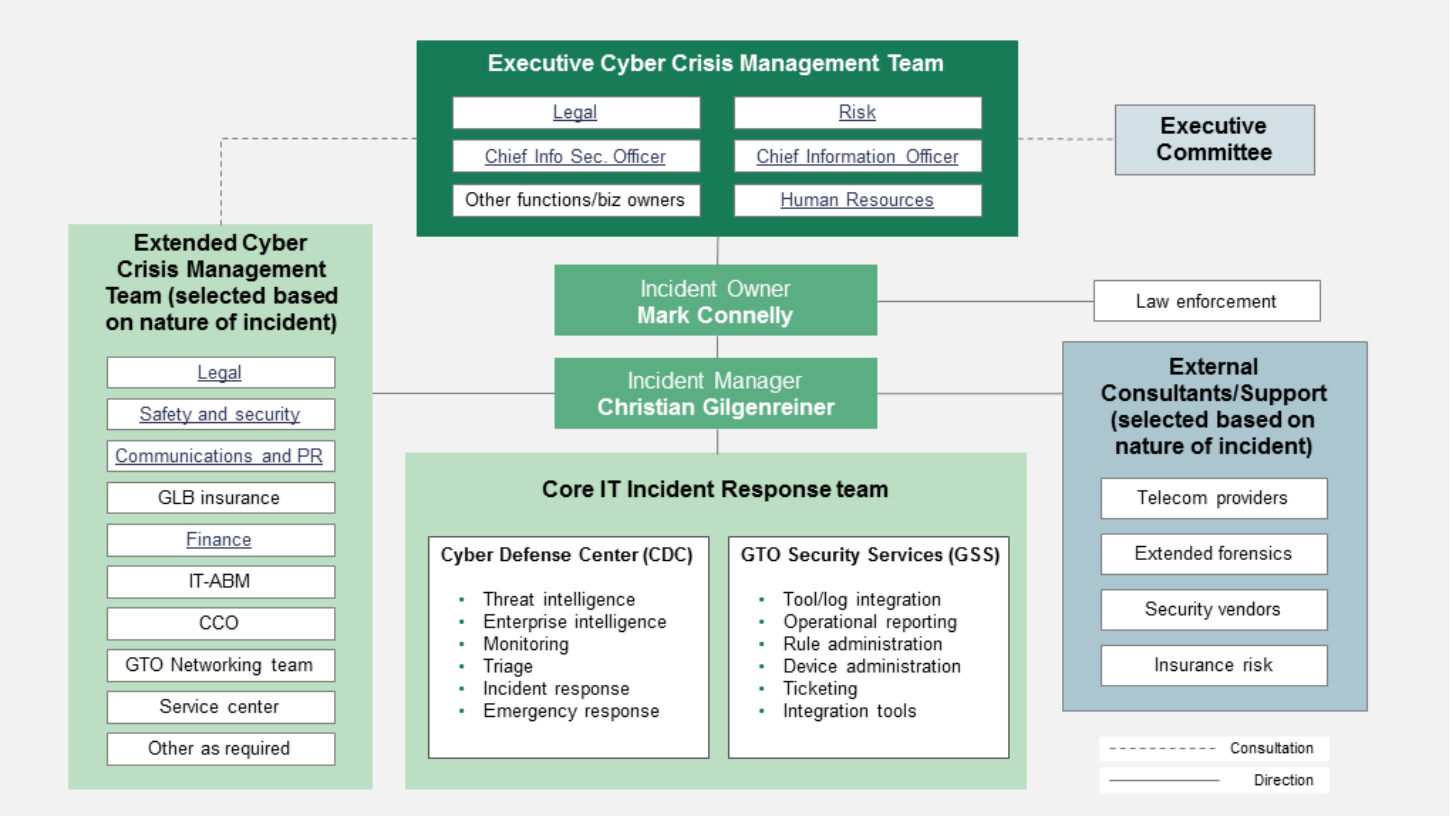
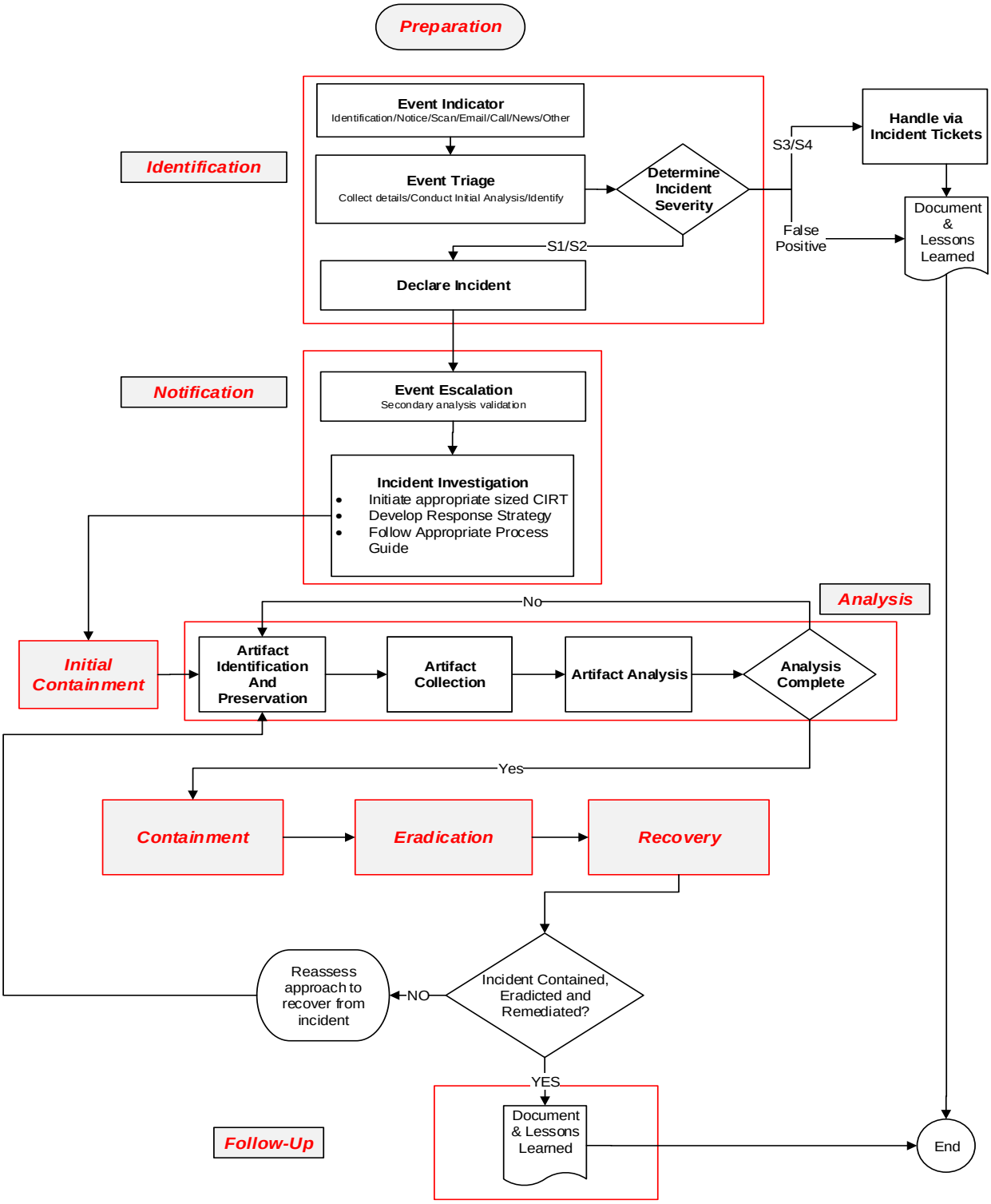
CYBERSECURITY INCIDENT RESPONSE TEAM (CIRT) FUNCTIONAL RELATIONSHIPS DURING AN INCIDENT, DENOTING PROCESS AND INFORMATION FLOW ALONG WITH MANAGEMENT HIERARCHY.



NINE-STEP INCIDENT MANAGEMENT LIFECYCLE



CYBER INCIDENT CATEGORIES AND SEVERITY

Category	Definition
CAT 0:	Used during cyber security exercises and approved activity testing of the internal/external network defenses or response capabilities.
CAT 1:	Used if an individual gains logical or physical access without permission to a BCG network, system, application, data, or other resource.
CAT 2:	Used if an attack successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources (i.e. DDoS).
CAT 3:	Used if an attacker successfully deploys malicious software that infects a BCG operating system or application.
CAT 4:	Used if an attacker/individual violates acceptable computing use policies.
CAT 5:	Includes any activity that seeks to access or identify a BCG computer, port(s), protocol(s), service, or any combination for later exploit.
CAT 6:	Includes unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

Severity	Description
S1	• Potential for widespread impact. • Potential that sensitive data will be disclosed or stolen (privacy and/or proprietary). • Potential that client and/or data subjects and/or public notifications will be required. • Recovery from the incident is unpredictable and/or not possible.
S2	• Potential for widespread impact. • Potential that sensitive data will be disclosed or stolen (privacy and/or proprietary). • Unlikely that client and/or data subjects and/or public notifications will be required. • Will require additional resources to recover from the incident.
S3	• Likely to be limited to few affected systems. • Unlikely to lead to loss or theft of sensitive data. • Unlikely that client and/or data subjects and/or public notifications will be required. • Will require additional resources to recover from the incident.
S4	• Likely to be limited to few affected systems. • Unlikely to lead to loss or theft of sensitive data. • No impact to brand. • No additional resources needed for recovery.

MOST COMMON CYBER INCIDENT TYPES

Event or Incident Type	Description	Category (As defined in table 3 above)
Acceptable Use Violation	An internal employee or contractor utilizes their authorized access to engage in actions that violate the Acceptable Use Policy.	4
Cyber Intrusion	Unauthorized privileged and remote access to a system. Privileged access, often referred to as administrative or root access, provides unrestricted access to the system. Interactive access may include automated tools that establish an open channel of communications to and/or from a system. This category includes unauthorized access to domain administrator accounts and may include the loss or potential loss of non-regulated data.	1
Data Loss	Unauthorized disclosure of business sensitive data or data protected by various regulations or contractual obligations.	1
Denial of Service	Activity that denies, degrades, or disrupts normal functionality of a system or network. The severity of this can and should be raised proportionate to its effect on the network and business operations.	2
Device Loss or Theft	The loss or theft of a physical computing asset that may contain confidential or regulated data. The loss or theft of a computing device may or may not result in unauthorized disclosure of the data residing on the device.	1
Email Blacklisting	The inclusion of BCG email servers on one or more of many email blacklisting services' lists of malicious email servers. Presence on these lists could prevent legitimate BCG business email from reaching its destination. Email servers get blacklisted when they are observed sending spam or malicious content.	2
Insider Threat	Internal staff, contractors, or authorized partners exceeding their authority to access systems or data.	4
Malware	Detection of software designed and/or deployed by adversaries with malicious intentions for example, with the purpose of gaining access to resources or information without the consent or knowledge of the system owner or user. Types of malware include viruses, trojans and worms. Ransomware is classified separately. Malware that operates with elevated system privileges should be assigned a higher incident severity than malware that operates without elevated privileges.	3
Ransomware	A class of malicious code that is employed by attackers to encrypt local files and shared files in order to induce victims into paying a ransom that would result in the files being decrypted.	3
Recon and Information Gathering	Activity that seeks to gather information used to characterize systems, applications, networks, and users that may be useful in formulating an attack. This includes activity such as mapping networks, systems, devices and applications, interconnectivity, and their users or reporting structure.	5

Event or Incident Type	Description	Category (As defined in table 3 above)
Social Engineering	Human interaction or deception used to gain access to resources or information through email (phishing), telephonic (vishing) or physical solicitation.	5
Web Site Compromise	An exploit of a web site or web server for the purposes of web site defacement (hacktivist, Cat 2) or preparatory intrusion (advanced threats, Cat 5).	2, 5
Zero-day Vulnerability	A vulnerability in software or firmware for which there is no available patch.	3

STANDARD TEMPLATES

- Incident Declaration Message Template
- Cybersecurity Incident Response Team Participant Daily Report Message Template
- Incident Manager Daily Report Message Template
- Incident Timeline Form
- Incident Threat Indicator Tracking Form
- Chain-of-Custody Form
- Final Report Template
- Personal Data Breach Register Report Template