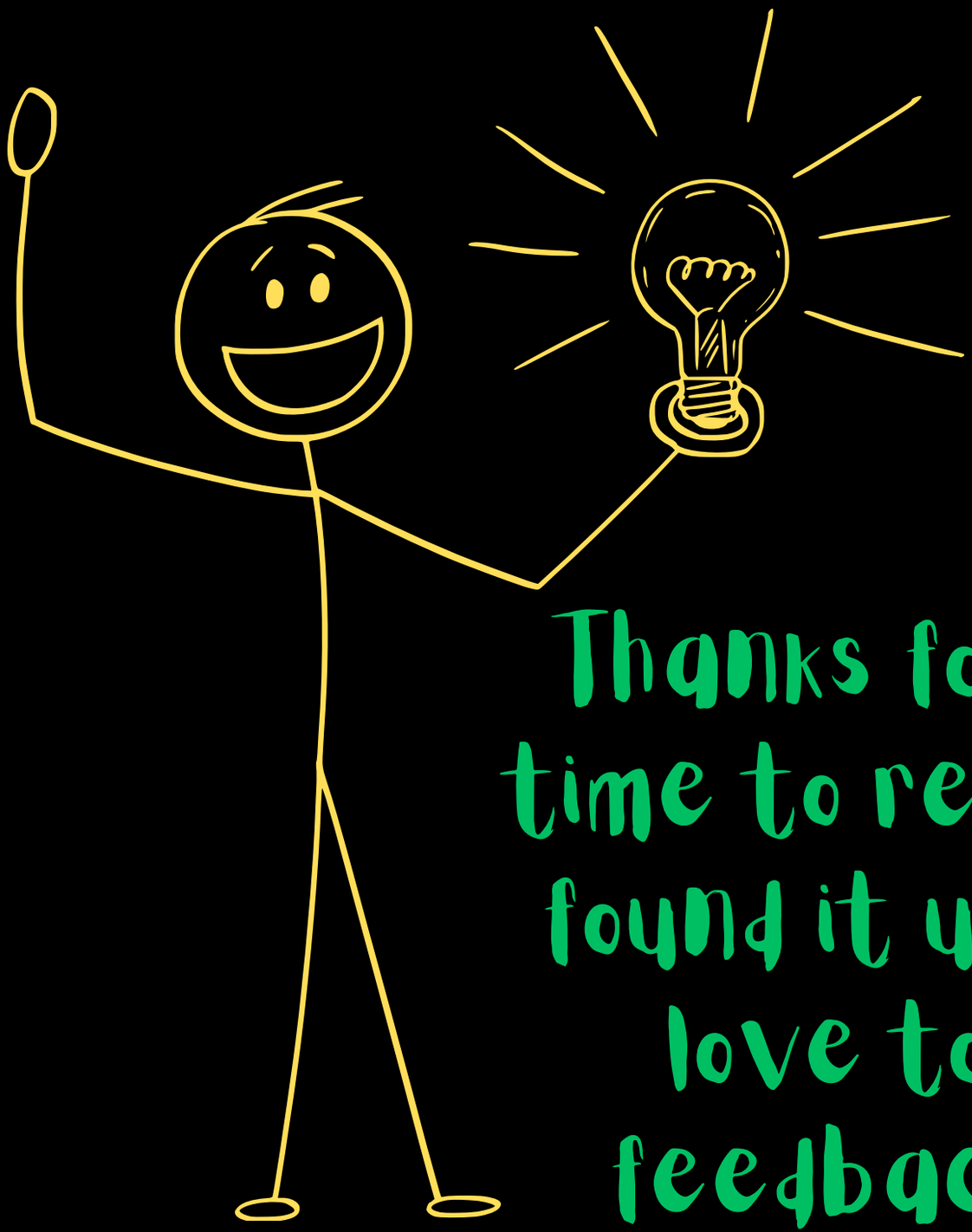
key terminology

-INCIDENT: AN EVENT THAT COULD COMPROMISE CONFIDENTIALITY, INTEGRITY, OR AVAILABILITY.

-BREACH: UNAUTHORIZED ACCESS OR COMPROMISE OF SENSITIVE INFORMATION

-EXPLOIT: AN ATTACK THAT TAKES ADVANTAGE OF SYSTEM VULNERABILITIES.

-ZERO DAY: A VULNERABILITY THAT IS UNKNOWN TO SYSTEM MAINTAINERS AND COULD BE EXPLOITED WITHOUT PRIOR DETECTION.



Thanks for taking the time to read! I hope you found it useful, and I'd love to hear any feedback you might have.

By BELKHiR Selma